Cognitive Load and Subjective Time Pressure: How Contextual Factors Impact the Quality of Cyber-Security Decision Making

George Raywood-Burke

A thesis submitted in partial fulfilment of the requirements of Cardiff University for the degree of Doctor of Philosophy

School of Psychology, College of Biomedical and Life Sciences, Cardiff University

December 2023

Thesis Summary

The quality of decision-making goes beyond simply considering outcomes as it is also determined by the suitability of the decision-making framework in the given circumstances, the probability of outcomes coming true, combined with the quality of the information available being utilised. However, with contextual pressures such as cognitive load and time pressure posing a threat to decision-making in cyber-security – how do people know whether they are making good decisions? This thesis aimed to examine the impact of cognitive load, how it applies to cyber-security decision-making quality, and subsequently how research to address this could be utilised in the development of tools and user-centric interventions to reduce risky cyber-security decision making. From theoretical cognitive science approaches to applied cyberpsychology research, 10 novel studies were developed, supported by systematic literature reviewing, with data collected from over 2000 participants. From this work, it was found increases in task difficulty could potentially increase insider threat when people are given the opportunity to act dishonestly, but this risk could be reduced by increasing awareness of time pressure. Sources of subjective time pressure, such as time urgency cues in emails, were found to increase susceptibility to cyber incidents – although, risk of such factors varies depending upon the perception of risk probability and outcomes. Whilst measures for individual differences in subjective time pressure were found to have a limited ability to predict safe cyber-security practices, other individual difference predictors were capable of explaining up to 43.5% of cyber-security behaviour variance. Through indicating when and where risky decision-making results in maladaptive behaviour, gain in knowledge has culminated in the creation of a new phishing susceptibility tool, based upon Expected Utility Theory, which could accurately explain 68.5% of behaviour. By highlighting risks in the overarching decision-making process, metacognitive interventions could be targeted to support quality cyber-security decision-making.

Contents

List of Tables and Figures

List of Appendices

Acknowledgements

First and foremost, I would like to thank Endeavr Wales for providing the opportunity for me to pursue my love and passion for psychological research by funding my PhD studentship. I have thoroughly enjoyed the experiences I have had working within Airbus Cyberlab and the Airbus Human-Centric Cyber-Security Accelerator; and from the networks and friendships I have developed through the Human Factors Research Excellence (HuFEx) group and the Centre for Artificial Intelligence, Robotics, and Human-Machine Systems (IROHMS) at Cardiff University. Thank you to my third supervisor, Dr Phoebe Asquith, for helping to proofread early drafts of experimental designs and for interrater reliability checks with the systematic review. Many thanks are due to the participants who had volunteered to take part in my research – without you, none of this would have been possible.

I am very grateful for the moral support from family, friends, colleagues, and loved ones throughout the period of the studentship – particularly my partner Sacha who has endured me along this journey: I look forward to the good times ahead. I would like to give special thanks to my dearly departed colleague Prof Bill Macken, and my second supervisor Prof Dylan Jones OBE, for their quick wit and wise advice - both of whom have left a lasting impression upon me.

Last, but certainly not least, is the person I would like to thank the most – my first supervisor, colleague, and friend, Prof Phil Morgan. Never have I met a more thoughtful, caring, and supportive individual who is passionately dedicated to what they do than Phil. I could not have wished for a better person to have been a guide along the way – a man who I would be proud to call my academic dad. Thank you.

Chapter 1: Decision Making under Pressure - Bounded Rationality versus Reality

1.1 – General Introduction: The Realities of Risk in Cyber-Security

When dealing with cyber-security, it is important to consider what poses a threat to users of technology across all environments (e.g., workplace, home, public spaces), what strengths and vulnerabilities may there be relating to managing these threats, and what are the consequences, both real and imagined, if these threats come to pass. Types of threats vary from malware attacks (e.g., viruses, ransomware, spyware) – to Denial-of-Service attacks designed to overload technology systems and hinder the ability to function normally (NCSC, 2016). Cyber-security could be breached, for example, through use of hardware connecting with workplace equipment, through Wi-Fi hotspots, or from engaging with phishing emails containing attachments, links or false web addresses. To try and address these real and ever evolving threats, technological interventions have been developed to reduce risk; for example - adopting machine learning based models to improve firewalls (Al-Haijaa & Ishtaiwia, 2021), novel improvements to Data Execution Prevention (DEP) methods which supersede antivirus software (e.g., Okamoto, 2015), and blockchain-based learning data environment models developed to verify the integrity of learning data from cyber-security systems using artificial intelligence – which in turn may prevent cyber-attacks (Kim & Park, 2020).

Whilst these technological advances have been shown to be useful in shoring up cyber-security, it is also important to consider the role of human interaction with technology (Morgan et al., 2020; Singh & Silakari, 2009). In recent years, over 80-90% of cyber incidents (CybSafe, 2020; Verizon, 2022; World Economic Forum, 2022) within businesses and involving individual users have human errors in e.g., decision making as significant factors. Across home and non-home working environments (and whilst on the move), humans have increasingly interacted with technology and the Internet of Things (IoT) – i.e., the interconnectivity and exchange of data between devices and systems over networks. This is part of most modern lifestyles, occurs daily in work and leisure situations, and across developed and developing countries (e.g., Darshan & Anandakumar, 2015; Li, Xu, & Zhao, 2015; Vilhelmson, Thulin, & Ellder, 2017); thus, there is great need for human-centric cyber-security research to understand risks in decision making and to develop interventions to help prevent them.

Increasing awareness to cyber-security policies is one example of a human-centric approach to cyber-security which could reduce engagement in risky behaviours, as studies seem to indicate when people are more aware of their companies' cyber-security policies, they are more likely to engage in safer behaviour in-line with the policy (e.g., Bishop et al., 2020; Li et al., 2019; Raywood-Burke et al., 2021). However, the longer-term effects of such interventions are less understood. Enforcement of information security policies with the aim of avoiding maladaptive behaviours has also been a key focus of this line of research whereby reward/punishment approaches – with some evidence suggesting that punishment of non-compliance and rewarding compliant behaviour can be effective in ensuring more secure cyber behaviours are encouraged (e.g., Chen, Ramamurthy, & Wen, 2014), though in other cases these interventions may not have large, or any, significant improvements upon compliance (e.g., Trang & Nastjuk, 2021). Even though evidence such as that provided by Trang and Nastjuk (2021) shows some benefits (albeit with a small effect size in reducing the influence of time stress) in adopting a punitive approach to ensuring policy compliance, other factors such as wellbeing and stress should be considered in the cost-benefit analysis when determining whether such an approach would be appropriate on balanced. Punishments could potentially increase fatigue over time (Danet, 2020), and result in even less compliance with cyber-security policies. Other sources of cognitive load, i.e., pressures which increase mental demand, such as task difficulty and time pressure are also important variables to consider in cyber-security – but more research has been needed to develop supporting theories and apply finding to a broader range of cyber-security behaviours.

Whilst these approaches are valid and useful focuses of human-centric cyber-security research, the optimal outcome desired from this area of research is the development of targeted interventions – tailored to circumstances and individuals (one-size-will-not-fit-all) who are making decisions under varying levels, and types of, time pressure. Thus, the approach of the research in this thesis, from a Cyberpsychology, Human Factors, and Cognitive Science perspective, was to focus on the significance of contextual factors which may overlap across different settings, to gain insight into differences in decision-making which can be applied to a range of cyber-security behaviours. The overarching aim was to examine the impact of cognitive load, how it applies in, and impacts upon, cyber-security decision making, and subsequently use this research as a platform to develop targeted tools and interventions to reduce human risk – specifically maladaptive behaviours. This was achieved through carrying out a systematic review and 10 studies, adopting a range of observational (Studies 6 and 7) and experimental methods (Studies 1-5, and 8-10). Together, these involved the assessment of all relevant literature (to the authors knowledge and based on systematic review criteria applied) from targeted topics and the collection of data from over 2000 individuals in a mixture of online and in-person studies with a range of tasks and paradigms. Collectively, the findings from these studies, implications and recommendations progress from the refinement and evaluation of psychological theory – with a key focus on cognitive load and time pressure - to more applied research to highlight the ability to predict, and evaluate, critical strengths and weaknesses in decision making across different cyber-security behaviours and contexts.

Initially, it was necessary to evaluate the theoretical development of a well-established cognitive science area highly linked to risky cyber-security behaviours – that of decision-making – to define how good decision making could be defined. As well as potentially identifying frameworks to underpin some aims and predictions, this approach also allowed exploration of gaps in the extensive cyber-security literature specifically linked to the main aims of the current thesis. Chapter 1 provides a detailed review of decision making theories and the impact of different types of workload (that could impact cyber-security decision making and subsequent behaviours) across various settings. Following the review of theoretical and applied literature, data was collected from over 1000 participants across five experiments to test to test theoretical gaps in our understanding of potential workload sources (i.e., task difficulty, awareness of time, type of task, and point in time in which cognitive resource depletion is instilled). Subsequent discussions of findings which can be drawn from these experiments (Studies 1-5) are detailed, and suggested implications of findings for cyber-security behaviour are made.

Chapter 2 transitions from Studies 1-5 on cognitive resource depletion theoretical evaluation established in Chapter 1 to explore a key focus of cognitive load in more applied settings - the relevance of time pressure in applied cyber-security contexts. This second chapter highlighted key findings in current research, what areas warrant further investigation, and informed the development of later studies to explore this phenomena. This was achieved by means of developing an extensive systematic review of subjective time pressure research in relation to cyber-security behaviours, using a refined search strategy across six databases to identify and assess relevant literature which was first carried out in 2020, but was updated to the date of the final search (11th February 2023). This built upon previous reviews which have largely focused on objective sources of time pressure (e.g., Choudhury et al., 2019), and highlighted evaluations of research on subjective time pressure where less has been previously explored in the context of cyber-security.

Chapter 3 applies knowledge gained from the findings of the systematic review of subjective time pressure by adopting novel designs to understand how subjective time pressure can influence judgement formation and behaviours. Chapter 3 consists first of a behavioural and subjective assessment of time urgency to evaluate their relevance as predictors of a range of cyber-security behaviours (in comparison with previously research individual difference predictors – Study 6) – with the additional aim of improving the validity of self-reported individual difference measurements through theoretical comparisons of data collected from an alternative to traditional Likert scales known as Visual Analogue Scales (VAS). Chapter 3 also investigates the accuracy of time perception and the significance this may have in cyber-security decision-making through the comparison of online and in-person behavioural data on time estimations (Study 7).

Finally, Chapter 4 involved the investigation of the potential interaction between objective and subjective time pressure in the key cyber-security context of phishing emails – comparing the impact of these factors with other major persuasive techniques (e.g. authority and scarcity) and email context (e.g. invoice reviewing, conference invitations). These three experiments (Studies 8-10) consist not just of comparisons between likelihood of responding to emails but collected reported utilities of outcomes and estimations of phishing probability to build decision-making profiles as a tool to highlight biases which increase or decrease the likelihood of responding to phishing.

The General Discussion unifies and evaluates all research conducted throughout the thesis – and critically in relation to related research including theoretical frameworks – to inform conclusions and future directions (as well as limitations) for human-centric cyber-security research – with a key focus on how targeted interventions could be developed to reduce susceptibility to maladaptive behaviours.

1.2 – Decision Making Theories

When setting out to investigate maladaptive behaviour in cyber-security, it is vital to first understand the nature of decision making. Think of an example of a good decision you have made and hold that in your mind. Now think of a bad decision you have made. What is the key difference(s) between the two? In a study carried out by Yates, Veinott, and Patalano (2003), participants were asked to think about examples of good and bad decisions they had made and consider why they would classify these decisions as "good" or "bad". They found outcomes of decisions dominated the reasons for labelling their decisions as such – but are the outcomes of decisions really the most important factors to decisions we make? An early attempt to model decision making is demonstrated by Expected Value Theory (EVT) – originating from letters exchanged between Blaise Pascal and Pierre de Fermat in the 17th century (noted in Hald, 1990). It is suggested the quality of a decision is based upon the *probability* of different outcomes in determining how specific actions may be more beneficial than others. The sum of outcome values (O) multiplied by their respective probabilities (p) is used to calculate the expected value (see equation below).

$$\boldsymbol{EV = \Sigma(O_n \times p_n)}$$

For example, in a coin toss gambling scenario where if the coin lands on heads you win £2 but win nothing if it lands on tails – the probability for each outcome is 50%. Therefore, the expected value in this case would be £1 (equation detailed below) – meaning if you were asked to pay more than this amount to play the coin toss then the option of choosing the play is not beneficial to you.

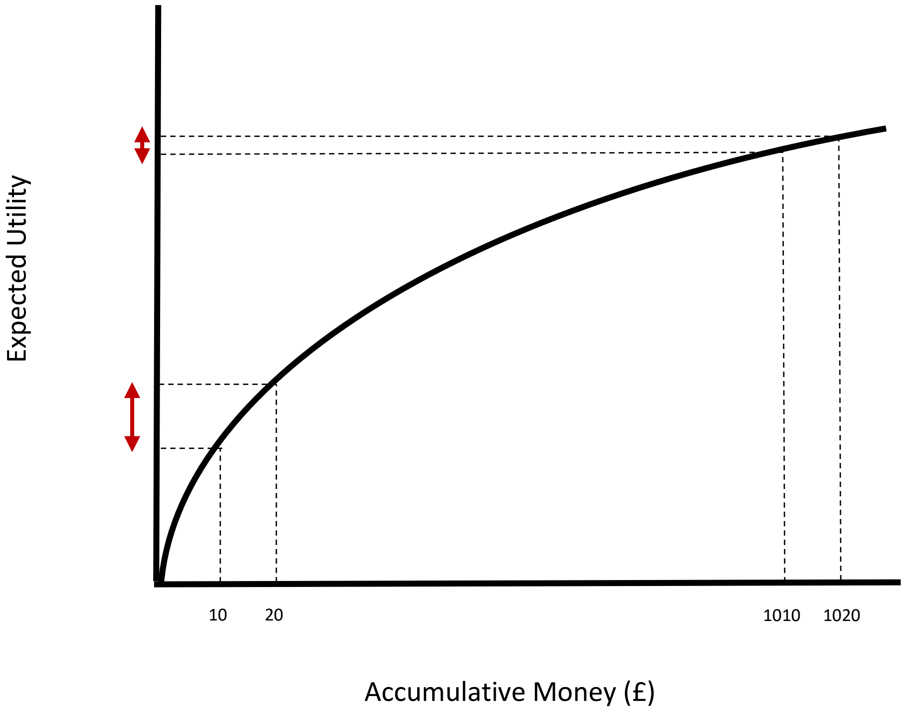
$$\boldsymbol{EV = (O_a \times p_a) + (O_b \times p_b) = (£2 \times 0.5) + (£0 \times 0.5) = £1}$$

There are however at least a few problems which are faced with this concept. Two things of psychological importance were detailed by Nicolas Bernoulli's cousin, Daniel Bernoulli (1738/1954), which offer an explanation for this difference between behaviour and EVT logic: the utility of money gained declines with increasing gains, and the utility of money gained is dependent upon the total money the individual already has (see Figure 1); therefore, this development by Daniel Bernoulli, known as Expected *Utility* Theory (EUT), built upon EVT in explaining a couple of reasons why human behaviour may vary from EVT predictions – the significance of perceived, proportionate, context.

In the context of cyber-security decision making, this point highlights – that actual human behaviour could differ from actuarially- or logically-based analyses of decisions – is important to note when judging where risks lie in cyber-security, and why interventions may, or may not, work. As an anecdotal example, adopting a security policy designed to prevent cyber breaches, such as increasing the complexity requirement of new passwords, whilst logically make it harder for passwords to be guessed or cracked, could in reality not consider other needs and motivations of users in the moment (e.g., ease of access, ability to memorise passwords). Subsequently, this could result in riskier work arounds (i.e., write down passwords, thus opening up the opportunity for others to gain access to online secured locations).

Figure 1.

A logarithmic graph demonstrating the visual concept for the relationship between wealth and perceived utility. Red arrows and dotted lines indicate comparative difference in expected utility in gaining £10 when starting with £10 versus £1010.



Von Neumann and Morgenstern (1953) built upon the notion of EUT to propose a model which could be used to improve rational decision making by maximising Expected Utility. Utilising this model, further developed by Savage (1954) to include the significance of subjectivity to information involved in decision making, would require obtaining a breakdown of subjective ratings for factors considered by the decision maker to be important consequences. This would include ratings for the expected utility of different potential outcomes along with the subjective probabilities each of these potential outcomes would come true. The Expected Utility for outcomes would be multiplied by their assigned subjective probabilities to generate the total Expected Utility for the options in the given decision – with the higher total Expected Utility of the decision options indicating the decision maker should enact this action.

To demonstrate, imagine you face the decision of choosing whether to reply or not reply to an email. However, it is possible for the email to be of the type phishing or genuine (i.e., non-malevolent). You imagine a list of aspects for the consequences of the choices of replying/not replying to an email which could be genuine or phishing and rate how important each of these aspects are for each the decision options there are available and then add them up (see Table 1 for an example). For example, there could be higher utility to respond to a genuine email for which the receiver could gain something consequently (such as getting to go to a conference or getting to purchase an item at a reduced amount) with not much lost if the decision was to not respond. However, the choice to respond to a phishing email would have no utility as the recipient could stand to lose personal wealth, information, or expose others to risk – thus there may be some utility in choosing not to respond by way of trying to reduce risk and maximise personal gains (e.g., through weighing up pros and cons in a form of cost-benefit analysis – Drèze & Stern, 1987; Kahneman & Tversky, 1979). Next, the probability of whether the email is likely to be genuine or phishing needs to be estimated (e.g., from looking at cues within the email such as the email address, links, images, as well as considering possible attachments). The subjective utility estimations for each potential outcome are then multiplied by the probabilities for phishing likelihood to calculate overall outcomes utilities for each possible outcome. These are then added together for each decision option, and whichever action expected utility value is highest indicates which option would be the best to choose – in the example highlighted in Table 1, the best choice suggested would be to respond to the email.

Table 1.

Example list of factors subjectively valued for whether to respond to an email depending upon the likelihood of the email being genuine or phishing (States of the world: Genuine or Phishing) where each state has 50% probability of being true. Ratings from 0=least valued, 100=most valued. Below the Table is a demonstration of the expected utility calculation using this data.

Action	**States of the world**	
	Genuine	**Phishing**
Respond	100	0
Not respond	30	50

$$\boldsymbol{EU\ (Action) = \Sigma\ (U(Outcome) \times P(State))}$$

$$\boldsymbol{EU\ (Respond) = 100 \times .5 + 0 \times .5 = 50}$$

$$\boldsymbol{EU\ (Not\ respond) = 30 \times .5 + 50 \times .5 = 40}$$

This process of predicting *rational* decision making for EUT is dependent upon four axioms: *cancellation* (states of the world which give the same outcome regardless of one’s choice or action can be eliminated), *transitivity* (if A is preferred to B, and B is preferred to C, then A is preferred to C), *dominance* (whereby one characteristic is better in A than B, and at least as good in all other respects compared to B, A will always be preferred to B), and *invariance* (preferences of choice should not be dependent upon how the options of decisions are described or presented). If one or more of these axioms are violated, then the decision made is not deemed to be rational by EUT standards. Although, even if none of these axioms are violated - this does not guarantee the decision made is rational; other factors such as time pressure – whereby time to collect evidence to form judgements could be constrained, or at least a belief that time is constrained - may also interfere such as the quality of information which will be covered in more detail later.

However, there have been many examples which demonstrate that using EUT is not always accurate in describing how people should be making decisions, as key principles can be violated. Most notable examples are that of the *Allais paradox* (Allais, 1953) and the *Ellsberg paradox* (Ellsberg, 1961) whereby the axiom of cancellation is violated – i.e., participants would be more likely to avoid uncertainty, even when outcomes for decision options may be the same – a finding which has also been replicated across settings more applicable to the real world – e.g., within healthcare decision-making (Oliver, 2003). The axiom of transitivity has been observed to be violated in contexts in which priorities may shift in what are known as money pump problems (e.g., Ranyard, 1977; Tversky, 1969). When people are presented with a logical series of decision options, they may return to their original choice (e.g., A > B, B > C, but C > A), which in turn could be exploited at a cost to the decision maker (e.g., because of shifting outcome priorities over time). Dominance and invariance as axioms of EU rational decision making have also been shown to be violated in other published research (e.g., Kourouxous & Bauer, 2019; Loomes, 1989).

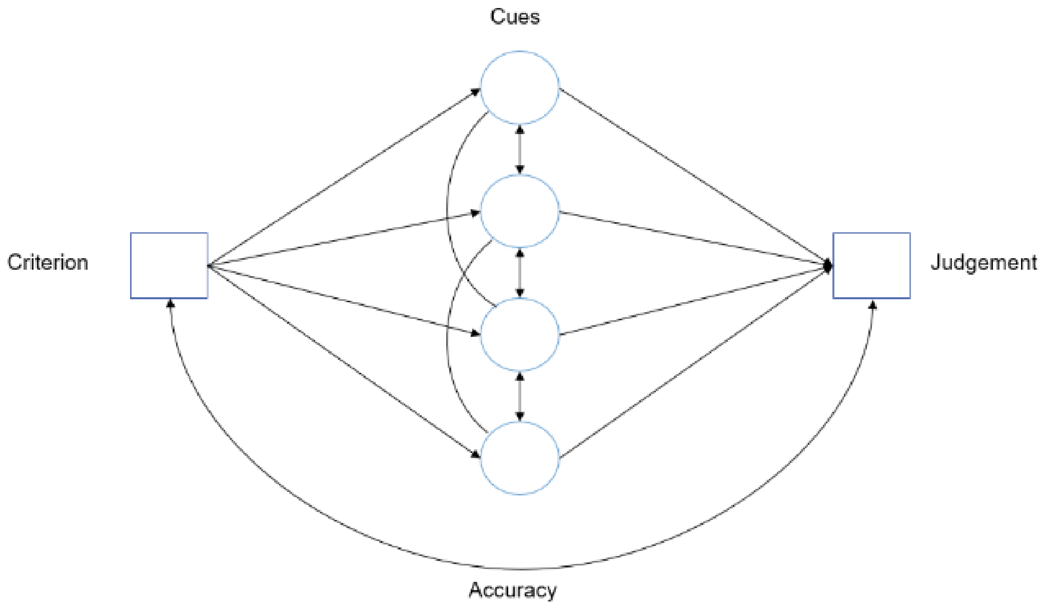
These observed violations of axioms used to indicate the alleged degree of rational decision making highlighted a need to note differences in how people *should* make decisions to optimise their goals based upon normative analysis, how people *ought* to make decisions from an ethical perspective, and how people actually *do* make decisions. Reflecting on this in the context of cyber-security decision making – in the knowledge that over 80-90% of cyber incidents had human factors on the receiving end to threats as a contributing factor (CybSafe, 2020; Verizon, 2022; World Economic Forum, 2022) – we must consider the subjective nature of human decision making as multiple “irrational” elements may be relevant to understanding *actual* decision making. For example: perception of security risk (Van Shaik et al., 2017), security culture and awareness (Parsons et al., 2015), intentional and unintentional maladaptive behaviour (see Figure 3 in Chowdhury et al., 2019), individual vulnerabilities and strengths (Bishop et al., 2020; Raywood-Burke et al., 2021), and contextual pressures (Dykstra & Paul, 2018).

Ultimately, all of these aspects involved with cyber-security decision making are defined by bounded rationality (Simon, 1957). That is, humans have limits (even under the best of circumstances) to their ability for decision making, and often have to rely upon utilising cues obtained through senses to form judgements of the world (Brunswik, 1956 – see Figure 2 below). To conceptualise the cognitive aspect to bounded rationality in judgement formation (and in turn how this may affect subsequent decisions), reflect upon the following example: An individual wants to tell the time. Time passing is simply part of the world we live in which everything travels from the past, through to the present and into the future. However, our perception of time is not always an accurate reflection of reality. Individuals judge reality through the perception of cues which could be used to describe reality. In terms of telling the time, one common way (an environmental cue) in society would be to look at a timepiece such as a clock. The clock would provide the individual with a numerical output which could be used to inform time telling, perhaps to the second; thus, could be a good cue to provide an accurate judgement. But what if the clock was not set to the correct time? What if you had two clocks next to each other presenting different times – which should be believed as accurate? Other cues could also be used such as where the sun/moon is in the sky, being explicitly told about the time by asking someone else, or estimating time taken between landmark perception intervals (e.g., watching a car travel at a fast speed from one point to another to estimate how much time it took for the car to travel between the points, or comparison between a memory earlier in the day vs the present moment).

However, in the example above, the individual is posed with multiple factors which could affect the accuracy of judgement formation of reality. Which cues – all or any – should be used? Which cues are the most reliable? What other cues might be available to inform the judgement? Are some cues more accurate than others? Are other cues being overlooked or is attention to come cues biased vs others? What about the motivation of the individual – to what degree do they want to tell the time and to what level of accuracy (years, months, days, hours, minutes, seconds)? How important is it that the individual gets an accurate representation of the time? Is the individual in a hurry to do something which is time dependant? Are others conveying urgency to the individual? Is the individual doing something physically and/or mentally demanding?

Figure 2.

A conceptualisation of the accuracy of judgement formation adopting Brunswik's lens model framework (1956).



How much information an individual should or does need to use to form a judgement could vary significantly as a result of changing environments and other factors (e.g. pressures – such as workload, deadlines etc.). Other theories and associated research following on from variations of EUT have captured previously overlooked aspects of human decision making –

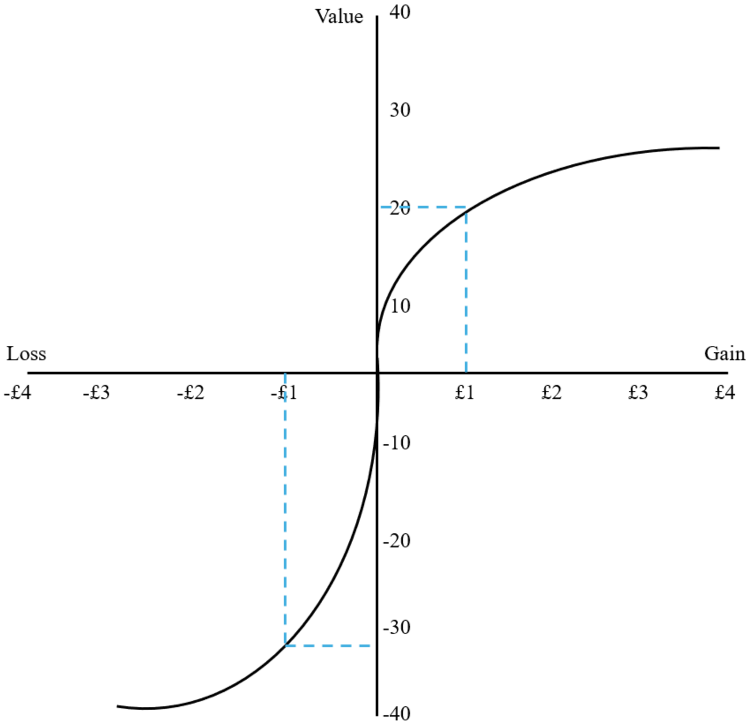
intuition. Humans can, and do, form judgements and make decisions which need not be based upon all information presented to them – even to the extent they are sometimes (perhaps often) based upon very little information over a short period of time (e.g., Ambady & Rosenthal, 1993; Borkenau et al., 2009). Kahneman (2011) describes this intuition as one of two parts of a decision-making mode of thought. This first system of decision making is more heuristic (i.e., based upon mental shortcuts). For example, choosing to reply to an email based upon the first pieces of information encountered – in which judgements and decisions can be made quickly, using less information to inform, but may be more reliant upon the role of emotion and be based upon a less accurate representation of reality. The second system, counter currently, is slower but involves a more deliberative and logical approach which requires more effort to process information, which may in turn be more appropriate for more complex issues.

The determination of which mode of decision making is adopted could vary depending upon the circumstances involving uncertainty, though such factors could promote biases. Tversky and Kahneman (1974) described some biases in judgement which demonstrate that heuristic modes of thinking can be adopted in reality, and how they influence subsequent behaviour. *Representativeness bias*, for example, may occur in instances of making judgements of the probability of an outcome occurring, and involves the comparison of an event with an existing prototype (imagined similar example) which already exists in the mind which can result in inaccurate estimations. An example of this is stereotyping which can result from neglecting base rate information in favour of prototypical preconceptions such as the expectation someone is a writer rather than a construction worker because they like to read books (Turpin et al., 2020). The *availability bias* – when the frequency, or frequent availability, of information is high – can result in judgements being weighted in favour of such information, thus also forming a potentially less accurate judgement of reality. A classic example by Loftus and Palmer (1974) can be seen from manipulating language in leading questions following the observation of an event: and estimations of the real-life event, i.e., the speed of which a car was travelling when it crashed into another can vary significantly. In the case of Loftus and Palmer when participants were asked “about how fast were the cars going when they smashed each other?” (p. 586) the average estimated speed was 39.3mph compared to 31.8mph when the word ‘smashed’ was replaced with the word ‘contacted’. *Anchoring and adjustment* can occur when individuals have an initial judgement but adjust their it in relation to a landmark piece of information – for example in credit-card repayments, if a minimum repayment limit is enforced, people are more likely to pay off less on average (i.e., closer to the limit) from their credit card debt compared to when no limits are enforced (Stewart, 2009).

Kahneman and Tversky (1979) also collectively detailed critiques of EUT as an accurate descriptive model for human behaviour and proposed their alternative model – *Prospect Theory* – which further details a key significant bias influencing decision making: *loss aversion*. Prospect Theory proports the subjective utility of gains from a decision are not equal to the equivalent loss. Furthermore, the subjective utility of loss is significantly greater in proportion than equivalent gains (see Figure 3). As a result of this perception of loss, on average - people may be more likely to avoid risky decision options – as has been demonstrated within a substantial amount of research on the subject (Brown et al., 2021). Brown et al. (2021) conducted a large-scale systematic review of interdisciplinary research and carried out a meta-analysis on 607 empirical estimations of loss aversion from 150 articles. They found the mean loss aversion coefficient is between 1.8 and 2.1; meaning as perceived gains increase by a scale of one, perceived losses for the same amount are approximately doubled.

Figure 3.

Visual adaptation of the asymmetrical shape of subjective utility for gains and loses depicted in Kahneman and Tversky's Prospect Theory (1979). Blue dotted lines indicate relative differences in subjective value for gains versus losses for the same monetary quantity.



Whilst Prospect Theory and subsequent research on loss aversion demonstrate a significant impact of subjective perception of reality influencing risky decision making (noting application to cyber-security contexts where risky decisions often have to be made), there are some critiques of the model's ability to accurately describe human behaviour. First, people do not always have access, or utilise, accurate cues of reality to form decisions, such as when security operation centre (SOC) analysts are trying to determine whether network threat alerts are genuine or false alarms. Consequently, the subjective utility relating to gains and losses could vary greatly depending upon other biases previously touched on (anchoring and adjustment, representativeness bias, availability bias, framing etc.) or from ranking subjective values based upon memory (i.e., Decision by Sampling – DbS - Stewart, Chater, & Brown, 2006). Second, preferences may change over time, and judgements could in turn also depend upon when they are made. For example, a conscientious individual in work may be keen to check they are connecting to a secure network before committing, but when in a rush to submit something before a deadline and perhaps when in a public place may choose to connect to a local Wi-Fi: forgetting to check whether the network they have joined is secure. Subsequently, the impact of cost-benefit analysis could vary depending upon when judgements are formed, when the decision needs/can be made, and when the outcomes may occur.

Decision-making theory development discussed thus far highlights how the quality of information input into decision analysis is as important as the decision analysis system adopted itself in assessing the quality of the decision make. What could, therefore, define what makes a decision good or bad (or anything in between) is not so much the sentiment that is often drawn from Machiavelli's *The Prince* (Machiavelli, 1469-1527/1981) – the end justifies the means – which gives into the misconception previously discussed that outcomes are the key to good decision making (not to mention the insidious ethical implications), but rather that the means justify the end. The quality of a decision could therefore be defined by the suitability of the framework of the decision-making process in the given circumstances, which considers the potential for desirable and undesirable outcomes coming true, combined with the quality of the information available being used. A good decision would thus involve the adoption of the most suited method of decision making in the given circumstances, providing the most desired outcome with the highest potential of coming true, based upon the utilisation of the highest quality information available. It must also be noted, therefore, that it is still possible for good decisions to result in undesirable outcomes – and vice versa – even in the best of conditions. As the majority of people have a tendency to act honestly on average (Jiang et al., 2023), this also applies to the context of cyber-security – whereby most people do not set out to make bad decisions, with malicious intent, but many decisions are susceptible to the conditions under which they are made (e.g., Chowdhury et al. 2019).

With this in mind when confronted with the challenge of bounded rationality, and its associated nuisances, one factor of frequent appearance has a significant impact upon our bounded rationality is that of *cognitive workload*. This is a common influence upon decisions and behaviour across many contexts, including decision making in cyber-security (e.g., Dykstra & Paul, 2018; Giacobe et al., 2013; Nthala & Flechais, 2017; Vance et al., 2014). However, in order to understand the risks workload may pose to cyber-security decision-making contexts, it is necessary to review literature of the phenomenon to evaluate the key mechanisms involved before addressing the following questions: What sources of workload pose significant risks in cyber-security? Does the type of workload differ in impact? Why and how exactly do these sources pose a threat to cyber-safe decision-making? Can the point in time in which workload occurs influence its impact upon decision making? In the next subsection, a review of a broad range of workload factors across multiple settings is presented – with the key aims of highlighting critical findings, evaluating methods used, and noting gaps which would be worth exploring in order to further the theoretical background used to inform fundamental decision-making mechanisms applicable to cyber-security decision-making.

1.3 – On the Significance of Workload in Decision-Making

Workload as a whole can simply be defined as the amount of work an individual has to carry out (Jex, 1998). Having a higher workload is generally believed to lead to a decrease in overall performance and performance quality (e.g., higher occurrence of errors) of a given task(s). Based upon decision-making theory discussed previously, this decrease in performance, decision quality, and occurrence in errors could result from a reduced ability to process information, focus attention, and incur an overreliance upon unreliable information due to the bounds of rationality (Simon, 1957). Although, there are a at least a few key distinctions that need to be made as the concept of workload is comprised of many aspects and moderating influences.

On one hand there are the more physical sources of workload and related biological mechanisms such as, but not limited to: physical effort, stress and stress tolerance, sleep fatigue, as well as some medical conditions which could seriously reduce an individual's ability to manage workload (e.g., chronic fatigue syndrome and exercise – De Becker et al., 2000). Much research to date has evidenced the influence of these physical sources of workload upon task performance – and generally appears to suggest these factors not only influence ability to manage workload but that at least some are interrelated. Physical fatigue and sleep deprivation can lead to degraded performance at cognitive tasks (such as visual target detection and go no/go tasks - Eddy et al., 2015) and slower skill acquisition due to fatigue and sleepiness associated conditions (e.g., Neu et al., 2010). Choi et al. (2018) assessed the relationship between sleep duration and perceived stress from a large sample of workers (n=67,425) across a range of professions from data collected from the 2015 Community Health Survey (CHS) in South Korea. They found those who slept on average for five or fewer hours reported higher perceived stress than those who had slept more - with authors suggesting more sleep than this is required for workers (in particular specialist and office workers pertaining high levels of educational achievement) to better manage stress.

Whilst it could be concluded from this that average sleep length could be related to stress levels, and subsequently hold the potential to influence workload management, it is unclear to what extent sleep could hinder the ability to manage stress as sleep *quality* can be a moderating factor. For example, university students with low self-assessed sleep quality have been found to be almost five times more likely to have higher stress than those with good quality sleep (e.g., Herawati & Gayatri, 2019). Counter currently, the ability to manage stress can influence sleep quality – whereby those with poorer stress management may be more likely to have poorer sleep quality (Linares et al., 2019), and stress management programs which introduce new coping skills can be successful in reducing perceived stress and increase sleep quality (e.g., over a 6-week period - Stachelle et al., 2020). However, the significance of high stress negatively affecting job performance, whilst evidenced, may in turn be moderated by other variables such as motivation and experience (Hunter & Thatcher, 2007).

Given these examples are largely based upon observational data and/or self-report measures, firm and generalisable conclusions on the significance, and causal direction, of sleep mechanisms upon workload management are limited. There is some evidence, however, of interventions involving changing environmental factors which can successfully reduce physical workload as well as reducing mental effort – e.g., introducing robotic surgery methods as an alternative in surgical scenarios can reduce the physical and mental effort required, resulting in fewer errors, and suggesting this reduction in workload could benefit other situational decision-making demands (Moore et al., 2015). It is, therefore, also important to consider mental workload (also referred to as cognitive load – Sweller, 1988) – the other half of the equation which could also influence task performance and decision-making quality.

Early research on mental workload can be traced back to George Armitage Miller’s work assessing information processing capacity and short-term memory. Miller (1956) proposed there was a limit to the ability to recall newly presented information – commonly referred to as the 7 plus or minus items 2 rule. His work suggested the ability to recall information items is relatively independent of the type of item – e.g., digits, letters, syllables, words– though an individual’s ability to recall such items could be increased by “chunking” (i.e., the process of binding pieces of information together into groups). Whilst there is an ongoing debate on what the precise limit threshold in recollection may be (e.g., 4 plus or minus 1 - Cowan, 2001), and how memory models should be conceptualised (e.g., Atkinson & Shiffrin, 1968; Baddeley & Hitch, 1974; Brown, Neath, & Chater, 2007; Cowan, 1988, 1995; Jones & Macken, 2018; Waugh & Norman, 1965), what can be concluded from this research is – in line with Simon’s Bounded Rationality concept (1957) – there is a cognitive limitation to human ability to process and retain information regardless of the circumstances. Therefore, this is a key factor to consider when trying to understand risky decision making in time-pressured cyber-security settings, and how interventions could help support strengths and vulnerabilities. However, what different forms might this cognitive limitation appear in, when might increases in cognitive restrictions occur, and what influence might they have in relation to the quality of judgement formation and decision making? These are all crucial questions.

Evaluating Cognitive Load Theory (CLT), developed by John Sweller (1988) based upon his work on problem solving, and related research which will be discussed later, sheds some light into the possible answers to these questions. Sweller (1988) detailed three different types of cognitive load: *Intrinsic*, *Extraneous*, and *Germane*. Intrinsic cognitive load is where there is an aspect of a task which is innately difficult – e.g., solving the sum 2 + 2 versus solving an algebraic equation to calculate the diameter of a sphere, or having a fixed amount of time in which a task can be completed. Capraro (2017) and Capraro et al. (2019) noted that the hard limitation of time for completing a deception task can increase acts of dishonesty in lab experimental conditions. This has also been evidenced in cyber-security settings to increase engagement with risky decision making – such as the role of time constraints upon maladaptive behaviour engagement highlighted in a systematic review by Chowdhury et al. (2019).

Extraneous cognitive load, on the other hand, is manipulated by contextual factors which can influence perception. Many examples have been detailed in the decision-making literature previously discussed, and especially biases which largely result from manipulations in the presentation and availability of information (e.g., Tversky & Kahneman, 1974). Another example is social influence, which can involve the manipulation of perceived time pressure (i.e., when people are told by others the task they need to complete should be done urgently, or informed there is insufficient time for them to complete the task well) and has been found to result in the increase of risky decision making in well-established paradigms such as the Iowa Gambling Task (DeDonno & Demaree, 2008). This has also been found in employed participants from organisations when controlling for task complexity (e.g., Nordqvist et al., 2004, where the negative effects of perceived time pressure on job satisfaction and goal achievement could be mitigated by team support).

Through these changing circumstantial cognitive loads (intrinsic and extraneous), priorities could shift, subjective utilities for outcomes could change, but also may subsequently influence what information may be sought out to form judgements. Crescenzi, Capra, and Arguello (2014) noted that as perceived time pressure was reported to be higher in participants when there was lower satisfaction in the search process for information in an information searching task set for them. Subsequently, this feeling of satisfaction in information searching strategy could hold the potential to influence the type of decision-making strategy people may employ in a given situation. Furthermore, intrinsic and extraneous cognitive load sources are often found to be related (e.g., stress derived from time perception is strongly related to changes in time constraints in the context of making decisions in line with cyber-security policies – Trang & Nastjuk, 2021), though it is important to consider their independent impacts upon behaviour in order to understand the effect size weightings.

Finally, Sweller et al. (1998) detailed Germane cognitive load – i.e., the proportion of memory devoted to integrating new information, and the creation and modification of a schema (i.e., a cognitive framework used to organise and interpret information). For example, creating a set of instructions for a task can increase this type of cognitive load, but, having created a framework in which to make decisions could reduce the effects of other types of cognitive load (Cierniak, Scheiter, & Gerjets, 2009). The greater the structure of decision-making complexity, the more time and effort is required to pre-plan, but subsequent mental demand may be reduced as a clear procedure may be followed. However, the utility of germane cognitive load management could be greatly affected by levels of uncertainty in a given scenario. Incident management in cyber-security, for example, can involve many instances in which teams of analysts in security operation centres (SOCs), with different teams dedicated to specific stages of incident management, try to identify, contain, eradicate, and learn from cyber threats. Analysts may be provided with a "playbook" which contains protocols, instructions, guidance, and policies to help manage how certain types of cyber threat situations (e.g., Onwubiko & Ouazzane, 2020). Although these playbooks may be updated (even over short periods) and can provide some assistance in managing workloads, analysts still have to deal with high levels of uncertainty and time pressure as a consistent part of their job.

What information could be gathered to inform decisions? What information should be relied upon? What amount of information is considered sufficient enough in making a judgement call? These are but a few questions key to answer when carrying out the job of a SOC analyst - which can be subject to the availability of information (extraneous cognitive load), all under the guise of constant time constraints (intrinsic cognitive load). When might it be suitable to break away from protocol, and adopt a more creative approach, to adapt to the situation as it unfolds is also a key questions which highlights the importance of germane cognitive load management – as the quality of planning, the automation/ritualistic/habitual nature of behaviour, and learning process could influence how accurately cyber incidents are managed.

Metacognition – the reflection upon one’s own thinking processes (Flavell, 1985; Metcalfe & Shimamura, 1994) – involved in the SOC scenario described above also highlights how each type of cognitive load can relate and interact with each other – compounding effects which taken collectively can influence the quality of decision making (of which there are many notable examples of for intelligence analysis failures – e.g., Prague Spring, Pearl Harbour, the Cuban Missile Crisis - Brand, 2019).

From the current discussion of workload – it is clear several factors can contribute to the depletion of cognitive resources and these in isolation or combination may result in maladaptive behaviour – and therefore could be a key reason for errors and the like in human-centred cyber-security. With cognitive load being more relevant to the broader basis of this thesis - decision making and maladaptive behaviour applied to cyber-security - compared to more physical aspects of workload, research within this thesis has been more focused on the cognitive aspects of workload. From establishing that maladaptive behaviour can often result from, but not solely the result of, manipulations in cognitive load, there is a need to explore potential gaps in the mechanisms of the cognitive load theories to understand how it might apply to cyber-security research and practices. Two such areas of concern are dishonesty and insider threat in cyber-security. However, in order to understand precisely how the gaps in research could influence behaviour – research whereby a high level of control can be administered should be adopted first to test the gaps in psychological theory, then use findings to inform more applied research. This approach has been adopted throughout the thesis, with the next section detailing the background of research into the role of cognitive load in dishonest and maladaptive behaviour, and five experiments which have been subsequently carried out with discussion around key findings – and conclusions which can be drawn to inform both further understanding of cognitive load theory and the implications for cyber-security behaviour.

1.4 – Cognitive Load, Dishonesty, and Maladaptive Behaviour

1.4.1 – Study 1 & 2: Background

To a degree, we control voluntarily what our cognitive faculties are used for. Though, as discussed in previous subsections, there are considerable environmental influences which can bias judgement formation and decision-making quality. Human ability for self-control - an internal process of regulating cognition, affect, and behaviour (Baumeister, Heatherson, & Tice, 1994), which can overrule selfish impulses in favour of acceptable behaviour (Baumeister, Muraven, & Tice, 2000; Vohs & Faber, 2007) is subject to these cognitive load factors. In social situations, these metacognitive self-control processes are essential in maintaining an individual's self-concept: the collection of beliefs a person holds about themselves and responses to others (Henrich et al., 2001). Considering threats to cyber-security could come from communication sources between individuals (e.g., emails), and those working in cyber-security contexts may involve considerable interaction within and between groups (e.g., SOC environments in cyber incident management), how self-control could be influenced by cognitive load is key to understanding risks such as insider threat through acts of self-interest and dishonesty.

Insider threats largely represent individuals within organisations whose actions could pose a threat to security due to malicious, non-malicious, misinformed, or uninformed intentions behind maladaptive behaviour. Maladaptive behaviour could therefore be unintended to do harm to oneself or others, but may result in harm consequently, in cases involving individuals are uninformed or misinformed on information security protocols, for example. The same holds true for non-malicious maladaptive behaviour, for example trying to find work arounds to information security policies to save time or for greater convenience (as seen in Trang & Nastjuk, 2021). However, in the case of non-malicious maladaptive behaviour the actor stands to gain on a psychological level through cheating the system to reduce cognitive workload. Malicious actors, on the other hand, may seek either to gain in other means such as seeking financial gains, or actively intend to do harm to others through acts of sabotage. Whilst the consequences and goals may differ between malicious and non-malicious behaviour (i.e., cheating the system for psychological benefits or acts of dishonesty to reward oneself financially), both can be considered maladaptive as the rewards for both can be perceived as benefits for not protecting themselves from cyber-security threats (Rogers & Prentice-Dunn, 1997).

(Dis-)honesty is central to self-concept maintenance and is susceptible to the self-control between internalised societal norms and self-motivation (Mizar, Amir, & Ariely, 2008). Individuals may express honesty to gain trust and develop healthy relationships with others. On the other hand, if the truth is perceived as damaging to one's self-image or may harm a relationship, honesty may not be preferential. Such self-control flexibility has been shown in laboratory-based experiments (Gino, Ayal, & Ariely, 2009; 2013; Hagger et al., 2010). When individuals were given the opportunity to cheat for personal monetary gain instead of being judged and rewarded on their actual performance, they reported more correct answers and chose to pay themselves a higher reward. In contrast, drawing attention to social norms of pro-social behaviour through moral reminders decreased the likelihood of dishonesty (Mazar, Amir, & Ariely, 2008). When rudeness between individuals is observed before a similar task to Mazar et al. (2008), people have also been found to be more likely to cheat potentially due to a depletion of self-control or due to the observed spread of norm-violating behaviour (e.g., Buehner & Townsend, 2015). This is highlighted by broken window theory – i.e., that people may be more likely to engage in breaking with socially acceptable norms when a lack of previous engagement in such norms has been evidenced (Keizer, Lindenberg, & Steg, 2008).

Whilst acts of dishonesty may appear to be adaptive to the environmental conditions when one can get away with it, they may often be maladaptive strategies due to the risk of consequences which could cause harm to the actor - particularly when the ability to get away with cheating is not certain. When participants seemingly acted dishonestly in the matrices task detailed in Buehner and Townsend (2015), it was not certain they would get away with overpaying themselves: they risked possible negative consequences from the experimenter. In the procedure for the experiment, no reaction was planned from the experimenter after payments were provided, but from the participants' perspective it was possible negative consequences could have been enacted (e.g., loss of payment/participation credit). As such, just like the cyber-security example discussed on insider threat, such behaviour from the participants could be deemed as maladaptive as the rewards can be perceived as benefits for not protecting their self-concept.

It has been suggested that cognitive resource depletion impacts self-control, which in turn affects self-concept maintenance – i.e., increasing the likelihood of engaging in dishonesty, highlighting the possibility that self-control and cognitive resources may share a common source. For example, after primed with a cognitive depletion task, Mead et al. (2009) had found people were more likely to cheat on their performance in a matrices task with monetary incentives, if they had such opportunities. Similarly, when self-control resources were depleted, an individual's ability to identify cheating behaviour was inhibited, and greater effort was required to resist cheating due to a greater susceptibility to situational cues has been argued by some researchers with consistent findings over a series of experiments (Banker et al., 2017; Gino et al., 2011; Vohs & Faber, 2007; Wu et al., 2019). Such mechanisms of self-control depletion have also been noted in workplaces (Wehrt, Casper, & Sonnentag, 2022) whereby participants reporting daily measures for organising, meaning-related strategies, and self-reward across a 2-week period were examined in relation to task performance. They found that self-rewarding behaviour counteracted the adverse effects of depletion upon task performance.

It is of concern, however, that some researchers have attempted replications but not found the same results. For example, from a meta-analysis of 19 attempted replications of Experiment 1 from Mazar, Amir and Ariely (2008), Verschuere et al. (2018) did not find the effect reported and interpreted within the original Mazar et al. (2008) ten commandments paper. Kristal et al. (2020) had conducted a replication of an earlier published paper - Shu et al. (2012) - which examined self-control and dishonesty in signing insurance policy documents and concluded signing at the beginning of a document could result in greater honesty compared to signing at the end. Kristal et al. (2020) however, had not been able to replicate the findings. To a degree of irony, the original paper (Shu et al., 2012) has since been retracted as it was alleged the work was based upon fraudulent data (Marcus, 2021; Shu et al., 2012). Two of the leading authors of this area of research – Dan Ariely and Francesca Gino – have also more recently been publicly questioned around the replicability and descriptions of other key works (e.g., Mazar, Amir, & Ariely, 2008) in terms of how the experiments were really carried out (News 13, 2022; Quinn, 2023). Subsequently, there is a need to further develop work behind the psychological concept for self-control and cognitive load to validate the findings from this type of paradigm, and further the previously reported conclusions and potential implications.

In addition to these concerns, previous studies adopting the well-developed matrices paradigm from Mazar, Amir, and Ariely (2008), whereby participants would be asked to complete items involving addition of numbers to two decimal places and are judged upon performance, have only manipulated cognitive resources depletion. For example, through using a Stroop task (a test for inhibitory control where participants need to state the colour of words presented rather than the word itself) or essay writing, prior to the main task (Gino et al., 2011; Mead et al., 2009). However, it is unclear whether depletion of cognitive resources during the main task itself would also elicit dishonest behaviour. To address these highlighted issues, participants in the current Study 1 took part in the matrices task and procedure similar to Mead et al. (2009). However, instead of priming cognitive load, the matrices task itself included two levels of difficulty as a depletion manipulation. Whilst the motivations for self-rewarding behaviour may not be explicit from the matrices paradigm adopted in the examples discussed above (e.g., Mead et al., 2009) – for example, individuals paying themselves more for personal gain, believe they are more deserving due to greater cognitive effort required, or wish to incur a greater cost to the source of reward – the adoption of this experimental procedure (allowing for the ability to control for potentially confounding variables) could provide insight into the psychological mechanisms which underpin the likelihood individuals becoming insider threats to cyber-security. This controlled experimental approach would develop the theoretical basis for which later, more applied research on insider threat causes, could be informed from. With insider threats being a contributing element to cyberbreaches (approximately half – Bailey et al., 2018) largely comprised of malicious self-serving intent or negligence, the matrices paradigm – requiring participants to reward themselves financially on the basis of performance - had the potential to provide insight into the root causes for insider threat; and was particularly relevant as Bailey et al. indicated a significant minority of breaches (approximately 15%) could be motivated by financial stress.

Based on previous findings on the impact of self-control depletion upon subjective reported behaviour, the primary hypothesis across both Study 1 and 2 was that participants were more likely to over-report their performance when the task was difficult, combined with having the opportunity to act dishonestly. As with previous research adopting this paradigm (Gino et al., 2011; Mazar, Amir, and Ariely, 2008; Mead et al., 2009), it was predicted participants would be more likely to overreport performance when not under public judgement compared to when the experimenter would mark their work.

As a secondary note, this work also furthered previous studies by the inclusion of a post-task questionnaire – a composite of the NASA-Task Load Index /TLX (Hart & Staveland, 1988) - to check whether the manipulation of task difficulty and dishonest opportunity affected subjective evaluations of cognitive load (mental demand, effort, performance, and frustration). This manipulation check is key to include as the principle behind the task difficulty manipulation is an increase in intrinsic cognitive load should result in an increased likelihood of engaging in maladaptive decision making (Sweller, 1988). As a result of these changes to the environment, on average participants would alter their judgements to assess what would be the most beneficial decision to make in the given circumstances.

In relation to the hypotheses for these two studies adopting experimental designs on the basis of this theoretical background, participants on average may believe there may be more benefit to overstating performance for difficult tasks which they are not publicly judged for. This increase in self-reported performance could be of benefit to participants, whom at the time likely believe they will receive a greater chance of winning a reward. However, in cyber-security settings, self-preserving/bolstering acts could seemingly benefit the individual in the short term but put others at risk (be it with malicious or non-malicious intent). It was predicted, therefore, that there should be higher ratings for the NASA-TLX ratings for conditions with greater task difficulty, but no differences were expected in these ratings between private versus public judgement conditions as there was no basis for any to be expected. Study 2 was an online replication of the first experiment from Mead et al. (2009) – in order to test whether key findings are consistent and valid. Methods and results for Studies 1 and 2 are described in subsections below, followed by a collective discussion around findings from both.

1.4.2 – Study 1: Methods

Participants

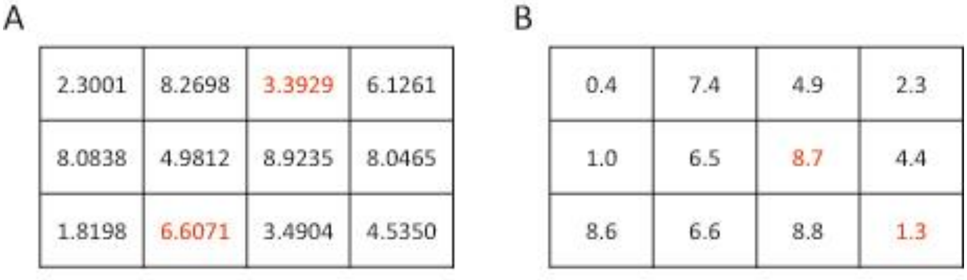
With a minimum sample size of 52 to 128 participants calculated using G*Power (Faul et al., 2007; 2009) on the basis of a medium to large effect size (*f* = 0.25 to 0.4) based upon previous evidence discussed above, and maintaining sufficient power (0.8) to avoid type two statistical errors, one-hundred and twenty-six participants were recruited from the Cardiff University School of Psychology participant panel (mean age = 19.40 years, *SD* = 2.39; age range = 18-40 years; 113 females). Participants had normal or corrected-to-normal vision, had either English as a first language or were proficient in it as a second language, and none reported a history of neurological or psychiatric illness. Participants were rewarded with course credits for participation (equivalent to one credit per 15-minutes), and a raffle ticket per correct answer on the matrices task to win one of two £25 Amazon vouchers. This experiment was approved by the Cardiff University School of Psychology Research Ethics Committee (SREC) with a low risk assessment also approved. Written informed consent was obtained from all participants.

Materials/Apparatus

Participants performed the matrices task adapted from previous studies (Mead et al., 2009). There were 30 matrices - five printed on each of six A4-sized answer sheets. Each 3×4 matrix contained 12 different numbers, and only two of the 12 numbers totalled 10 when added. Participants were required, in each matrix, to identify and circle the two numbers that add up to 10. An instructions cover sheet was provided along with the matrices task informing participants how it should be completed. In the easy conditions, the numbers in all the matrices had one decimal point (Figure 4a). In the difficult conditions, the numbers had four decimal points (Figure 4b). Items after the task were marked as completed or not completed, and of those completed were marked as correct or incorrect.

Figure 4.

Example of a matrix used in the (A) difficult and (B) easy conditions for Study 1, 3, 4 and 5. Correct answers (the two numbers that add up to 10) are highlighted in red.



A

2.3001	8.2698	3.3929	6.1261
8.0838	4.9812	8.9235	8.0465
1.8198	6.6071	3.4904	4.5350

B

0.4	7.4	4.9	2.3
1.0	6.5	8.7	4.4
8.6	6.6	8.8	1.3

To measure if the matrices task inducted any emotional change, all the participants completed the Positive and Negative Affect Schedule (PANAS) questionnaire (Watson, Clark, & Tellagen, 1988) before and after the matrices task. The PANAS includes 20 5-point Likert scales measuring the extent participants experienced various positive and negative feelings and emotions (1= Very slightly/not at all, 5= Extremely). After the matrices task, participants also completed a composite of the NASA Task Load Index (NASA-TLX) (Hart and Staveland, 1988, see also Appendix A), which consisted of four 7-point Likert scales measuring mental demand, subjective performance, effort, and frustration (1= Not at all, 7= Extremely). Items on physical and time demand from the NASA-TLX were not included as they were not deemed to be relevant to this experiment.

Design and Procedure

The study adopted a four-group, 2x2 randomised between-participants design with two independent variables: (1) task difficulty (easy: matrices with one decimal digits; difficult: matrices with four decimal digits), and (2) reporting routine (experimenter-marked and unmarked – i.e., the matrices task after completion was either handed back to the experimenter to be marked or was thrown away into a recycling bin). Participants were not made aware of the group assignment until the debrief at the end of the experiment.

Participants were randomly assigned to groups, ensuring close to equal distributions across conditions, to one of the four groups: Unmarked Difficult (*N* = 32), Marked Difficult (*N* = 33), Unmarked Easy (*N* = 32), and Marked Easy (*N* = 29). Each experiment session included 2-8 participants from the same group spaced out within a sizable cognitive psychology laboratory to allow for the belief in conditions which involved throwing away the matrices task actual performance cannot be traced. After completing consent forms and the pre-task PANAS, participants were given examples of matrices and were instructed the rules of the matrices task, the five-minutes time limit to complete all items, and that they would win a raffle ticket for a £25 Amazon Voucher per correct answer. The short time limit of five minutes was chosen according to a pilot study and in accordance to the previous time constraint adopted in previous literature (i.e., Mead et al., 2009). It ensured that most participants were unlikely to correctly complete all the 30 matrices before the deadline for both the easy and hard variations.

In the experimenter-marked groups, and after the 5-minutes time limit, participants first handed their answer sheets to the experimenter to be marked and then were given a paper slip to report how many correct answers they had. In the unmarked groups, participants were instructed to throw away their answer sheets into a recycling bin, after which they were given a paper slip to report how many they thought were correct. Importantly, in unmarked conditions participants were told that the answer sheets did not contain their personal identities. However, until the debrief, the participants were not aware that the numbers in the example matrix on the instruction coversheet could be used to match their subjective reports and actual performance. In the unmarked groups, the combination of anonymity, group testing, and throwing away answer sheets would give the impression that actual performance would not be marked by the experimenter, and the payment of raffle tickets would depend on subjective reports - implied from the instructions provided at the start of the experiment. As a result, it was expected that the unmarked groups would exhibit an increase in dishonest cheating behaviour, i.e., reporting more correct answers than their actual performance.

After the matrices task, participants completed the post-task PANAS and the NASA-TLX questionnaires. The latter served as a manipulation check for the self-control resource depletion, and we expected that the difficult task led to higher cognitive depletion levels than the easy one. At the end of the experiment, all participants were fully debriefed – including with information about the experimental aims and conditions.

1.4.3 – Study 1: Results

One-sample Kolmogorov-Smirnov tests of normality revealed pre- and post-PANAS scores were normally distributed, thus comparisons were analysed using Analysis of Variance tests (ANOVAs). However, tests of normality revealed scores of performance accuracy ($D(126) = .311$, $p < .001$), the number of correct answers ($D(126) = .096$, $p = .006$), number of answers reported to be correct ($D(125) = .1$, $p = .004$), and the difference between objectively correct vs reported correct ($D(125) = .197$, $p < .001$) were found to be not normally distributed; thus differences were analysed using Kruskal-Wallis and Mann-Whitney U tests.

Objective Performance and Number of Correct Answers

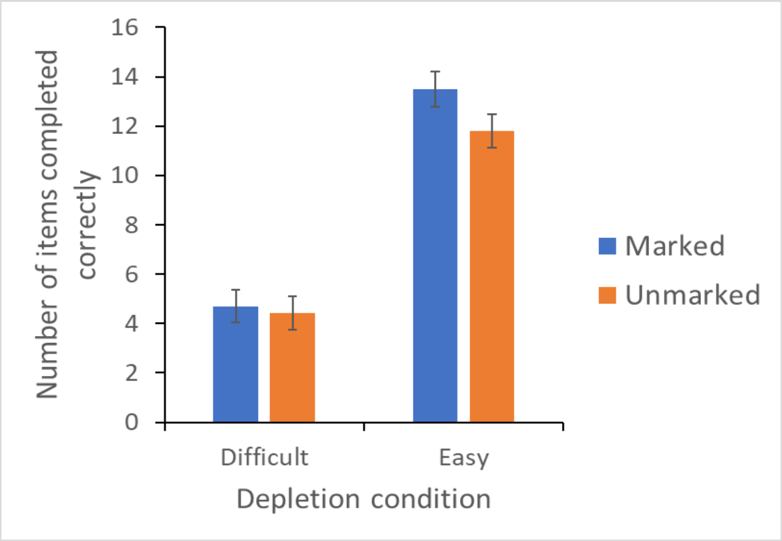
From the number of items completed correctly (Figure 5a) compared with the total number of items completed, the proportion of correct answers for each condition was calculated - to indicate objective performance (Figure 5b). Kruskal-Wallis tests revealed there were significant differences between conditions for both the number of correctly completed items ($H(3) = 72.01$, $p < .001$), and for proportion of items answered correctly ($H(3) = 32.078$, $p <$

.001). From Mann-Whitney U tests there were no significant differences between unmarked and marked difficult groups for total correct answers (*U* = 514, *p* = .853) and proportion of correct answers (*U* = 508.5, *p* = .792). Significantly and proportionately more items were answered correctly for the easy marked group compared to the difficult marked group (Total correct: *U* = 42, *p* < .001; Proportion correct: *U* = 188.5, *p* < .001), more in the easy unmarked group than the difficult marked group (Total correct: *U* = 114, *p* < .001; Proportion correct: *U* = 301.5, *p* = .001), higher in the easy marked group than the difficult unmarked group (Total correct: *U* = 24, *p* <.001; Proportion correct: *U* = 200, *p* <.001), and more in the easy unmarked group than the difficult unmarked group (Total correct: *U* = 84.5, *p* <.001; Proportion correct: *U* = 309, *p* = .003). There were no significant differences between the total correct items for easy marked and unmarked groups (*U* = 359, *p* = .128), though it was found there were proportionately more items answered correctly in the easy marked group than the easy unmarked group (*U* = 324, *p* = .004).

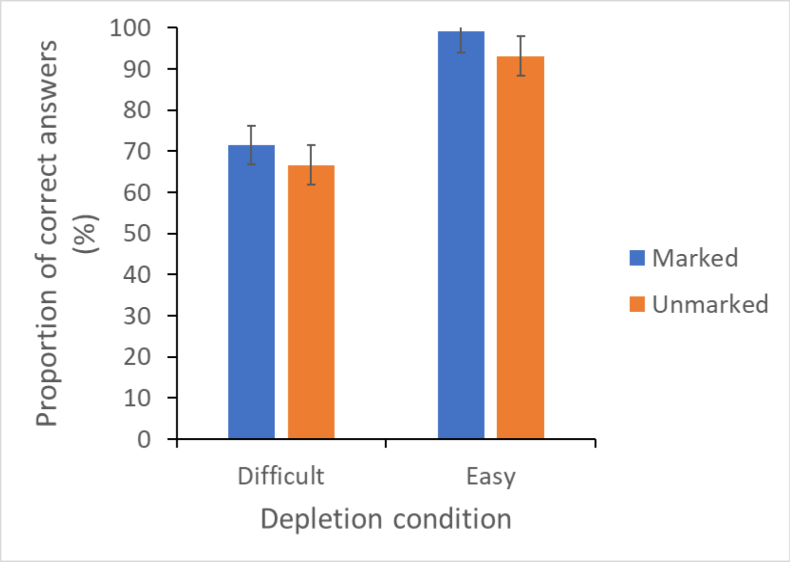
Figure 5.

Mean number of correct answers (a, top), and mean proportion of correct answers (b, bottom) in each group at different levels of task difficulty (difficult and easy) and reporting condition (marked and unmarked) in Study 1. Error bars represent standard errors.

a)



b)



Subjectively Reported Task Performance

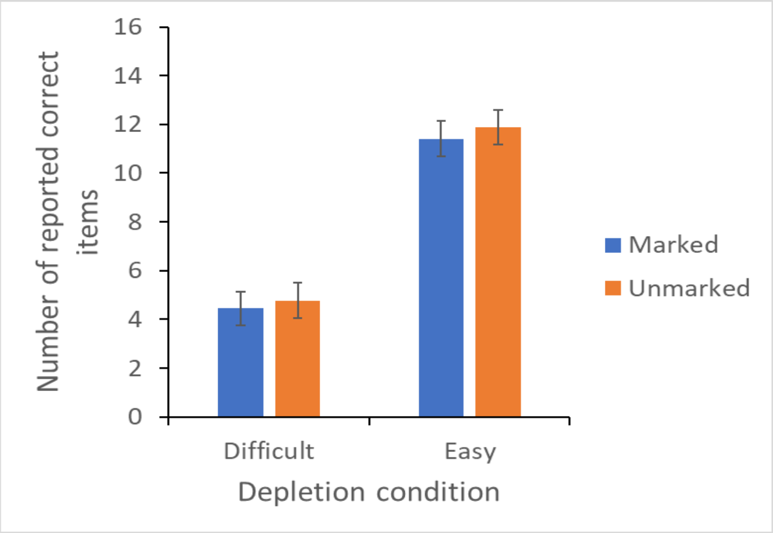
As illustrated in Figure 6a, significant differences were found across conditions for the number of answers reported to be correct by participants (*H*(3) = 60.937, *p* < .001). Mann Whitney U tests indicate there were no significant differences in the number of items reported to be correct between either difficult groups (*U* = 464, *p* = .521) or easy groups (*U* = 453.5, *p* = .879), but significantly more items were reported to be correct in easy unmarked and marked groups compared to difficult marked and unmarked groups (easy marked vs difficult marked: *U* = 78.5, *p* < .001; Easy unmarked vs difficult marked: *U* = 121, *p* < .001; Easy marked vs difficult unmarked: *U* = 67.5, *p* < .001; Easy unmarked vs difficult unmarked: *U* = 110, *p* <.001).

When examining for differences between objectively correct and reported correct answers (Figure 6b) – significant differences were found between conditions (*H*(3) = 17.507, *p* < .001). Mann Whitney U tests revealed that on average participants in the easy marked group were significantly more likely to underreport their performance compared to those in the difficult marked (*U* = 289, *p* = .007), difficult unmarked (*U* = 201, *p* <.001), and easy unmarked groups (*U* = 257, *p* = .002). However, no significant differences were found between other groups.

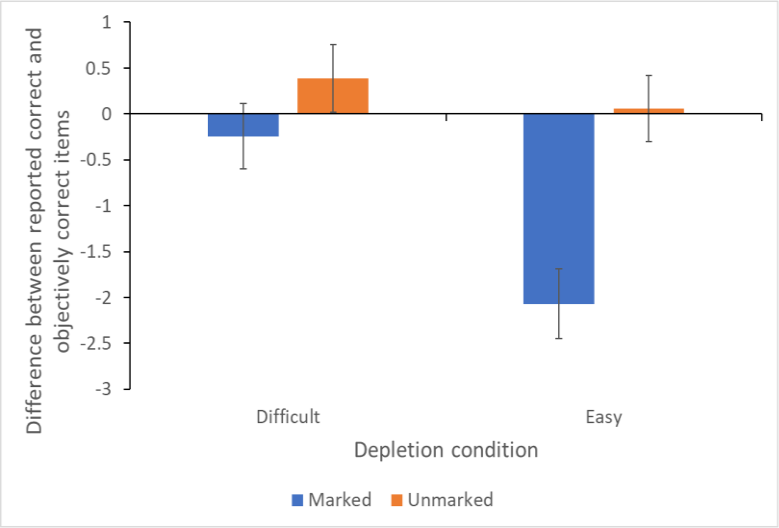
Figure 6.

Average number of subjective-reported correct answers (a, top) and the mean response bias (b, bottom) in each group at different levels of task difficulty and reporting routine in Study 1. Error bars represent standard errors.

a)



b)



PANAS and NASA-TLX

Comparisons were made for the scores of NASA-TLX questionnaires (Appendix A) between groups. Compared with the easy groups, the difficult group had significantly higher mental demand (U = 778.5, p < .001) and lower subjective performance (U = 2573, p < 0.001), together with higher effort (U = 1233, p < 0.01) and frustration (U = 1275.5, p < 0.05). Regarding the reporting routines, no significant difference was found for all ratings (mental demand: U = 1642, p = .598; subjective performance: U = 1932, p = .279; effort: U = 1766.5, p = .864; frustration: U = 1858, p = .501) – thus indicating cognitive load was significantly higher when task difficulty was increased but was not significantly different based upon private versus public judgement.

PANAS ratings between all groups recorded prior to the main phase of experiment were compared. There was no significant interaction (F(1, 118) = .741, p = .391) or main effects for task difficulty (F(1, 118) = 2.875, p = .093) and reporting routine (F(1, 118)= .169, p = .682). Prior mood could therefore be ruled out as a potential confound.

1.4.4 – Study 2: Method

Study 2 was an attempt to replicate experiment 1 from Mead et al. (2009) and served a few other key purposes. First, considering the mixed findings from previous research examining the relationship between dishonesty and cognitive load (including the findings from Study 1 which are discussed later in this chapter), there was a need to evaluate the validity and reliability of this paradigm. Second, as the majority of previous research using this paradigm had utilised university students as participants, this poses a potential problem with the generalisability of findings of such research to a more representative sample of the population – a key consideration with the need to understand how consistent cognitive load mechanisms are across different populations and different settings. Although the COVID-19 pandemic restrictions at the time limited the ability to prioritise the recruitment of in-person participants for studies, there was still the option to recruit from online platforms such as Prolific (2022) whereby participants from the general population could be paid to participate in online research. Therefore, an online adaptation of the first experiment from Mead et al. (2009) was developed with the aim of replicating their findings collecting data from participants via Prolific in December 2022.

Participants

A UK representative sample of 290 participants were recruited via the Prolific (2022) online marketing tool. Of these, 46 were excluded from analysis due to missing/incomplete data and another due to invalid responses. Two-hundred and thirty-five full datasets were therefore included in the analysis, consisting of 121 males, 113 women, and one person who preferred not to say. This was above the minimum sample size (52 to 128) detailed from G*Power (Faul et al., 2007; 2009) calculations for a medium to large expected effect size with a power of 0.8. Ages ranging from 18-76 (*M* = 43.48, *SD* = 15.06), with 80.9% having obtained at least A-levels or equivalent UK qualifications and 67.6% having obtained at least an undergraduate degree or equivalent educational qualification. All participants were highly proficient in English language with it either being their first language or fluent as a second language. They had normal/corrected-to-normal vision and completed the survey on either a laptop or desktop computer. Participants were randomly assigned to one of four conditions upon signing up (low load – marked = 61; high load – marked = 61; low load – unmarked = 59; high load – unmarked = 54). Informed consent was obtained from all participants and upon completion they were fully debriefed and compensated £2.50 for participation and an additional bonus payment of £2 as part of the study reward incentive detailed in the procedure. This experiment was approved by Cardiff University School of Psychology Research Ethics Committee (CU-SREC).

Materials/Apparatus

The first aspect of the experiment was created online using *Qualtrics©* which consisted of a series of basic demographic questions to collected data on gender, age, and highest level of education. The following sections after instructions consisted of the PANAS questionnaire (Watson, Clark, & Tellagen, 1988) as used in Study 1, followed by instructions for a section requiring participants to write a short essay – in 5-minutes – on what they had done the day before. Qualtrics prevented participants from moving onto the next section whilst encouraged to write the essay until the five minutes were up with no option to progress. Upon 5-minutes passing, a button would become available to move onto the next section of the study. The following section consisted of a link to a program created in *Pavlovia* which replicated the matrix paradigm with 20 matrix items in total presented in a randomised order from Mead et al. (2009) experiment 1. Matrix items were presented one at a time, and participants had to click on which two numbers they thought matched to move onto the next item. There was a five-minute limit to complete as many items as possible within this limit, then after five minutes had passed, or if all items were completed within five minutes, participants were presented with a question of what should be done with their data and either a button labelled "delete" or "save" depending upon their condition. Regardless of condition, pressing the button would move participants onto the next section and data was saved (i.e., never deleted). Following this, returning to Qualtrics, participants would be asked to report how many matrices items they had completed correctly, and the composite of the NASA-TLX used in Study 1 before being presented with the debrief.

Design and Procedure

The 2x2 between-participants experimental design adhered as closely as possible to replicating the procedures of Study 1 from Mead et al. (2009) with minor changes to adapt the design for online deployment. Upon signing up, participants were provided with a Qualtrics link to the study. Following informed consent to take part, completing demographic details and provided ratings on the PANAS, participants were instructed to reflect on what they had done the previous day and write an essay within five minutes but only using words which did not include the letters X or Z (low cognitive load priming condition) or the letters A or N (high cognitive load priming). Participants were prevented from moving on until they had attempted the essay task to the best of their ability, then after five minutes they would be presented with a button to move on. Compliance rates (number of participants who adhered to the high or low load priming condition) calculated after data collection indicated approximately 75% of participants in the low load conditions complied with not including the letters “X” or “Z”, however only approximately 26% of participants in the high load conditions complied with not including “A” or “N”. It is worth noting nearly all instances of non-compliance involved only one instance of non-compliance, and the mean character count for the low load condition essays was 675.6 and 185.6 for the high load conditions. All participants would then be redirected to a Pavlovia link whereby all participants would complete the same matrices task as in Mead et al. (2009). This would consist of 20 items for which participants were informed to complete as many as possible within five minutes, and that for they would be rewarded with £0.10 per item completed correctly (max £2.00).

Upon completing all items, or after five-minutes passing (whichever came first), participants were then informed whether they would like to save or delete the data from the matrices task they had just completed. For some participants, the only option was to save the data (experimenter marked condition) and others only had the option to click the delete button (unmarked condition) – unknown to participants regardless of saving condition data was always saved. Following this, participants were instructed to return to the Qualtrics survey and report how many items they had answered correctly. Finally, participants were asked to complete a composite NASA-TLX adopted as a cognitive load manipulation check as utilised in Study 1 in this thesis. At the end of the study, all participants were fully debriefed about the procedure of the experiment and were informed that regardless of actual performance all participants would be paid the maximum bonus of £2 in addition to their payment for participating.

1.4.5 – Study 2: Results

One-sample Kolmogorov-Smirnov tests of normality revealed PANAS scores were normally distributed, thus comparisons were analysed using an ANOVA. However, tests of normality revealed scores of performance accuracy (*D*(235) = .291, *p* < .001), the number of correct answers (*D*(235) = .094, *p* = < .001), number of answers reported to be correct (*D*(235) = .139, *p* < .001), and the difference between objectively correct vs reported correct (*D*(235) = .189, *p* < .001) were found to be not normally distributed; thus differences were analysed using Kruskal-Wallis and Mann-Whitney U tests where appropriate.

Objective Performance

No significant differences were found between the percentage of items correctly completed (Table 2a – *H*(3) = .891, *p* = .828) or for the number of total correct items (Table 2b – *H*(3) = .354, *p* = .950) between all conditions.

Table 2.

Means and standard deviations for the percentage of items correctly completed (a, top) and the number of items correctly completed (b, bottom) across all conditions in Study 2.

a)

Condition (*N*)	Mean (%)	Standard Deviation
Low load – Marked (61)	86.54	23.32
Low load – Unmarked (59)	84.39	27.86
High load – Marked (61)	91.37	16.93
High Load – Unmarked (54)	88.26	20.27

b)

Condition (*N*)	Mean (out of 20)	Standard Deviation
Low load – Marked (61)	8.05	4.25
Low load – Unmarked (59)	7.58	4.13
High load – Marked (61)	7.93	3.43
High Load – Unmarked (54)	7.61	3.38

Subjectively Reported Task Performance

No significant differences were found between conditions for the number of items reported to be correct (Table 3 – $H(3) = .272$, $p = .965$) or for the mean difference between objectively correct and self-reported correct items (Figure 7 – $H(3) = .479$, $p = .923$).

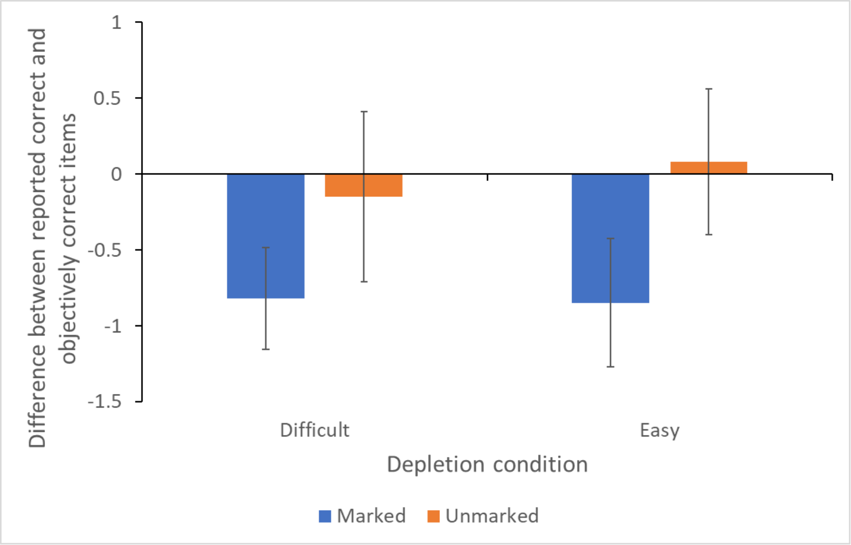
Table 3.

Means and standard deviations for the number of items reported to be correct in Study 2.

Condition (*N*)	Mean (out of 20)	Standard Deviation
Low load – Marked (61)	7.20	3.89
Low load – Unmarked (59)	7.66	4.40
High load – Marked (61)	7.11	3.47
High Load – Unmarked (54)	7.46	4.32

Figure 7.

Average difference in objective correct and self-reported correct items in each group at different levels of task difficulty and reporting routine in Study 2. Error bars represent standard errors.



PANAS and NASA-TLX

Comparisons were made for the scores of NASA-TLX questionnaires (Appendix A) between groups as a manipulation check for cognitive load. However, Mann Whitney U tests revealed no significant differences in ratings for mental demand, perceived performance, mental effort, or frustration between conditions for both the cognitive load and reporting routine manipulations. Therefore, this would suggest that differences in intrinsic cognitive load (Sweller, 1988) was not successfully achieved through the manipulations employed within this experiment.

To test the possibility of prior participant mood as a confound, PANAS ratings between all groups recorded prior to the experiment were compared, with no significant interaction found (*F*(1, 235) = .241, *p* = .624) or main effect for reporting routine (*F*(1, 235) = .863, *p* = .354). However, there were significantly higher mood ratings for low cognitive load conditions than high load conditions (*F*(1, 235)= 6.924, *p* = .009). Prior mood could therefore not be ruled out as a potential confound for comparisons between cognitive load conditions. However, given the pattern of results described in the above sub-sections it is unclear how mood has significantly impacted results.

1.4.6 – Studies 1 & 2: Discussion

The overarching aims of these first two studies were to examine whether the timing of cognitive load (i.e., the point at which cognitive load is induced in a chain of decisions) has any impact upon maladaptive behaviour. Is the likelihood of acting dishonestly when given the opportunity to do so consistent when the source of cognitive load is the main task compared to previous research examining priming tasks (e.g., Gino et al., 2011; Mead et al. 2009)? Study 1 evaluated the likelihood of maladaptive behaviour when the main task was the manipulated source of cognitive load, whereas Study 2 was a replication of the design from Mead et al. (2009) Study 1 which adopted a priming source of cognitive load (essay writing difficulty) using an online data collection method carried out to evaluate the reliability and validity of previous research findings. Understanding the underlying mechanics of cognitive load through controlled manipulation was key to determine what should be the aspect of focus for examining it in the context of cyber-security decision making – in subsequent experiments. If, like some of the previous research discussed (Gino et al., 2011; Mead et al. 2009), cognitive load sources had a tendency to increase the likelihood of engaging in risky, maladaptive, behaviour – then this would provide the foundation for exploring this phenomenon in applied cyber-security settings. If there were nuances found – e.g., effects from specific sources of cognitive load, when cognitive load occurred, public vs private judgement on reward seeking behaviour – then this would be the direction of the next steps to examine forms of insider threat.

Across both studies, it was hypothesised that participants would be significantly more likely to overreport their performance at the matrices task when under higher intrinsic cognitive load conditions, when it was perceived that actual performance would not be judged by the researcher. However, in Study 1 this was not found. As expected, the groups which completed the difficult task achieved lower accuracy and subjectively reported lower numbers of correct answers. The difference in NASA-TLX ratings between the easy and difficult groups further confirmed the effectiveness of difficulty manipulation in inducing cognitive load (Sweller, 1988; Thompson et al., 2014). In contrast to the hypothesis, participants in the difficult, unmarked group were not prone to subjectively report more completed answers than the other groups. Furthermore, participants in the condition where there was low cognitive load but where the researcher was marking performance, significant underreporting of performance was found despite the monetary incentive. In Study 2, the original findings from Mead et al. (2009) were not replicated - with no significant differences being found for subjective reporting between all groups (i.e., the average difference between actually correct items and self-reported correct items – Figure 7), suggesting cognitive load was not successfully manipulated when examining the NASA-TLX manipulation checks.

When participants were primed with cognitive depletion *prior to* the matrices task, they reported more completed items and paid themselves more if the reporting routine gives them an opportunity to do so, i.e., in the unmarked condition (Gino et al., 2011; Mead et al., 2009). The first experiment (Study 1) furthers previous findings on the relationship between cognitive depletion and dishonesty in a few ways. First, instead of using a primer task, resource depletion in the current study originated from the matrices task itself, in the form of task difficulty. This within participant manipulation resulted in a trend of more reported correct answer regardless of reporting routines (Figure 6a). Therefore, cognitive resource depletion prior to the main task, a procedure used in previous studies (Gino et al., 2011; Mead et al., 2009), seems necessary to induce over-reporting of performance specific to the unmarked condition. From examining the consistency of effect for the timing of cognitive load in decision chains we would have a greater understanding of the mechanisms of different sources of cognitive load. Second, to further validate the manipulation of cognitive load a composite of the most relevant items from the NASA-TLX was included to capture self-reported cognitive load (Appendix A) - with results indicating higher cognitive load was found in difficult task conditions (consistent with the differences found in actual performance between easy and difficult groups – Figure 5b). Third, both the participants' actual performance (Figures 5a and 5b) and their subjective reports (Figure 6a) were recorded, which allowed to quantify if the participants over- or under-estimated their objective performance (Figure 6b) for all conditions; whereas in Mead et al. (2009) comparisons were made between experimenter marked actual performance and participant self-reported performance for the dishonest conditions.

However, when examining the key findings from Study 1 – average differences between actual and self-reported performance between conditions – it was found the no significant overreporting of performance, and instead that participants underreported when under low cognitive load conditions, but only when they were under public scrutiny. This stands in contrast to what has been previously found not just in research adopting this matrices paradigm (Mead et al., 2009; Gino et al., 2011), but for other paradigms examining the burdening impact of cognitive load upon decision making (Banker et al., 2017; Vohs & Faber, 2007; Wu et al., 2019) which in the case of Wehrt, Casper, and Sonnentag (2022) even go to explaining the extent to which self-rewarding behaviour could occur is to counteract the impact of high cognitive load. This previous research would suggest cognitive load is still a high influential factor in decision making, but the results from Study 1 in this thesis and previous replications of research adopting the matrices task paradigm (e.g., Verschuere et al., 2018) could indicate replication issues lie with this specific design. Consequently, little can be concluded from the findings of Study 1 in relation to implications for psychological mechanisms which may increase insider threat in cyber-security.

Results from Study 2, which replicated the first experimental procedure from Mead et al. (2009), at a first glance could also suggest the fault of replication may also lie with the design – although in the case of Study 2, there is a likely specific reason for this lack of replication. In Study 2, analysis of the manipulation check data for cognitive load – a composite of the NASA-TLX (Appendix A) – indicated that cognitive load was not successfully manipulated as no significant differences in self-reported cognitive load were found. Despite essays being longer on average for low load conditions than high load conditions, there was also much lower compliance with essay rules for the high load condition than the low load conditions. This particular finding suggests the specific limitation for replication could be due to the manipulation of essay writing difficulty (originally utilised in Schmeichel, 2007) was not a reliable primer for cognitive load, and this could be why replication of findings was not found. Although, in Study 1, significant differences in NASA-TLX ratings were found between cognitive load conditions – indicating cognitive load was successfully manipulated through altering the difficult of the matrices task itself. However, despite this, Study 1 did not find overreporting in the difficult-unmarked condition as predicted; indicating other factors of the design could well be reasons for a lack of replicability. Humans have the tendency to overestimate their performance in difficult tasks and underestimate their performance in easy ones (Grieco & Hogarth, 2009), which is partially consistent with present results – thus could provide some explanation as to why this pattern of reporting behaviour was found.

A possible reason why participants underreported in the easy-marked condition in the first study, unlike the easy-unmarked condition, could be the impact of public scrutiny in which confidence in the participants' own ability is influenced (Swol & Sniezek, 2005; Van Swol, Braun, & Acosta Lewis, 2015). In other words, if an individual is completing a task which they believe to be easy, but their performance is being judged by others, that individual may overcompensate but underreporting performance to not come across as arrogant or overconfident in their ability. In the experimenter-marked groups, success and failure were open to scrutiny whereas in the unmarked groups, the behavioural performance was private to each individual. How humans evaluate themselves vary depending upon the likelihood of failure in public compared to private (Brown & Gallagher, 1992; Greenberg & Pyszczynski, 1985; Sedikides, Campbell, Reeder, & Elliot, 1998). Here, when participants became aware of their performance to be assessed by the experimenter, they are likely to have employed a defence strategy (i.e., underestimation) against the loss of self-esteem (Heatherton & Ambady, 1993; Regan, Gosselink, Hubsch, & Ulsh, 1975). With greater confidence in one's own ability and self-efficacy being correlated with higher interest in cyber-security and cyber-security job satisfaction (Wee, Bashir, & Memon, 2016), understanding how confidence and self-efficacy could be impacted by public judgement and other noteworthy factors is important to know how to better reduce insider threats if this were considerable causes to maladaptive behaviour. Consequently, this warranted further investigation into examining public judgement in combination with other possible factors discussed below.

Unlike Grieco and Hogarth (2009) overestimating performance in difficult tasks was not observed in the present study. There could be at least a few explanations to this which were worth investigating further. First, there could be an issue with the believability of the public versus private judgement manipulation. In some previous examples (Gino et al., 2011; Mead et al. 2009), participants would be told to either pass their matrices sheets to the experimenter for marking or to tear up and throw away in a bin. In practice, testing psychology undergraduate students with this design may be suspicious as to whether actual performance would be retained in reality – they may be inclined to expect something other than that in the instructions to occur. The use of a shredder instead of ripping up matrices tasks has been adopted in other adaptations (Buehner & Townsend, 2015; Gino et al., 2009; Gino, Ayal, & Ariely, 2013) and has been found to be an effective adaptation to elicit maladaptive behaviour. A variation has also been detailed in Ariely (2012) whereby instead of throwing away or actually shredding matrices tasks they would be put into a modified shredder (in which participants would believe it was shredded but actually it was still intact): however, no peer-reviewed publications appear to contain this methodology thus the reliability of such a method cannot be clearly justified without replication. Second, the reward mechanics in Study 1 differ to some extent from previous literature using the matrices paradigm. In Gino et al. (2011), Mizar et al. (2008) and Mead et al. (2009) for example, participants would be told they would be paid a small amount per item correctly completed upon the matrices task completion; whereas in the current Study 1, participants were told that for each item correctly completed they would win a raffle ticket to a drawing of a £25 amazon voucher (the more raffle tickets won, the increased likelihood they had of winning). By introducing a delayed reward which was based upon probability could mean the perception of reward utility differed significantly compared to the conditions from previous literature. It is worth noting previous research suggests there could be small, but notable, sex differences in dishonesty – with men being more likely to act dishonestly compared to women (Kennedy & Kray, 2022). Though while a female dominant participant sample was obtained in Study 1 (due to student sample recruited from), this imbalance was controlled for in later studies.

Ariely (2012) detailed variations of this paradigm in which token would be won instead of money, which could be exchanged for money at the end of the study and claimed to find the same result as in his other work – thus suggests the fact rewards in the case of Study 1 of this thesis were not immediate cash rewards should not significantly influence findings. Increasing perceived monetary value of rewards has also been found not to significantly increase acts of dishonesty (Williams et al., 2016), therefore monetary differences in reward in the present studies versus previous research should not act as a confound. There still remains the issue of probability of reward vs guaranteed reward – thus this was a point to address. Although it was not expected for the actual task performance to be dependent on the method of rewards, it is possible that participants would have a different response strategy for their subjective performance evaluation due to delay (Bickel, Odum, & Madden, 1999; Odum, 2011) and probability discounting (Shead & Hodgins, 2009). Third, a key confounding variable which might influence the impact of public perceptions could be another source of cognitive load – *time perception*. Gino and Mogilner (2014) manipulated prior awareness of time before completing the matrices paradigm and found such priming reduced the likelihood of acting dishonestly. Suggesting that time perception was a key factor warranted further investigation as time pressure can contribute to the perceived effectiveness of cyber-security measures for secure behaviour (Chowdhury, Adam, & Teubner, 2023). If increased salience of time passing, as manipulated in Gino and Mogilner (2014), reduced the likelihood of acts of dishonesty – this could imply time salience could be a successful nudge to reduce non-malicious insider threat behaviour. With little research to date exploring this possibility, time salience was considered as an additional factor to the matrices paradigm to explore the possible psychological mechanism to reduce dishonesty.

From the discussion of these initial two studies (1 and 2) – and highlighting the key reasons and limitations for the findings – further investigations were warranted to address three main points: Does the type of reward, cognitive load, and public/private judgement manipulation impact the likelihood of engagement in self-rewarding behaviour? Three variations of experiments were therefore designed to address this question. Study 3 replicated Study 1 in-person with the addition of the presence of a timer during the matrix task to address the potential confound of time perception. Studies 4 and 5 were online adaptations for Studies 1 and 3 in which an alternative method was adopted for the public/private judgement manipulation and included immediate monetary rewards similar to Mead et al. (2009) to address the concerns of reward type and method believability.

On the assumption that reward type and believability could be controlled for, it was predicted in line with previous literature previous discussed (e.g., Mead et al., 2009) participants would be more likely to overreport performance at the matrix task when not under public scrutiny across all experiments. For Studies 3 and 5 in which a timer was present, it was predicted that the higher self-rewarding behaviour in the high load/unmarked condition would be reduced compared to Studies 1 and 4 where no timer was present. From increasing the salience of time significance in decision making, this should reduce the likelihood of engaging in dishonest cheating behaviour (Gino & Mogilner, 2014).

1.5 – Time Awareness and Dishonesty

1.5.1 – Studies 3, 4, & 5: Methods

Participants

Study 3 - 120 participants were recruited from the Cardiff University School of Psychology participant panel (mean age = 19.58 years, *SD* = 1.48; age range = 18-27 years; 98 females) – within the range of the minimum sample size (52 to 128) detailed from G*Power (Faul et al., 2007; 2009) calculations for a medium to large expected effect size with a power of 0.8. Participants had normal or corrected-to-normal vision, and none reported a history of neurological or psychiatric illness. Participants were randomly assigned to one of four conditions upon signing up – with a near-equal distribution across all conditions (low load – marked = 31; high load – marked = 30; low load – unmarked = 30; high load – unmarked = 29). Participants took part in the experiment in-person, were rewarded with course credits for participation (one per 15-minutes), and a raffle ticket per correct answer on the matrices task to win one of two £25 Amazon vouchers.

Study 4 - A UK representative sample of 290 participants were recruited via Prolific (2022) online marketing tool. Of these, forty-two were excluded from analysis due to missing/incomplete data and another three was excluded due to invalid responses. Two-hundred and forty-five full datasets were therefore included in the analysis, consisting of 126 males (118 women, one prefer not to say), ages ranging from 19-77 (*M* = 44.04, *SD* = 15.236), with 93.5% having obtained at least A-levels or equivalent UK qualifications and 66.5% having obtained at least an undergraduate degree or equivalent educational qualification. The number of included participants (as with Study 5) was therefore above the minimum sample size (52 to 128) required, as detailed from G*Power (Faul et al., 2007; 2009) calculations for a medium to large expected effect size with a power of 0.8. Participants were randomly assigned to one of four conditions upon signing up – with a near-equal distribution across all conditions (low load – marked = 64; high load – marked = 60; low load – unmarked = 63; high load – unmarked = 58). All were compensated £2.50 for participation and an additional bonus payment of £3 as part of the study reward incentive.

Study 5 - A UK representative sample of 292 participants were recruited via Prolific (2022) online marketing tool. Of these, 49 were excluded from analysis due to missing/incomplete data and another three was excluded due to invalid responses. Two-hundred and forty-three full datasets were therefore included in the analysis, consisting of 121 males (121 women, one prefer not to say), ages ranging from 18-78 (*M* = 43.16, *SD* = 14.514), with 87.7% having obtained at least A-levels or equivalent UK qualifications and 67.5% having obtained at least an undergraduate degree or equivalent educational qualification. Participants were randomly assigned to one of four conditions upon signing up (low load – marked = 58; high load – marked = 63; low load – unmarked = 62; high load – unmarked = 60). All were compensated £2.50 for participation and an additional bonus payment of £3 as part of the study reward incentive.

Informed consent was obtained from all participants and upon completion they were fully debriefed. All three experiments were approved by the Cardiff University School of Psychology Research Ethics Committee. All participants were highly proficient in the English language with it either being their first language or fluent as a second language, normal/corrected-to-normal vision, and for Studies 4 and 5 completed the survey on either a laptop or desktop computer.

Materials/Apparatus

Study 3 – This experiment adopted the same materials as Study 1, with the addition of a timer for the matrices task. The timer was presented on a screen in front of participants and was controlled by the experimenter on a separate computer. The timer was presented with five minutes and would count down showing minutes and seconds remaining.

Study 4 - The first aspect of the experimental design was created online using Qualtrics which consisted of a series of basic demographic questions to collected data on gender, age, highest level of education. The following sections after instructions consisted of the PANAS questionnaire (Watson, Clark, & Tellagen, 1988), then provided with instructions and a link to a program created in Pavlovia which replicated the matrix paradigm with 30 matrix items in total presented in a randomised order. Matrix items were presented one at a time, and participants had to click on which two numbers they thought matched to move onto the next item. There was a five-minute limit to complete as many items as possible within this limit, then after five minutes had passed, or if all items were completed within five minutes, participants were presented with a question of what should be done with their data and either a button labelled “delete” or “save” depending upon their condition. Regardless of condition, pressing the button would move participants onto the next section and data was saved. Following this, returning to Qualtrics, participants would be asked to report how many matrices items they had completed correctly and provide ratings on the composite of the NASA-TLX (Appendix A). Additionally, manipulation measures for stress derived from time awareness were included. These consisted of a Visual Analogue Scale (VAS) scaled 0 (Not at all) to 100 (Completely stressed) to indicate how much stress was derived from the participants awareness of time passing during the matrices task; and an indication of whether they believe on reflection they would derive more/less stress from time passing of a timer was shown (More stress, less stress, same amount of stress as no timer, unsure). A full debrief was then presented at the end.

Study 5 – This study adopted the same materials as Study 4, but with the addition of a timer being shown during the matrices task starting at five minutes, counting down in minutes and seconds. The wording of the time stress reflection check (more/less/same stress/unsure) was altered slightly asking to indicate whether the participant would derive more or less stress from their awareness of time passing of the timer was *not* shown.

Design and Procedure

Study 3 – The design and procedure for this study was the same as Study 1, with the exception of a timer being presented to participants in the preparation of and during the matrices task.

Studies 4 & 5 - Upon signing up to the study on Prolific, participants were provided with a Qualtrics link to the study – following a similar procedure as Study 1 and 3. Participants would be asked to complete the PANAS, were randomly assigned to the difficult or easy version of the matrices task and provided with a Pavlovia link for the online version of the matrices task. In Study 4, no timer was visible during the matrices task whereas in Study 5 a timer was visible for the duration of the matrices task. As in Study 2, participants would be asked to "save" or "delete" their data. Participants were randomly assigned to the condition where they could only pick the delete option, or the save option. Participants were then instructed to return to Qualtrics to report how many items they had answered correctly, provide ratings on the NASA-TLX composite (Appendix A), and providing ratings on the time stress manipulation checks, before being fully debriefed. In addition to informing participants of the true nature of the procedure, participants were also informed regardless of actual performances all would receive the full £3 bonus.

1.5.2 - Study 3: Results

As with Studies 1 and 2, PANAS scores were normally distributed across Studies 3, 4, and 5, and therefore could be analysed using ANOVAS, but all other matrices DVs were not normally distributed (all *p* values < .05 according to one-sample Kolmogorov-Smirnov tests) and thus were analysed using Kruskal-Wallis and Mann-Whitney U tests where appropriate.

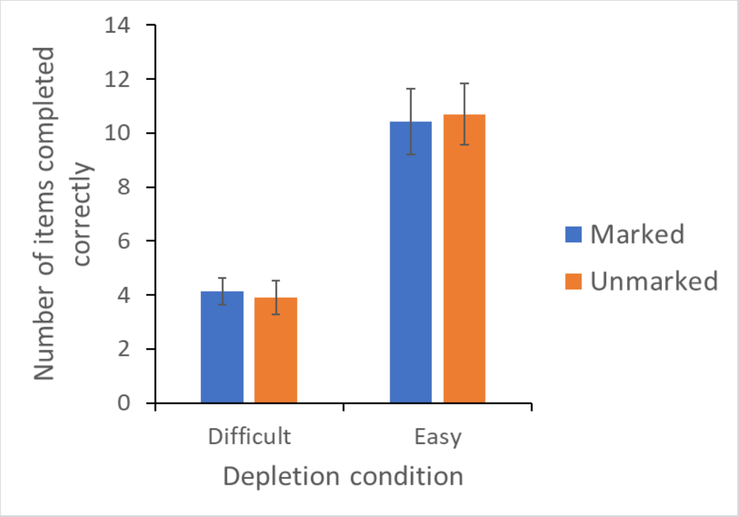
Objective Performance and Number of Correct Answers

Kruskal-Wallis tests revealed significant differences between conditions for both the number of correctly completed items ($H(3) = 37.72$, $p < .001$), and for proportion of answers correct ($H(3) = 29.68$, $p < .001$) – See Figures 8a and 8b. From Mann-Whitney U tests there were no significant differences between unmarked and marked difficult groups for total correct answers ($U = 391.0$, $p = .502$) and proportion of correct answers ($U = 400$, $p = .593$). Significantly and proportionately more items were answered correctly for the easy marked group compared to the difficult marked group (total correct: $U = 188.0$, $p < .001$; proportion correct: $U = 247.5$, $p = .001$), more in the easy unmarked group than the difficult marked group (Total correct: $U = 144.0$, $p < .001$; Proportion correct: $U = 197.0$, $p < .001$), more in the easy marked group than the difficult unmarked group (Total correct: $U = 171.0$, $p < .001$; Proportion correct: $U = 202.5$, $p < .001$), and more in the easy unmarked group than the difficult unmarked group (Total correct: $U = 134.5$, $p < .001$; Proportion correct: $U = 167.5$, $p < .001$). There were no significant differences between the total correct items for easy marked and unmarked groups ($U = 442.0$, $p = .740$), or the proportion of items answered correctly in the easy marked group than the easy unmarked group ($U = 380$, $p = .173$).

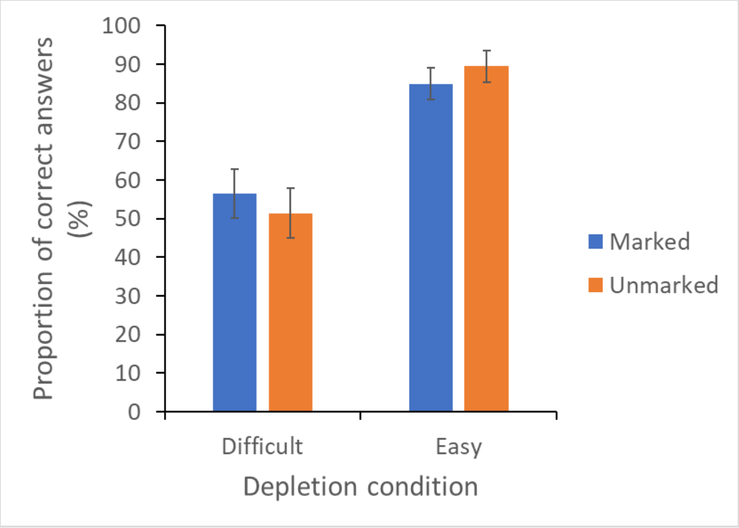
Figure 8.

The mean number of correct answers (a, top), and the mean proportion of correct answers (b, bottom) in each group at different levels of task difficulty (difficult and easy) and reporting condition (marked and unmarked) for Study 3. Error bars represent standard errors.

a)



b)



Subjectively Reported Task Performance

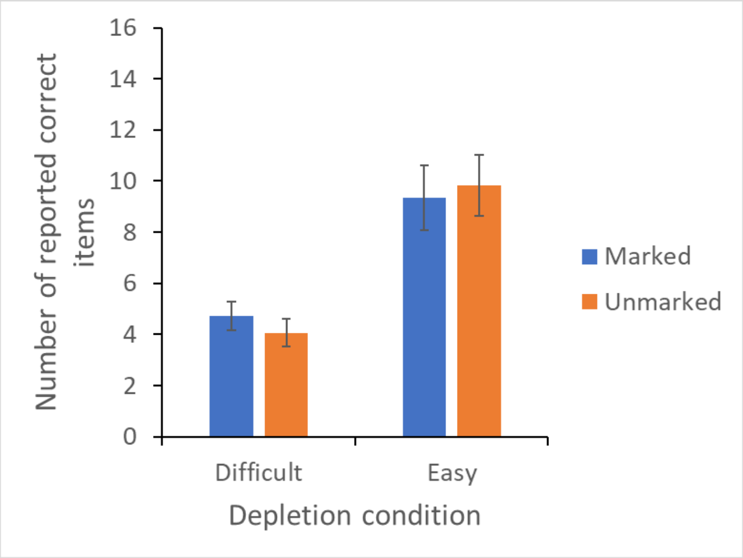
As illustrated in Figure 9a, differences were found across conditions for the number of answers reported to be correct by participants – and these were significant (*H*(3) = 30.140, p < .001). Mann Whitney U tests revealed there were no significant differences in the number of items reported to be correct between either difficult groups (*U* = 383.0, *p* = .425) or easy groups (*U* = 442.0, *p* = .739), though significantly more items were reported to be correct in easy unmarked and marked groups compared to difficult marked and unmarked groups (easy marked vs difficult marked: *U* = 238.0, *p* = .001; Easy unmarked vs difficult marked: *U* = 199.5, *p* < .001; Easy marked vs difficult unmarked: *U* = 186.0, *p* < .001; Easy unmarked vs difficult unmarked: *U* = 147.5, *p* < .001).

When examining objectively correct and reported correct answers (Figure 9b) – no significant differences were found between conditions (*H*(3) = 4.705, *p* = .195). Mann Whitney U tests revealed no significant differences for any group comparisons (all *p*s > .05).

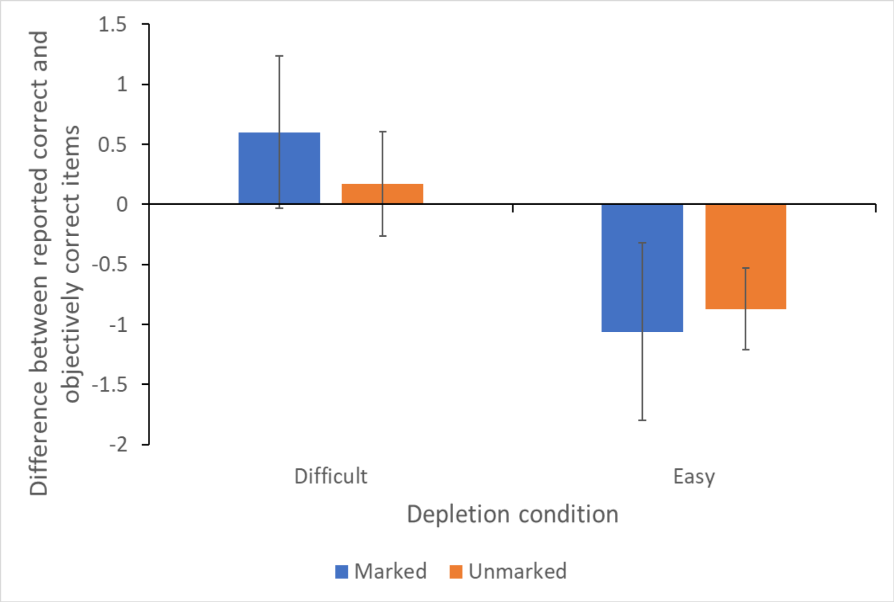
Figure 9.

The average number of subjective-reported correct answers (a, top) and the mean response bias (b, bottom) in each group at different levels of task difficulty and reporting routine in Study 3. Error bars represent standard errors.

a)



b)



PANAS and NASA-TLX

Comparisons were made for the scores of NASA-TLX questionnaires (Appendix A) between groups. Compared with the easy groups, the difficult groups had significantly higher mental demand (*U* = 1026.5, *p* < .001), lower subjective performance (*U* = 1095.5, *p* < 0.001), and higher frustration (*U* = 1342, *p* = .015). However, no significant differences were found for effort ratings (*U* = 1540, *p* = .157). Regarding the reporting routines, no significant difference was found for all ratings (mental demand: *U* = 1676, *p* = .506; subjective performance: *U* = 1627, *p* = .346; effort: *U* = 1716, *p* = .649; frustration: *U* = 1705, *p* = .614) – thus indicating cognitive load for the most part was significantly higher when task difficulty was increased but was not significantly different based upon private versus public judgement.

To test the possibility of prior participant mood as a confound, PANAS ratings were compared between all groups recorded prior to the experiment and found no significant differences from ANOVAs (*p* > .05). Prior mood could therefore be ruled out as a potential confound.

1.5.3 - Study 4: Results

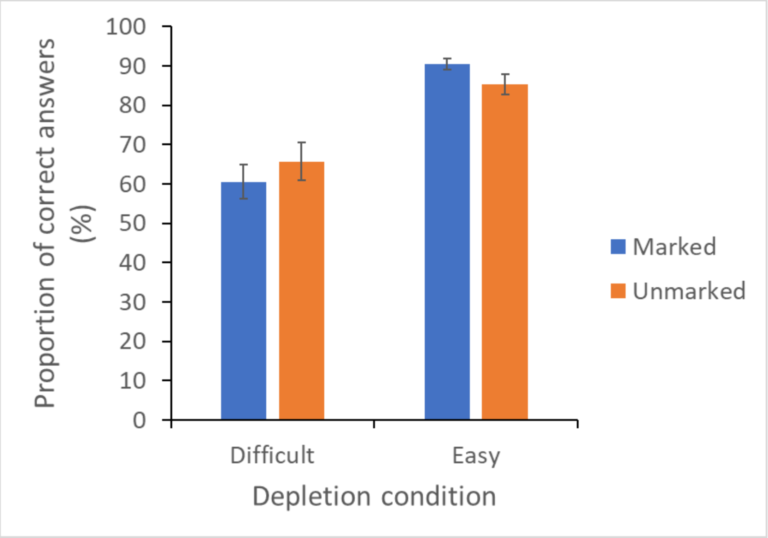
Objective Performance and Number of Correct Answers

Kruskal-Wallis tests revealed there were significant differences between conditions for both the number of correctly completed items (*H*(3) = 103.258, *p* < .001), and for proportion of answers correct (*H*(3) = 27.67, *p* < .001) – see Figures 10a and 10b. From Mann-Whitney U tests there appeared to be no significant differences between unmarked and marked difficult groups for total correct answers (*U* = 1701.5, *p* = .835) and proportion of correct answers (*U* = 1553.0, *p* = .306). Significantly and proportionately more items were answered correctly for the easy marked group compared to the difficult marked group (Total correct: *U* = 341.5, *p* < .001; Proportion correct: *U* = 945.0, *p* < .001), more in the easy unmarked group than the difficult marked group (Total correct: U = 581.0, p < .001; Proportion correct: U = 1120.0, p < .001), more in the easy marked group than the difficult unmarked group (Total correct: U = 378.0, p < .001; Proportion correct: U = 1292.0, p = .003), and more in the easy unmarked group than the difficult unmarked group (Total correct: U = 580.5, p < .001; Proportion correct: U = 1438.5, p = .04). There were no significant differences between the total correct items for easy marked and unmarked groups (U = 1982.5, p = .871), or the proportion of items answered correctly in the easy marked group than the easy unmarked group (U = 1834.0, p = .369).

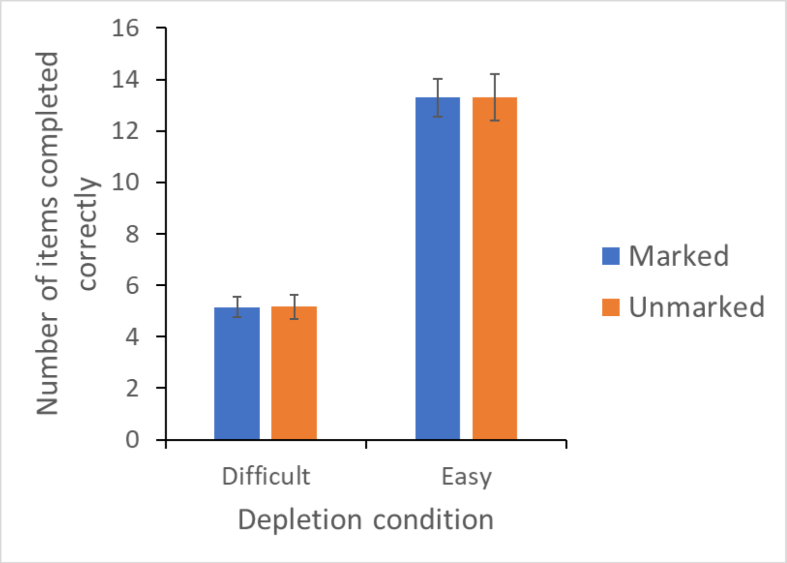
Figure 10.

The mean number of correct answers (a, top), and the mean proportion of correct answers (b, bottom) in each group at different levels of task difficulty (difficult and easy) and reporting condition (marked and unmarked) in Study 4. Error bars represent standard errors.

a)



b)



Subjectively Reported Task Performance

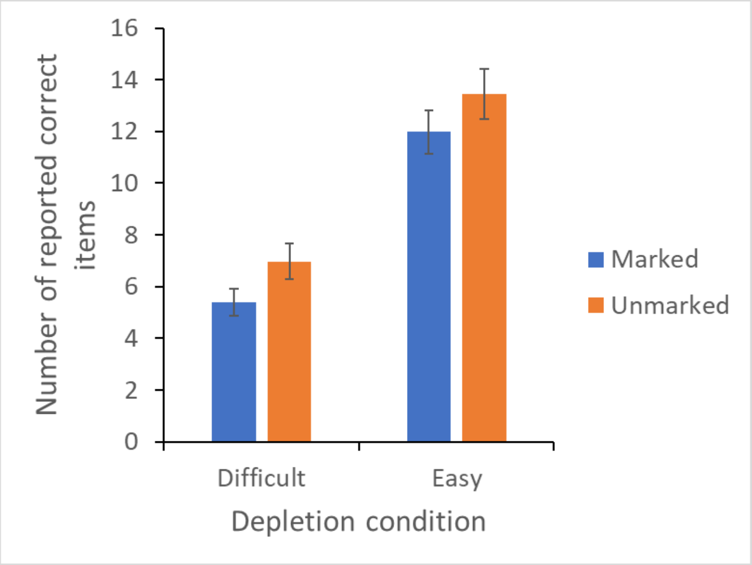
As can be observed in Figure 11a, differences were found across conditions for the number of answers reported to be correct by participants – and these were significant (*H*(3) = 62.935, *p* < .001). Mann Whitney U tests indicate there were no significant differences in the number of items reported to be correct between either difficult groups (*U* = 1449.5, *p* = .116) or easy groups (*U* = 1810.0, *p* = .319), but significantly more items were reported to be correct in easy unmarked and marked groups compared to difficult marked and unmarked groups (Easy marked vs difficult marked: *U* = 652.0, *p* < .001; Easy unmarked vs difficult marked: *U* = 680.0, *p* < .001; Easy marked vs difficult unmarked: *U* = 977.0, *p* < .001; Easy unmarked vs difficult unmarked: *U* = 892.0, *p* <.001).

When examining the objectively correct and reported correct answers (Figure 11b) – significant differences were found between conditions (*H*(3) = 16.763, *p* = .001). Mann Whitney U tests found the average difference between correct and self-reported performance was significantly lower for the easy marked condition compared to the difficult marked (*U* = 1361.5, *p* = .005) and difficult unmarked conditions (*U* = 1080.0, *p* < .001). The average difference between correct and self-reported performance was found to be significantly higher in the difficult unmarked condition than the easy unmarked condition (*U* = 1402.0, *p* = .027). No significant differences were found between any other group comparisons.

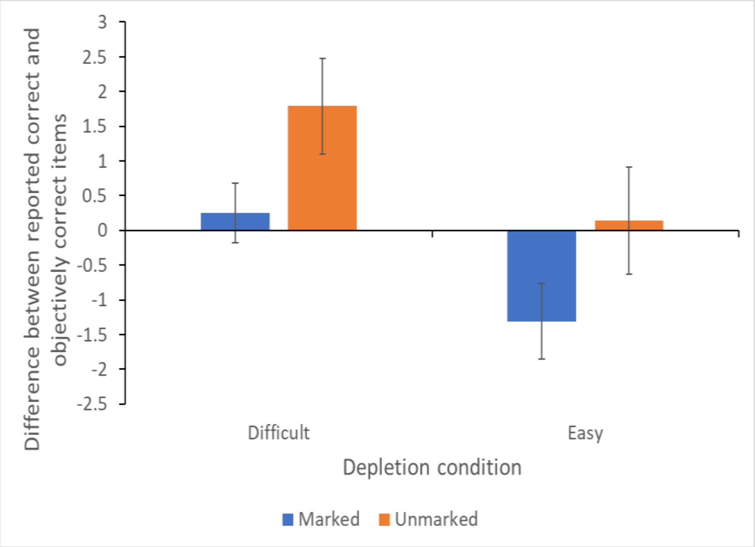
Figure 11.

The average number of subjective-reported correct answers (a, top) and the mean response bias (b, bottom) in each group at different levels of task difficulty and reporting routine in Study 4. Error bars represent standard errors.

a)



b)



PANAS, NASA-TLX, and Time Stress Descriptives

Comparisons were made for the scores of NASA-TLX questionnaires (Appendix A) between groups. Compared with the easy groups, the difficult group had significantly higher mental demand (*U* = 5307.0, *p* < .001) and lower subjective performance (*U* = 4447.5, *p* < .001). However, no significant differences were found for effort ratings (*U* = 7015.5, *p* = .434) or frustration (*U* = 7274.5, *p* = .775). Regarding the reporting routines, no significant difference was found for all ratings – thus indicating cognitive load to some extent was significantly higher when task difficulty was increased but was not significantly different based upon private versus public judgement.

To test the possibility of prior participant mood as a confound, ANOVAs compared the PANAS ratings between all groups recorded prior to the experiment and found no significant differences (*p* > .05). Prior mood could therefore be ruled out as a potential confound.

1.5.4 - Study 5: Results

Objective Performance and Number of Correct Answers

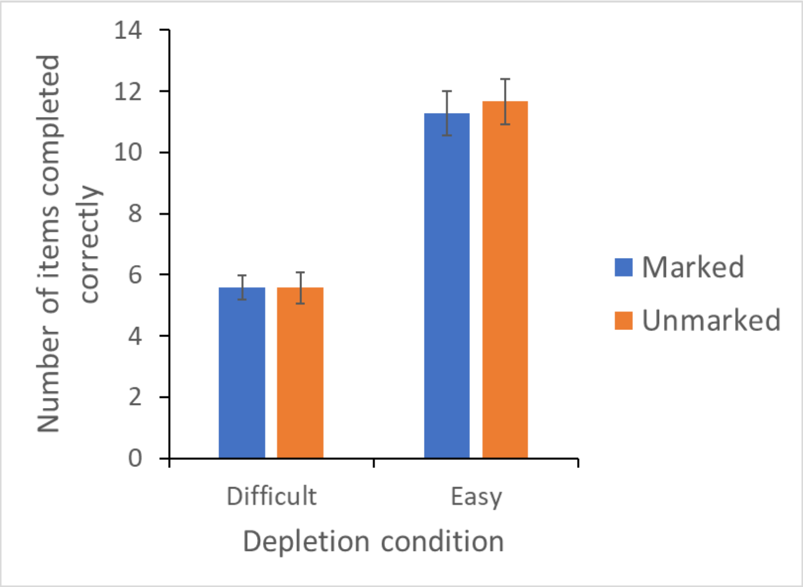
Kruskal-Wallis tests revealed there were significant differences between conditions for both the number of correctly completed items (*H*(3) = 69.785, *p* < .001), and for proportion of answers correct (*H*(3) = 26.627, *p* < .001) – See Figures 12a and 12b. From Mann-Whitney U tests there appeared to be no significant differences between unmarked and marked difficult groups for total correct answers (*U* = 1775.5, *p* = .560) and proportion of correct answers (*U* = 1777.5, *p* = .567). Significantly more, and proportionately more, items were answered correctly for the easy marked group compared to the difficult marked group (Total correct: *U* = 680.5, *p* < .001; Proportion correct: *U* = 1159.0, *p* < .001), more in the easy unmarked group than the difficult marked group (Total correct: *U* = 722.5, *p* < .001; Proportion correct: *U* = 1177.5, *p* < .001), more in the easy marked group than the difficult unmarked group

(Total correct: *U* = 693.0, *p* < .001; Proportion correct: *U* = 1108.5, *p* = .001), and more in the easy unmarked group than the difficult unmarked group (Total correct: *U* = 719.0, *p* < .001; Proportion correct: *U* = 1128.5, *p* < .001). There were no significant differences between the total correct items for easy marked and unmarked groups (*U* = 1741.5, *p* = .766), or the proportion of items answered correctly in the easy marked group than the easy unmarked group (*U* = 1766.0, *p* = .866).

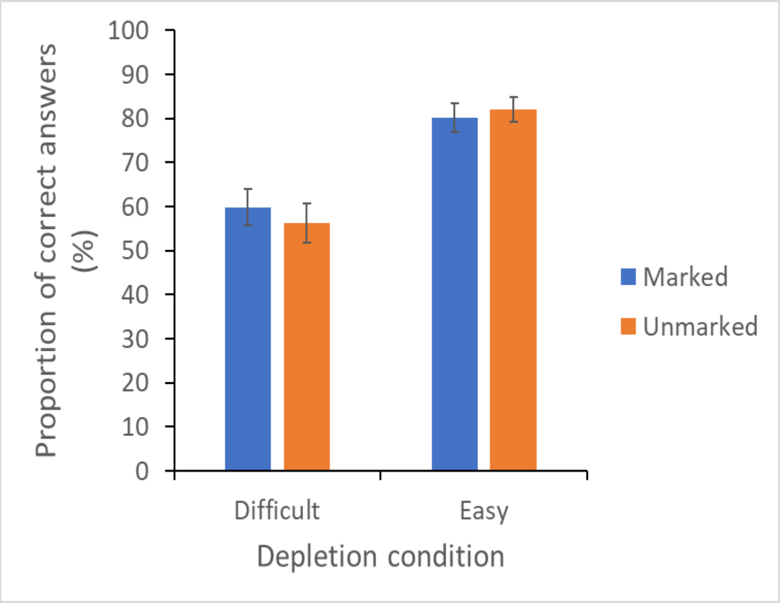
Figure 12.

The mean number of correct answers (a, top), and the mean proportion of correct answers (b, bottom) in each group at different levels of task difficulty (difficult and easy) and reporting condition (marked and unmarked) in Study 5. Error bars represent standard errors.

a)



b)



Subjectively Reported Task Performance

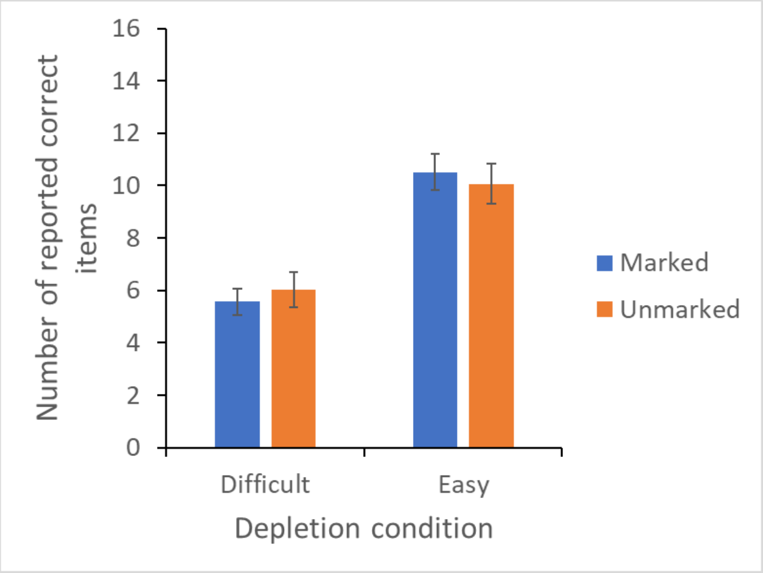
As seen in Figure 13a, differences were found across conditions for the number of answers reported to be correct by participants – and these were significant (*H*(3) = 46.602, *p* < .001). Mann Whitney U tests indicate there were no significant differences in the number of items reported to be correct between either difficult groups (*U* = 1877.0, *p* = .947) or easy groups (*U* = 1656.0, *p* = .453), but significantly more items were reported to be correct in easy unmarked and marked groups compared to difficult marked and unmarked groups (Easy marked vs difficult marked: *U* = 772.5, *p* < .001; Easy unmarked vs difficult marked: *U* = 1023.0, *p* < .001; Easy marked vs difficult unmarked: *U* = 829.5, *p* < .001; Easy unmarked vs difficult unmarked: *U* = 1056.5, *p* <.001).

When examining the difference between objectively correct and reported correct answers (Figure 13b) – no significant differences overall were found between conditions (*H*(3) = 5.861, *p* = .119). However, Mann Whitney U tests found the average difference between correct and self-reported performance was significantly lower for the easy unmarked condition compared to the difficult unmarked condition (*U* = 1464.5, *p* = .041), and marginally lower than the difficult marked condition (*U* = 1564.0, *p* = .053). No significant differences were found between any other group comparisons.

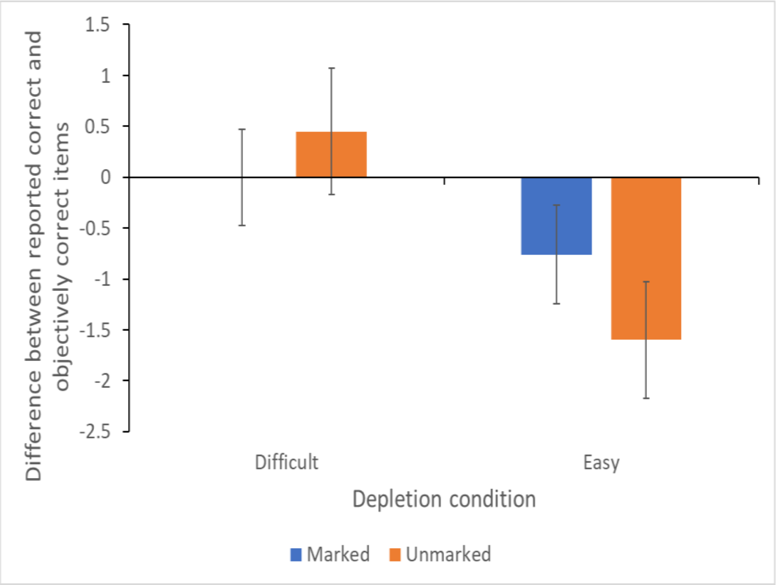
Figure 13.

The average number of subjective-reported correct answers (a, top) and the mean response bias (b, bottom) in each group at different levels of task difficulty and reporting routine in Study 5. Error bars represent standard errors.

a)



b)



PANAS, NASA-TLX, and Time Stress Descriptives

Comparisons were made for the scores of NASA-TLX questionnaires (Appendix A) between groups. Compared with the easy groups, the difficult group had significantly higher mental demand (*U* = 4325.0, *p* < .001), lower subjective performance (*U* = 4882.0, *p* < 0.001), and higher effort ratings (*U* = 6049.5, *p* = .012). However, no significant differences were found for frustration (*U* = 6835.5, *p* = .314). Regarding the reporting routines, no significant difference was found for all ratings – thus indicating cognitive load for the most part was significantly higher when task difficulty was increased but was not significantly different based upon private versus public judgement.

To test the possibility of prior participant mood as a confound, PANAS ratings were compared between all groups recorded prior to the experiment and found no significant differences. Prior mood could therefore be ruled out as a potential confound.

1.5.5 - Study 4 & 5 Time Stress Comparison

For Study 4, the average rating to indicate how much stress was derived from the participants awareness of time passing during the matrices task (0 = Not at all, 100 = Completely stressed) was 57.77 (*SD* = 27.999), with no significant differences found between the four conditions within Study 4 (*F*(3, 240) = 1.805, *p* = .147). On reflection, 71.7% of participants believed more stress would be derived if there had been a time visible during the matrices task compared to not being visible. Only 10.7% believed less stress would be derived, 11.5% the same amount of stress regardless of time presence, and 6.1% were unsure (one data point was missing).

For Study 5, the average rating to indicate how much stress was derived from the participants awareness of time passing during the matrices task (0 = Not at all, 100 = Completely stressed) was 64.86 (*SD* = 26.297), with no significant differences found between the four conditions within Study 5 (*F*(3, 239) = 2.061, *p* = .106). On reflection, 28% of participants believed more stress would be derived if there had *not* been a time visible during the matrices task compared to not being visible. 37.4% believed less stress would be derived, 27.6% the same amount of stress regardless of time presence, and 7% were unsure.

An independent *t-test* comparing time stress ratings between participants from Study 4 (no timer presented) and 5 (timer presented) and found stress ratings to be significantly higher in conditions in which a timer was presented to participants compared to those which did not have a timer visible (*t*(485) = 2.877, *p* = .004).

1.5.6 - Time Awareness Impact Upon Dishonesty

When comparing the average of the difference between objectively correct and self-reported correct matrices items for when a timer is presented (Study 5 – Figure 13b) and not presented (Study 4 – Figure 11b), no significant differences were found overall (*U* = 27555.0, *p* = .153). Although, in line with predictions, dishonesty was reduced in the difficult-unmarked condition when a timer was presented (*U* = 1326, *p* = .024). This significant difference, however, was not found for comparisons between Study 1 (in-person no timer presented – Figure 6b) and Study 3 (in-person timer presented – Figure 9b) difficult-unmarked conditions.

1.5.7 – Studies 3, 4, & 5: Discussion

Experimental designs in Studies 3, 4, and 5 each were developed and deployed to address key factors which had arisen from the first two studies (1 and 2) – believability in the public/private judgement manipulation, reward type, and the significance of time awareness. Studies 3 and 5 introduced the presence of a timer during the matrices task to increase time salience – thus comparisons could be made to understand whether a lack of dishonesty observed in Study 1 could be explained by heightened time awareness potentially confounding results. Studies 4 and 5 were deployed as online versions of the matrix paradigm with an alternative manipulation for public vs private judgement of performance (i.e., forced options to “save” or “delete” data before reporting performance), and involved immediate monetary rewards as adopted in previous studies adopting this paradigm (e.g., Mead et al., 2009) opposed to delayed rewards based upon increasing probability of winning (Study 1). Based upon the assumption that reward and public/private judgement manipulation confounds had been controlled for, it was hypothesised participants would be more likely to over report performance in higher cognitive load conditions when not under public scrutiny. In Studies 3 and 5, it was predicted that the presence of a visual timer during the matrices task would result in higher time stress ratings compared to those with no visual timer (also measured in Study 4, and relevant to Study 1). If this was the case, the increase in time awareness could explain any patterns of reduction in the engagement of cheating behaviour (Gino & Mogilner, 2014).

In Study 3 – involving an in-person replication of Study 1 with the addition of a timer – it was found again that no significant overreporting was found in the difficult-unmarked condition (Figure 9b), with a small amount of underreporting also being found in the easy conditions. This was akin to what was found in Study 1 (Figure 6b), but with underreporting now also being noted in the easy-unmarked condition. As found in Study 1, the marginal signs of underreporting in the easy-marked condition could indicate the increase of self-awareness and reduction in self-confidence at a task due to the public judgement of performance at a task which is perceived to be easy. Although, in the case of Study 3 this underreporting pattern was also noted for the easy-unmarked condition – potentially indicating the focus on time further reduced self-confidence (a pattern also replicated in Study 5 – Figure 13b). On average no significant overreporting was observed for the difficult-unmarked condition in Study 3 – whilst literature such as Mead et al. (2009) would suggest the increase in cognitive load should increase dishonest behaviour when provided with the opportunity to do so. The lack of such dishonesty in this instance could be due to a combination of a lack of believability in the public/private judgement manipulation in providing the perceived ability to cheat (as in Study 1), the expected reduction in dishonest behaviour for this group due to the increased awareness of time (as predicted based upon Gino & Mogilner, 2014), and the perceived utility of the probability-based monetary incentive. These issues remained for this study but were addressed in Studies 4 and 5 which shall be discussed shortly.

However, it is worth noting there was the addition of an unavoidable potential confound to the execution of Study 3 – COVID-19 data collection regulations. Only a small amount of data was collected for Study 3 from students in-person before data collection had to be halted with the outbreak of COVID-19. When data collection in-person was permitted once more, regulations (within the UK) such as social distancing of 2m, the wearing of face masks and limited numbers of people within university laboratories had to be adopted as part of the efforts to reduce the spread of COVID-19. Subsequently, during this period it could be the case - as with students across other sectors (e.g., Ilic et al., 2021) – that self-confidence was on average low; thus, as with increased time awareness, the likelihood of acting dishonestly could have been reduced.

When examining the levels of over/underreporting of performance across Study 4 – the online adaptation of Study 1 – the predicted patterns of behaviour had somewhat emerged. There was some evidence to suggest participants had overreported as predicted in the difficult-unmarked condition (Figure 11b) However, as there was no other evidence of statistical findings indicating consistent overreporting of this condition across the other conditions, little can be concluded which indicates consistent over-reporting is increased due to cognitive load when provided with the opportunity to act dishonestly. Although, for the pattern of underreporting in the easy-marked condition was replicated (as noted in Studies 1 and 3). Overall, this is congruent with Grieco and Hogarth (2009) which suggested people have a tendency to overestimate their ability at difficult tasks (to a lesser extent) and underreported for easy tasks, though with the caveat that overestimation could occurs when there is a lack of public scrutiny in difficult situations and underestimation in easy conditions with public scrutiny (Buehner & Townsend, 2015; Gino et al., 2009; Gino, Ayal, & Ariely, 2013; Mead et al., 2009). Whilst this study and Study 5, from involving data collected from an online sample of the general UK population, have the benefit of being able to generalise findings to a wider populus, this could have resulted in more variance in responses. Subsequently from this notable increase in standard error, this could explain why differences may not be completely clear cut. However, what these patterns of findings could still suggest is the manipulation of public/private judgement and instant monetary reward were successfully controlled for.

As anecdotal evidence of effective confound control, a number of participants (approximately 15) mentioned at the end of participating in Studies 1 and 2 they suspected that data of their actual performance would be retrained regardless of throwing away they task sheets; whereas during Studies 4 and 5, many participants when only offered the option to “delete” their data from the main task had messaged on prolific of their concern their data would be deleted and subsequently result in a rejection of payment for participation in the study due to producing an incomplete dataset. As users of Prolific are only likely to be permitted to sign up to studies on the platform if they have a good record of previous study completion, this observation of concern over potential loss of immediate and future reward versus gain could indicate high value in reward perceptions and believability in whether data was saved/deleted (and thus this online adaptation had improved upon previous versions in terms of believability in the public/private judgement manipulation).

Finally, Studies 3 and 5 introduced the presence of an observable timer during the matrices task as a way of increasing time awareness. Though less clear as to whether this was a significant factor in Study 3 due to points previously discussed, it was found significantly less dishonesty was found in the difficult-unmarked condition when a timer was presented (Study 5 – Figure 13b) compared to the difficult-condition when a timer was not presented (Study 4 – Figure 11b). With higher stress levels being indicated as a result of a timer being presented during task completion, it can be concluded, in line with my prediction and previous literature (Gino & Mogilner, 2014) that increased time awareness could reduce the likelihood of acting dishonestly when under cognitive load, provided there is a perceived opportunity to act dishonestly.

As previously hinted at, this could be because a greater awareness of time encourages more self-reflection upon one's own ability. When no timer is present, participants when making metacognitive references to their ability to complete items correctly within the fixed time limit – there is no objective, accurate, measure available to use as a reference. Without knowing how much time is left, other than a general sense based upon what sensual information there is available, their focus is likely to be on the task in front of them. However, when a timer *is* present, these participants were able to make objective comparisons of ability in real time, i.e. over the time-course of the task. Having more references to time passing could subsequently increase stress due to an increase in germane load – i.e., more in-depth, and frequent, evaluation and structuring of task approach and self-reflection – which is noted by differences in time stress self-report ratings from Studies 4 and 5. This could also be indicative of the Kappa effect (Kuroda et al., 2016) - whereby time duration between a series of consecutive stimuli used as temporal landmarks is thought to be shorter or longer than actual time passing. From having fewer temporal cues when no timer is presented, it could be perceived as there being more time than there is available to utilise, and thus lower stress levels compared to the opposite (Ogden, 2022). Whilst there were no significant differences of actual performance between timer/no timer comparisons, the difference found in dishonesty for the difficult-unmarked conditions with(out) a timer presented could indicate time awareness is more notable when examining perceived ability and self-rewarding behaviours. A summary of the findings from Study 3, 4, and 5 in light of how they can inform more applied cyberpsychology research is discussed below, in combination with Study 1 and 2.

1.6 – Chapter 1 Summary

Chapter 1 sought to further the understanding of what can influence the quality of decision making, with a focus on evaluating how cognitive load mechanisms can be significant influences on decision quality. From first being able to define the quality of decision making from a review of decision-making theories (e.g., EUT – Bernoulli, 1738/1954; Prospect Theory – Kahneman & Tversky, 1979; Bounded Rationality - Simon, 1957; Cognitive load - Sweller, 1988), a series of original experiments were developed to evaluate how the perception of good decision making could change due to these mechanisms. Through developing these highly-controlled experiments, this advances the knowledge of causal relationships between differing sources of cognitive load – the time point in which task difficulty was heightened and time stress – to establish common patterns of maladaptive behaviour under increased capacity for engagement in such behaviour (i.e., dishonesty/self-rewarding behaviour when there is a lack of public scrutiny). Such controlled studies allow for careful manipulation and control over key variables, and, through these five experiments, this chapter has been able to establish a foundation on which to move forward with. From developing variations of a well-utilised paradigm, these experiments demonstrated that once public judgement and cognitive load is successfully manipulated, there is no consistent statistically significant increase in engagement in dishonest behaviour when there is a lack of public judgement of performance. The priming of higher cognitive load does not appear to consistently increase this behaviour in the given context, with these studies demonstrating that real time increases of extraneous cognitive load, through task difficulty manipulation, can increase dishonesty but not consistently. No significant overreporting was noted in Study 1, 2, 3, or 5 for the difficult-unmarked conditions, and although in Study 4 overreporting appeared to be significantly higher in the difficult-unmarked condition than the easy-marked and easy unmarked conditions, it was not significantly higher than the difficult-marked condition (Figure 11b). Subsequently, the extent to which evidence from Studies 1-5 can inform the mechanisms of cognitive load upon acts of dishonesty which could underlie insider threat is limited. From this, however, there is a need to investigate, with an alternative focus, other sources of cognitive load to a) indicate how they apply to cyber-security, and b) explore how they influence cyber-security maladaptive behaviour.

However, there appeared to be some evidence in line with previous research (Gino & Mogilner, 2014) that heightened time awareness (germane cognitive load) could reduce dishonesty in difficult-unmarked conditions: over-reporting in the difficult-unmarked condition was significantly higher for the difficult-unmarked condition whereby participants had increased time salience (from Study 5) compared to those in the same condition with low time salience (from Study 4). When this same comparison was made between the in-person versions of the time salience manipulation, however, no significant differences were found. A reason for this inconsistency, though, could be due to differences in which the timer was presented to participants online versus in-person. Participants in-person in Study 3 who completed the matrices task off paper had the timer being presented on a computer screen which they would need to more actively look at compared to the online participants in Study 5 where the task and timer were both on a screen and visually closer together. Consequently, in conclusion, there is some evidence to suggest time salience could reduce dishonest behaviour in high cognitive load conditions when there is no public scrutiny, but further research adopting eye tracking methods should be adopted going forward to assess whether attentional differences could explain the differences in these findings for time salience. What these early findings could indicate, however, is that research into the significance of time pressure – in particular time perception – to cyber-security may be of interesting going forward with the overarching aim of the thesis to investigate how cognitive load could influence the quality of decision making in cyber-security. Nuances of time pressure, therefore, needed to be explored to better understand what research currently exists in the context of cyber-security, how time salience may be applicable to cyber-security decision making, and what gaps remain in the literature to date.

It could, based upon the discussion of the evidence from Studies 1-5, be argued that is unclear the extent to which behaviour observed may be driven by motivations behind dishonesty. As only behaviour was the key dependant variable across these studies, the motivation for such behaviour can be inferred from the manipulation of the context. However, what remains to be explored is the maladaptive nature of dishonesty – as acts of dishonesty could be driven by either malicious or non-malicious intent. It is possible that such behaviour was driven by an increased valuation of self-worth, to which a reward could be perceived as being more deserving of if greater effort has been exerted. The findings that public scrutiny and increased time awareness through simply the presence of a timer can reduce such behaviour demonstrates the importance, regardless of self-rewarding motivation, of how such measures could be adapted in other contexts to reduce maladaptive behaviour in more applied settings. However, recent evidence suggests the occurrence of dishonest behaviour is not normally distributed; with the majority of people acting honestly (Jiang et al., 2023). With a similar pattern being noted in Studies 1-5, research further examining the theoretical basis for acts of dishonest should explore 1) what individual difference markers are most likely to appear in people who act more dishonestly (e.g., high narcissism, psychopathy, Machiavellianism ratings – Blotner & Bergold, 2023; Wissing & Reinhard, 2019), and 2) investigate whether environmental manipulations such as reductions in cognitive load result in a significant reduction in dishonesty.

In cyber-security contexts, high cognitive load (that can vary between individuals) is a common occurrence (as with any workplace environment) due to, but not limited to, the presence of hard time constraints, periods of sustained high workload, engagement in complex tasks, social interaction in group contexts, with occurrences of interruptions and distractions. From understanding the mechanisms of cognitive load, we can sympathise with why some individuals could become insider threats – through malicious means for personal gain, or from non-malicious intentions (e.g., finding work arounds to reduce workload and increase self-value). The implications for the proportion of people being encouraged by malicious intent versus non-malicious intent in the context of cyber-security, however, is unclear from Studies 1-5. If individuals felt as though they could get away with small acts of dishonesty, as found to some extent in Study 4 (Figure 11b), in a cyber-security context this could have serious consequences for both the individual and the organisation they may work for – this even small, but significant, patterns of maladaptive behaviour are crucial to curtailing in applied settings.

Going forward and based on the current findings, the next key focus of the thesis was to explore time perception, and more specifically cognitive load derived from it, in applied cyber-security settings. Whilst it is important to note that increased task difficulty, regardless of where in time it occurs, can impact maladaptive behaviour engagement, in practice there may be greater difficulty in practical interventions to reduce this type of workload – work tasks and hard time constraints may be difficult to change. However, what has become apparent is the significance of time perception – something of which by its very nature is highly malleable (Di Lernia et al., 2018; Goldreich, 2007; Ogden et al., 2023), and could be more practically managed if investigated further. Counter to what findings from the first five experiments (Studies 1-5) indicate in controlled environments for time awareness, time *urgency* appears to be a significant problem from a cyber-security perspective (e.g., Marett & Wright, 2009; Nthala & Flechais, 2017) – perhaps indicating other mechanisms of time perception which could be noteworthy for evaluating risky cyber-security behaviour engagement. Therefore, the next chapter explored the wider literature of time perception through a systematic approach, investigating different types of time pressure, with a focus on how time perception mechanisms in applied cyber-security decision making are significant to risky decision making.

Chapter 2: Time Pressure in Cyber-Security Decision Making

2.1 – Subjective Time Pressure in Cyber-Security: A Systematic Review

2.1.1 – Objective versus Subjective Time Pressure

In human decision making, time pressure is defined as the “objective or subjective perceived limitation of the available time needed to consider information or to take a decision” (Giger & Pochwatko, 2008, p. 209). Time pressure can therefore be categorised into two different subgroups based upon the different types of sources of time pressure. *Objective* time pressure sources consist of hard time constraints (e.g., a set number of seconds, minutes, hours, days to complete a task, dealing with fixed-time interruptions or distractions during a task). Under these circumstances, there is a physical limitation to an individual’s ability to perform at a task. From the perspective of cognitive load theory, objective time pressure would be considered a form of intrinsic cognitive load (Sweller, 1988) as the constrain to cognitive ability is defined through the hard restriction of time to complete a task. *Subjective* time pressure sources, on the other hand, include levels of stress derived from an individual’s perception of time, sense of urgency, and perception of deadlines which could be manipulated by variables such as social influence, emotional regulation, time management decision making values, and the internal body clock. Subjective time pressure, therefore, would be considered a form of extraneous cognitive load (Sweller, 1988) as it is the interpretation and manner in which information is presented in which can cause a distortion in the perception of time, and subsequently influence the quality of decision making as urgency changes – influenced by factors such as emotional regulation (Gable, Andrea, & Poole, 2022) and subjective valuation of outcomes over differing spans of time (from temporal discounting - Abdellaoui, Gutierrez, & Kemel, 2018). Considering the Brunwik Lens model (Brunwik, 1956) discussed in Chapter 1, the objective passing of time and the subjective perception of time both exist simultaneously and may not always be the same due to how cues are used to judge time perception along with the associated stress derived from the disparity between them and goal an individual is trying to achieve. In some cases, which will be explored later in the chapter, the perception of objective time may be associated with the stress derived from it (e.g., Trang & Nastjuk, 2021) – demonstrating a relationship between objective time pressure resulting in the cause to subjective time pressure. However, other cues which relate to time do not indicate explicit time scales but could influence feelings of urgency (e.g., time urgency cues indicating the need to respond in emails – Raywood-Burke, Jones, & Morgan, 2023) indicate instances where subjective time pressure sources are independent of objective time pressure sources.

These distinctions are important to consider, both in theory and applied practice, as it is key to determining how behaviour may be influenced – and in turn identifying what needs to change in order to reduce the likelihood in engaging in maladaptive behaviours. Given approximately 80-90% of cyber incidents within business listed human errors in decision making as significant factors (CybSafe, 2020; Verizon, 2022; World Economic Forum, 2022), from a Cyberpsychology perspective, research examining such time pressure factors is necessary to fulfil the need for a holistic human-computer interaction (HCI) approach to cyber-security as well as to inform awareness and training interventions.

Laboratory research exploring the influence of *objective* time pressure has broadly revealed that performance in experimental tasks is significantly worse under time restrictions (e.g., Capraro, 2017; Capraro, Schulz & Rand, 2019; Moore & Tenney, 2012) at the individual (e.g., Ordonez & Benson, 1997) and group level (e.g., Karau & Kelly, 1992). Such task performance impairments also appear in different task types (e.g., essay writing, planning an action, and discussions - Kelly & McGrath, 1985) and even where additional practice trials are permitted prior to the main task which involved time constraints (Gonzalez, 2004). These findings also generalize to cyber-security decision making contexts with hard time constraints increasing risky decision-making behaviour (e.g., Acar et al., 2016; Jones et al., 2019; Kirlappos & Sasse, 2012; Vance et al., 2014). However, Parkinson's Law (1957) suggests that an increase in time made available to complete a task does not necessarily mean performance is increased as time spent on tasks decreases the marginal return in performance (also noted by Moore & Tenney, 2012). Therefore, in addition to researching hard time constraints it is also important to consider *subjective* time pressure to understand why performance does not improve linearly, why productivity may increase under hard constraints, and whether subjective time pressure has a similar negative affect to hard constraints.

Research to date concerning *subjective* or perceived time pressure has revealed mixed findings under laboratory conditions. For example, an increase in perceived time pressure through social valence (i.e., others highlighting insufficient time for learning and successfully completing task) worsened analytical performance in e.g. the Iowa Gambling Task (DeDonno & Demaree, 2008) but not in creative performance (e.g., as tested by the Remote Associates Task; Stein, 2016). In Stein's study there was no significant interaction between task difficulty and perceived time pressure; however, the pattern of results was in the predicted direction. This non-significant finding could be as a result of insufficient power to detect an effect of small magnitude due to the low number of participants. It could also be that individuals may have differing innate perceptions of time. For example, when Alison et al. (2013) examined the influence of perceived time pressure in police investigation simulations outside of the laboratory, those with a greater sense of time urgency were more likely to generate fewer hypotheses under external time pressure, had encouraged more heuristic decision-making strategies, and also were more susceptible to confirmation bias (i.e., adopted the tendency to search for information reinforcing prior beliefs).

There has been some research exploring theoretical frameworks of time pressure within cyber-security (e.g., Chowdhury et al., 2020), and research also noting that time pressure hinders productivity within work settings (e.g., Kirlappos et al., 2014). However, to progress with research on the topic of subjective time pressure in cyber-security it is necessary to collate and examine all relevant research on this topic to evaluate to what extent this phenomenon has been investigated, then identify directions for future research. Key questions are outstanding: Has Cyberpsychology (and/or indeed human aspects of cyber-security) research clearly distinguished between subjective and objective time pressure? Upon evaluation, has research to date been able to accurately investigate the relationship between subjective time pressure and cyber secure behaviours? These will be focused on (amongst others) within this chapter.

For example, Jeske et al. (2016) explored the relationship between impulsivity and decision-making when interacting with mobile devices. All participants were instructed that they have "an hour to submit some urgent work and decide to go to a public café to connect to the internet using one of several available wireless connections" (p. 549). As such, it cannot be determined whether subjective time pressure has a relationship with cyber secure behaviour for a few reasons. First, time urgency from instructions was not manipulated and simply an instruction presented to all participants – therefore this source of time urgency cannot be used to investigate the significance of this relationship. Second, impulsivity was the main concept being investigated; and while time urgency could be considered as a component of impulsivity (e.g., Hu et al., 2015) it was not in the measurement of impulsivity in the Jeske et al. (2016) study. Impulsivity has additional components to time urgency such as the role of emotion, cost-benefit analysis, attention, and self-control (Patton et al., 1995) which may be related to time urgency but cannot demonstrate time urgency cyber secure behaviour relationships.

Taken together, these findings highlight the need for a systematic approach to be used to identify relevant cyber-security research, of which strengths and weaknesses could be evaluated, to address outstanding key questions on time pressure distinctions. The present systematic review, therefore, aimed to address this need as well as highlight the next steps necessary to facilitate the understanding and impact of subjective time pressure upon practice in Human-Computer Interaction (HCI) and Cyberpsychology fields.

2.1.2 – Proposed Systematic Review

A fairly recent systematic review investigated the impact of time pressure including both time constraints upon actual behaviour and time urgency induced in hypothetical scenarios with the aim of developing a theoretical framework of psychological concepts relating to cyber secure behaviour (Chowdhury, Adam, & Skinner, 2019) including relevant research published over a 15-year period between 2002-2017. They found 21 relevant papers according to the criteria adopted and developed a theoretical framework summarising contextual factors (simulation, source and level of time pressure within cyber-security), psychological constructs (affect, perception, and cognition), moderating factors (task and user characteristics), and their relationship with non-secure human cyber-security behaviour from identified studies. From the identified studies it was universally found that all forms of time pressure adversely affect cyber secure decision making.

However, there are limitations to the findings drawn from the Chowdhury et al. (2019) review. First, most studies included were conducted using student participants. Whilst this allows for some degree of control over individual differences, there are limits on the degree to which findings can be generalised to the wider population as student populations, typically young adults (most within the 18-25 age range based on the studies), might arguably be more prone to higher risky decision making than older adults (e.g., Weller et al., 2011). Second, most studies identified only measured behaviour intentions rather than actual behaviour. This limits conclusions as behavioural intentions may not necessarily result in the same intended behaviours in practice (Ajzen, Brown, & Carvajal, 2004; Webb & Sheeran, 2006). Third, most (17 of the papers) employed subjective self-report or inferred measures for time pressure with very few (only four papers) using objective measures such as behavioural outcomes or employing neurophysiological equipment; thus, also limiting the validity of conclusions. Whilst subjective measures can be useful to investigate perception, perception of the world is not always a strong reflection of reality – nor do subjective measures of intention/belief/attitude necessarily result in action congruent with those values. Subsequently, there is a clear need for more research adopting more objective measures as well to compare perceptions of individuals, and interactions with the reality around them in cyber-security settings.

Other limitations of the Chowdhury et al. (2019) review included not having fixed criteria for inclusion/exclusion. Neither did they clearly distinguish between objective and subjective time pressure. This meant studies which had any time pressure component were included and later categorized studies by the simulation of time pressure as *explicit* (setting deadlines), *implicit* (imagining time pressure in hypothetical situations), or *self-referred* (studies were not designed to study time pressure but participants reported time pressure or haste as a cause of behaviour). Whilst this categorization of *explicit*, *implicit*, and *self-referred* does help identify some differences in study design (e.g., behavioural manipulations vs hypothetical situations versus observations/studies not directly testing time pressure), as well as aid the development of a theoretical framework, there was no clear evaluation of the significance of subjective time pressure.

As a significant body of research has already focused on the role of objective time pressure, this necessitates the need to extensively investigate the impact of subjective time pressure upon cyber-security. Thus, the focus of the present review was on sources of subjective time pressure using a refined search strategy. Furthermore, as technological developments and research outputs in the context of cyber-security have and continue to increase rapidly, it is essential we continue to keep up to date with all relevant studies and developments. Therefore, to provide a basis for future research to understand the influence of subjective time pressure in cyber-security, the current systematic review - using an extended search strategy with no date or journal restrictions – was conducted to try and answer the following primary research question:

- What is the body of knowledge examining the significance of the relationship of subjective time pressure with human cyber-security behaviour?

Furthermore, based upon findings and recommendations for research set out by Chowdhury et al. (2019), the current review also took note of the following secondary points of interest:

- Have there been behavioural or neurophysiological measures of the impact of subjective time pressure on cyber-security behaviour?

    If so, what was used and how valid are they?

- To what extent is actual behaviour measured within workplaces settings compared to home and laboratory settings?

Exploring these secondary points of interest is necessary to evaluate the efficacy of designs to understand the relationships between subjective time pressure and cyber secure behaviours in the different human-computer interaction (HCI) contexts in which people may be at risk. If behavioural and/or neurophysiological measures have been used in addition to subjective self-report measures, this could provide clarity to the true extent of risk significance, as well as allow for efficacy evaluation of using these measures in this area of research – for example, electroencephalogram (EEG) technology could be used to identify significant neural pathways in depth of cognitive processing (Nicolae et al., 2017; Schreiter et al., 2019) combined with eye tracking and pupil dilation measurements indicating the depth of stimulus processing (Langer et al., 2017), with heart rate monitors and skin conductance monitors to detect stress responses (Can, Arnrich, & Ersoy, 2019).

It is also necessary, whilst accounting for all cyber-security contexts which were reflected in the inclusion/exclusion criteria and search strategy, to distinguish between the contexts of laboratory, home, travelling, and work. Studying cyber-security behaviours within the laboratory may provide insight into manipulations under controlled conditions, whilst research in home and work contexts can aid understanding of HCI behaviour in real-life scenarios. Home and work cyber-security contexts may overlap as many of the same devices may be used for similar purposes; even more so for people working from home or taking a blended work environment approach. However, there are differences between work and home environments: 1) Workplaces may enact cyber-security policies which are actively enforced through training and practice which may not always apply, or be applied, to home users; 2) There are often differences in device use between work and home; 3) If workplaces are separate to home then there may be differing social or physical environmental influences; and 4) *Home* environments could also be defined as *not work*, meaning leisure behaviours involving technology could also be extended outside the physical home environment to internet use in public spaces, for example. Furthermore, due to the COVID-19 pandemic, the distinction between work and home environments became and still is to some extent increasingly blurred with an increase in people working from home – therefore searching for and evaluating research examining the significance of this blending of environments is also noteworthy in relation to the present review aims.

2.2 – Systematic Review: Methods

Search Strategy

Six databases, either specific to a field (e.g., psychology, business, information technology) or multidisciplinary to maximize search exploration and relevance (*Web of Science, psycINFO, SCOPUS, ACM, ABI/INFORM Proquest, and EBSCO Business*) were selected. Relevant studies were then searched for using a strategy including terms falling under the following themes: subjective time pressure and cyber-security. Each research theme comprised of a list of corresponding search terms which were combined with each other within each theme using the OR function to increase breadth (Table 4) alongside relevant subject headings (Medical Subject Headings – i.e., MeSH terms) where applicable. The combined search terms for each research theme were then combined using the AND function to add specificity. The search included references from any publication date up to the day of the final search – 11th February 2023. Search terms for each database research theme were thoroughly tested before inclusion in the search strategy by using multiple word combinations/reordering/alternate spellings to include the most references possible whilst retaining relevance (e.g., using *cybersecurity* and *cyber security* captured additional references, however *cyber-security* did not).

The *Google search engine* was also searched using relevant search phrases ("time pressure cybersecurity" and "subjective time pressure cybersecurity") to find relevant grey literature. A total of 60 links (30 per search phrase) from the first three pages of *Google* were examined for both search phrases. Subsequent pages were also searched for relevant publications; however relevant links were not found thus searching inclusion stopped after page three for each phrase. As *Google* searching differs to database searching (inclusion of more key words drastically reduces search results), a shorter search strategy using multiple relevant key words was tested to evaluate the optimal combination or phrases to detect the most relevant links.

Inclusion and Exclusion Criteria

For inclusion in the current review the reference was required to:

1. Include data on human behaviour relating to the manipulation or observation of the influence of subjective time pressure.

2. Include data on people in a position to be at risk of being cyber attacked.

Exclusion criteria were used to add further specificity to the search. References were excluded if:

1. Data did not include measures related to subjective time pressure within a cyber-security context.

2. Data only related to objective time pressure.

Table 4.

List of research themes with corresponding search terms used in the systematic review search strategy.

Research theme	**Search terms**
Subjective time pressure	*time pressure* *pressure of time* *time constraint* *constrained time* *time limit* *limit of time* *limited time* *time stress* *time perception* *perception of time* *perceived time* *time awareness* *awareness of time* *perceived duration* *time estimation* *estimation of time* *estimated time* *subjective time* *internal clock* *sufficient time* *insufficient time* *rushed* *hurried* *time management* *management of time* MeSH terms (psycINFO only): *time management, time perception, temporal frequency, stimulus duration, interstimulus interval*
Cyber-security	*cyber security* *cybersecurity* *cyber attack* *computer security* *data security* *security of data* *information security* *security of information* *IT security* *security of IT* MeSH terms (psycINFO only): *Information security*

Only peer-reviewed journal articles, conference papers, and detailed studies with replicable methods published in book chapters were included. Full books, theses/dissertations, and reviews were not excluded from the search strategy, but after abstract screening remaining publications of these types were excluded. These relevant books, reviews, and theses/dissertations were saved and used for citation searching (i.e., searched for relevant references through reference lists and author publication lists). Studies may have been conducted in any country, but the publication text had to be in the English language. Full texts obtained in other languages translations were found where possible and noted where not. Studies for which a translated full text could not be obtained could not be included. There were no limits by journal or publication date.

Screening, Eligibility, and Assessment

After removal of duplicates, 6162 unique titles were identified from the database searches. As key words linked to the study may not have been included within the title explicitly, researchers agreed prior to searching that records with ambiguous titles were included at the title searching stage to allow for a more in-depth screening at the abstract searching stage based upon the inclusion/exclusion criteria. Furthermore, to reduce selection bias, a random sample of 100 titles were originally selected and then independently screened for inclusion at this stage (lead reviewer – LR, and interrater 1 – IR-1) with the aim of 95% minimum initial agreement. The first screening stage resulting in 81% agreement between researchers, thus another 100 titles were randomly selected and screened independently using feedback from the previous screening – resulting in 95% agreement. Where initial disagreement remained for five titles, these were discussed together and full agreement on screening was reached at this stage. The remaining 5962 titles were screened by the LR.

Following title screening, one-hundred random abstracts were selected from references not excluded at title screening stage to be independently screened (LR and IR-2). The first abstract screening (100 abstracts) resulted in 89% initial agreement, and therefore another 100 randomly selected abstracts were screened using feedback from discussions with the aim of reaching 95% minimum initial agreement. Of the second abstract screening, 95% agreement was reached with the remaining five abstracts further discussed, and actions agreed upon collectively. Remaining abstracts were then screened by LR, acquiring full texts for all considered to be includable or doubtful. Full texts were then screened by LR, referring any doubtful cases to IR-1 and IR-2 for discussion and resolution. Full texts were citation searched for further relevant papers. Relevant studies were shortlisted and discussed between all researchers with agreement on what should be included in the analysis based upon the criteria previous defined, then data was extracted into tables as appropriate and assessed for inclusion whereby a clear relationship was shown between subjective time pressure and cyber secure behaviour. Quality and risk of bias of included studies was assessed using the Mixed Methods Appraisal Tool (MMAT - Pluye et al., 2011). No studies were excluded on the basis of quality assessments in order to allow for all relevant research to be reviewed and evaluated for strengths and limitations.

Analysis Plan

Before undertaking the deeper review, a meta-analysis was planned to test the direction, size, and consistency of the effect of perceived time pressure upon human cyber behaviour. However, if there was insufficient data for a meta-analysis, or if studies were too diverse, then a descriptive account of effects was planned between studies. Studies were examined for important common themes - i.e., source of subjective time pressure, design, participants recruited, and key findings – and were grouped, and data extracted accordingly to evaluate the extent to which we can be certain the current body of research addresses our research aims. The review adhered to the PRISMA 2020 guidelines for systematic reviews (Page et al., 2021).

2.3 – Systematic Review: Results

2.3.1 - Overview

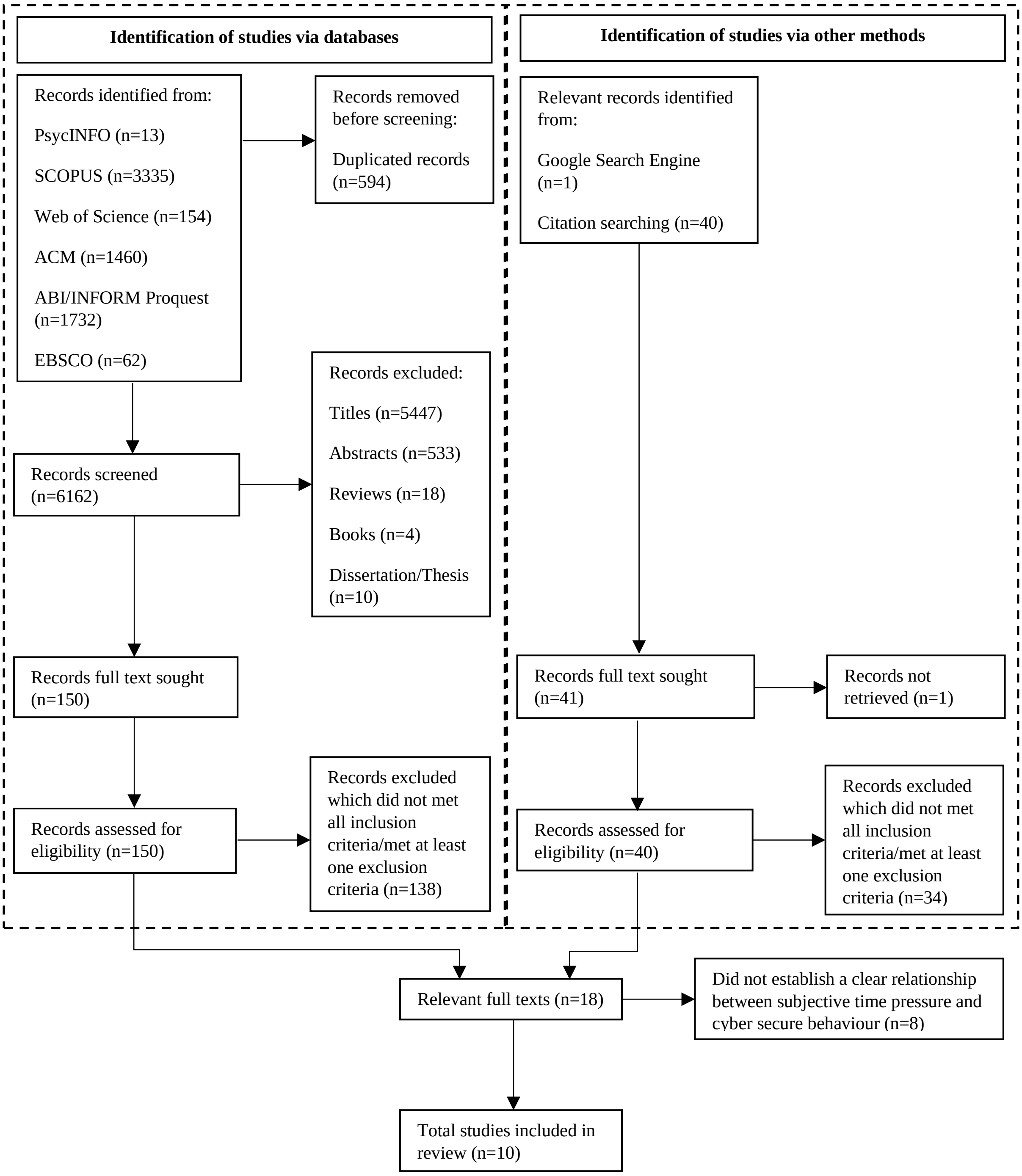
Figure 14 confirms that the full search of the six databases yielded 6162 unique references – of which most could be eliminated by title and abstract (n=5980). References excluded by publication type after abstract screening (n=32) were pearl searched (i.e., searching for relevant references cited in other relevant references) for relevant references along with records found to fit all criteria and a further 40 references were yielded and required full text to be acquired. *Google* searching only resulted in one more unique reference being found. Of the 191 full texts sought; one could not be obtained due to restricted access despite being requested. Eighteen papers were identified (12 from search strategy, six from pearl searching) as meeting all inclusion criteria and no exclusion criteria (Appendix B). However, only data from 10 papers demonstrated clear relationships between subjective time pressure and cyber secure behaviour (Appendix C).

Of the 18 papers deemed relevant based upon the review criteria, eight were not included in the subsequent analysis for numerous reasons. A paper by Beautement et al. (2009) investigated perceived costs and benefits of time pressure in cyber-security compliance but did not distinguish whether participant responses were in relation to subjective or objective time pressure. Chan et al. (2005) only included one relevant survey item which did not distinguish whether responses related to subjective or objective time pressure. Chowdhury et al. (2020) conceptualized an integrative framework and explored what countermeasures could be used to reduce the impact of time pressure on behaviour. However, there was no attempt to investigate and demonstrate clear relationships between subjective time pressure and cyber secure behaviour. Fagan et al. (2017) contained one relevant survey item but again it cannot be determined whether ratings for this item were due to a source of subjective or objective time pressure. Hu et al. (2015) included measures related to the role of time urgency and information security policy compliance. However, these measures formed part of a larger measure of ‘impulsivity’. Because impulsivity is comprised of concepts separate from subjective/objective time pressure the specific relationship between time pressure and policy violations cannot be determined. Williams et al. (2017) and Williams and Polage (2019) aimed to examine the role of influence techniques in susceptibility to maladaptive cyber behaviour and did detail how urgency cues within emails could be used as an influence technique. However, within these two papers, analyses were carried out on influence techniques as a whole rather than comparing the significance of each type of influence technique – thus the significance of urgency cues were not clear. Li et al. (2020) included the use of urgency cues in phishing emails, however there was no manipulation of this factor in the study, thus cannot determine the significance of this source of subjective time pressure in relation to cyber secure behaviour. Because of the reasons outlined above these eight papers were not included in the analysis.

The remaining 10 papers (Cui et al., 2020; De Bona & Paci, 2020; Marett & Wright, 2009; Nthala & Flechais, 2017; Parsons et al., 2015; Trang & Nastjuk, 2021; Vishwanath et al., 2011; Wang et al., 2012; Williams, Hinds & Joinson, 2018; Wright, Marett & Thatcher, 2014) differed greatly in terms of methodology which prevented conducting a meta-analysis. As such, a narrative was synthesized detailing information on important topics relating to the review aims and previous research.

Figure 14.

PRISMA diagram demonstrating the systematic review process of reference retrieval and screening for relevant studies.



Identification of studies via databases
Identification of studies via other methods
Records identified from:
PsycINFO (n=13)
SCOPUS (n=3335)
Web of Science (n=154)
ACM (n=1460)
ABI/INFORM Proquest (n=1732)
EBSCO (n=62)
Records removed before screening:
Duplicated records (n=594)
Relevant records identified from:
Google Search Engine (n=1)
Citation searching (n=40)
Records excluded:
Titles (n=5447)
Abstracts (n=533)
Reviews (n=18)
Books (n=4)
Dissertation/Thesis (n=10)
Records screened (n=6162)
Records full text sought (n=150)
Records full text sought (n=41)
Records not retrieved (n=1)
Records excluded which did not met all inclusion criteria/met at least one exclusion criteria (n=138)
Records assessed for eligibility (n=150)
Records assessed for eligibility (n=40)
Records excluded which did not met all inclusion criteria/met at least one exclusion criteria (n=34)
Relevant full texts (n=18)
Did not establish a clear relationship between subjective time pressure and cyber secure behaviour (n=8)
Total studies included in review (n=10)

2.3.2 – Synthesised Narrative

In this narrative, key aspects of included studies are detailed which break down important themes to consider when evaluating their quality and their authors' conclusions. First, it was identified what sources of subjective time pressure have been investigated to highlight common areas of investigation and areas which could be explored in future research. Second, the review acknowledges key differences in study designs detailing their relevance to understanding the relationship between subjective time pressure – followed by information about participant samples to note divergences in size and demographics. Below details all relevant findings and later the discussion evaluates the implications these findings have for this area of research.

Source of subjective time pressure. In eight out of 10 included studies, with data collected from six participant samples, the source of subjective time pressure originated from visceral triggers either within the email title or main email body (Cui et al, 2020; De Bona and Paci, 2020; Marett and Wright, 2009; Parsons et al, 2015; Vishwanath et al, 2011; Wang et al, 2012; Williams, Hinds and Joinson, 2018; Wright, Marett, and Thatcher, 2014). These consisted of language used to suggest a necessity to respond immediately and/or within a limited amount of time. Nthala and Flechais (2017) reported urgency to complete work requiring internet connections, derived from physical time constraints, was also a relevant source of subjective time pressure in data security. In circumstances involving urgency to complete a primary task, the perceived importance of the primary task was something users considered to determine the importance of urgency vs the importance of security. Trang and Nastjuk (2021) examined how time constraints could increase the likelihood of non-compliant behaviour with information security policies by increasing perceived time stress. Taken together, it appears research on this topic has focused mainly upon one key source of subjective time pressure with more which need to be accounted for.

Study design. Each of the 10 studies included within the systematic review adopted different designs. Nthala and Flechais (2017) used a qualitative approach whereby participants were interviewed using semi-structured questions on a wide variety of topics with the aim to investigate what information is used in data security decisions made by home users. Questions required participants to consider relevant topics such as the costs and benefits involved in decision making, the role of time pressure, and the significance of urgency in completing different tasks.

Using a quantitative approach, participants in Vishwanath et al. (2011) and Wang et al. (2012) were presented via an online survey after being exposed to original phishing emails containing information intended to invoke a sense of urgency to respond and other phishing email cues (e.g., grammar errors, sender address). Participants were then asked to report their likelihood to respond to the email, attention to cues in the email, and other self-report measures relating to cognitive effort in email processing using 5-point Likert scales.

Also examining the likelihood of responding to phishing emails, Marett and Wright (2009) and Wright, Marett, and Thatcher (2014) using a field experiment design investigated the effectiveness of deceptive tactics used in email phishing during an introductory management information systems (MIS) course. At the beginning of their course participants were provided with unique passwords in sealed envelopes for access to software needed for the enrolled course and instructed of the importance of not disclosing this password to anyone under any circumstances as this could be a breech to the secure grading process; signing a non-disclosure agreement that they would abide by their class policy. After 8 weeks, participants were sent an email from a fictitious IT employee asking participants for their passwords to help recover data from a data management accident. This email varied with the use of phishing tactics between participants including mimicked sender information, personalization, name-dropping, and a call to action inducing time urgency – with the number responses recorded for each condition. One condition manipulated the presence of an urgent need to respond within the email whereas in the other condition there was no call for urgency to respond.

Similarly, De Bona and Paci (2020) sent out phishing emails to employees in an Italian company whereby the email either required the recipient to change an account password otherwise their account would be blocked (urgency condition), would claim to have been from the Chief ICT (Information and Communication Technology) Officer (authority condition), or just have been from a fake sender (control condition). Following this, De Bona and Paci followed up with a second phase using employees who had fallen susceptible to the phishing attack in phase one to observe whether participants had learned from their previous training. In phase two, participants were sent an email requesting participants to check their payslips in case they may be wrong from a technical error – however for participants the email either requested they check within two days otherwise they may not be able to take off other days, claimed to have been sent from the human resources chief, or simply contained a fake sender address and cloned link for the payslip.

Adopting a within-participants experimental design, Cui et al. (2020) examined participants in a role-playing scenario, from the perspective of a foreign financial trader, indicating their likelihood to responding to or deleting emails. Of the 16 emails presented in total, half contained cues to phishing, and the researchers manipulated the presence of time urgency cues and recipient information. A study by Trang and Nastjuk (2021), using a mixed-factors experimental design, also involved participants being asked to take part in a role-playing scenario in which they had to reply to emails from the perspective of a company employee. Participants were provided with either an information security policy (ISP) in which compliance would be rewarded (reward condition), punished with disciplinary action (punishment condition), or given basic regulations (control) before being asked to reply to all emails consisting of requests from individuals which would break the ISP. Participants were either told it would take 10-minutes to respond to all emails, but they were only given 6 (pre-determined from a pre-study) and given a timer upon clicking the first email (time constraint condition) or were not restricted by time/given any time pressure cues (control). Upon completion, participants provided 7-point Likert ratings on four items measuring their perceived time stress. Trang and Nastjuk coded email responses after the study as ISP non-compliant behaviour if participants had shared confidential information, or found workarounds which violated the ISP, or were coded as compliant if they had not breached the policy.

Parsons et al. (2015), using data collected from participants assessing whether 50 presented emails were genuine or phishing in a previous study (Parsons et al., 2013), involved five experts to assess the presence or absence of 13 cues (including time urgency) which may be used to assess whether emails were phishing or genuine. From this, researchers were able to determine which cues participants from their previous study had used and assess the likelihood these cues affected choices on how to manage these emails. Using data collected across a 6-week period in 2015 (Study 1), Williams, Hinds and Joinson (2018) simulated phishing emails and their responses were collected and coded by researchers as to whether they contained any authority cues (i.e., indications authority was used in the email as a persuasion technique) or time urgency cues. Williams et al. then examined whether the frequency of responses to these emails were related to these two methods of persuasion.

Collectively, these study design details highlight several differences in methods – qualitative, quantitative, observational, and experimental. However, all 10 studies have used either self-report or behavioural measures to examine this phenomenon: with none adopting neurophysiological measures.

Participants. Participants from Marett and Wright (2009), Wright, Marett, and Thatcher (2014), Vishwanath et al. (2011), and Wang et al. (2012) consisted of internally recruited undergraduate university student volunteers. These four studies were relatively large in terms of sample sizes (n=224 in the first two, and n=321 in the last two, respectively – see Table 3), close to evenly balanced for gender, had similar mean ages, and recruited from either business or communication courses in the USA. Participants in the De Bona and Paci (2020) study consisted of 191 employees from an Italian company in Northern Italy, also balanced in gender but consisted of a wider range of ages, job roles, education, and area of work (see Table 3). Cui et al. (2020) collected data from a larger sample (n=518) also balanced in gender. However, most were undergraduate students, and the majority had previous experience of different forms of phishing. The 229 participants within the Trang and Nastjuk (2021) study had a good balance between men and women, most were highly educated, though all were required to have some form of work experience. Nthala and Flechais (2017), however, had a very small sample of home users from Oxford, UK (n=15) recruited through snowball sampling with a wider age range. Data from participants in Parsons et al. (2015) were selected from a previous study as these participants were not specifically aware they were taking part in a phishing study, thus would arguably better represent real world responses. In Williams, Hinds and Joinson (2018), retrospective data was collected from approximately 62,000 employees from a UK public sector organization. However, the researchers state they did not have access to demographic information, thus the balance of participants' across potentially relevant demographic information is unknown for this data set.

From the mix of participants across these 10 studies, conclusions from the analyses of their data could be considered to be generalizable to both laboratory and some workplace settings – as well as across sexes and a range of age groups due to balanced samples. However, studies lack details on potentially relevant demographic information (e.g., cyber-security training experience, information technology competence, previous experience of cyber incidents/breaches); thus, the extent to which findings could be applicable to different groups of people on these bases may be require further exploration. Furthermore, due to little data being collected from home-users, the extent to which findings can be applied to home environments and blended work strategies warrants further investigation.

Significance of subjective time pressure on cyber secure behaviours. All studies revealed that subjective time pressure had a significant adverse impact upon cyber secure behaviour. In Nthala and Flechais (2017) interviewees reported they considered the significance of the task they needed to complete and how they would spend their time in data security decisions, with in some cases physical time constraints altering their sense of urgency. One interviewee stated that due to the urgency to complete some work requiring an internet connection, they did not spend time focusing attention on the security of networks they connected to - later finding after completing work whilst connected to an unsecure network someone had been reading their unread emails.

Using a logistic regression analysis, Marett and Wright (2009) and Wright, Marett, and Thatcher (2014) found the presence of email cues invoking the need for immediate response significantly increased the likelihood of responding to a phishing email by 3.19 times. Cui et al. (2020) also found participants were more likely to reply to emails containing time urgency cues; however, they also noted this finding regardless of whether recipient information was present or not. Phishing emails were more likely to be deleted if no sender information was present, however presence of time urgency did not impact likelihood of deletion. Cui et al. noted participants were more likely to search for relevant information in emails with no recipient information when no time urgency cues were present. Although, they also found participants were less likely to search for relevant information with emails did contain recipient information and no time urgency cues.

Vishwanath et al. (2011) and Wang et al. (2012) also found their participants would be significantly more likely to consider responding to a phishing email due to their attention to visceral attention cues invoking a sense of urgency to respond. Higher attention to visceral attention cues also significantly reduced cognitive effort in processing a targeted phishing email. However, Vishwanath et al. and Wang et al. found the effect of attention to visceral attention cues was weakened by an increased knowledge of email-based scams. In the De Bona and Paci (2020) study, participants were also more likely to fall susceptible to phishing attacks because of urgency cues in emails. Those in the urgency conditions were also more likely to respond phishing emails compared to sources of authority as a persuasion technique, as well as compared to the control condition. De Bona and Paci also found that previous training was not effective in reducing phishing susceptibility.

The study by Parsons et al. (2015) revealed that multiple cues in emails contributed to whether participants correctly responded to emails, but notably found discrimination between genuine and phishing emails was worse when emails contained urgency cues. Participants in Parsons et al. were least likely to respond to emails correctly, with only 42% accuracy for these emails. Furthermore, Williams, Hinds and Joinson (2018) from analysing a large number of responses to phishing emails, also found the presence of time urgency cues was significantly related to an increased likelihood of response to malevolent emails. Critically, Trang and Nastjuk (2021) found that physical time constraints can increase an individuals' perceived time stress, which in turn was related to an increase in risky cyber behaviour. However, they also found that adopting an information security policy (ISP) which involves elements of punishments can significantly weaken the positive relationship between perceived stress and non-compliant behaviour.

Taken together, the findings collectively suggest subjective time pressure may significantly increase the likelihood in engaging in risky maladaptive behaviours. However, the majority of these findings (eight out of 10) relate to time urgency cues within emails. Of the 10 studies analysed, only one study (Trang & Nastjuk, 2021) examining the significance of stress derived from different hard time constraints, and one study (Nthala & Flechais, 2017) explored the significance of time management and task prioritization. As a consequence, the extent to which current findings from this research can be generalized to other sources of subjective time pressure and different cyber-security behaviours is limited.

2.4 – Systematic Review: Discussion

A systematic review was carried out for the body of knowledge regarding the impact of subjective time pressure on human cyber secure behaviour. Using a refined search strategy along with clear inclusion and exclusion criteria, eighteen papers were found to include relevant data from people who were in a position to be at risk of cyber-attack (Appendix B). However, eight of these studies (Beautement et al., 2009; Chan et al., 2005; Chowdhury et al., 2020; Fagan et al., 2017; Hu et al., 2015; Li et al., 2020; Williams et al., 2017; Williams & Polage, 2019), whilst meeting inclusion and exclusion criteria, did not demonstrate clear significant relationships between subjective time pressure and cyber secure behaviour thus nothing could be concluded from these papers about the impact of subjective time pressure on cyber-security. Only data from eight datasets, analysed in 10 papers, were included within the main analysis as they demonstrated a clear relationship between subjective time pressure and human cyber secure behaviour (Appendix C).

The 10 papers included in the narrative analysis demonstrated subjective time pressure having an adverse influence on cyber secure behaviour and could therefore mean that people will put themselves or others (including the organizations they are affiliated with/work for etc.), at greater risk of a cyber-breach. Eight out of the 10 papers found elements of phishing emails which increase the need for an urgent response significantly increase the likelihood of falling victim (Cui et al., 2020; De Bona & Paci, 2020; Marett & Wright, 2009; Parsons et al., 2015; Vishwanath et al., 2011; Wang et al., 2012; Williams, Hinds & Joinson, 2018; Wright, Marett, & Thatcher, 2014). These studies collectively evaluated the same source of subjective time pressure using large samples across different populations – students and employees across different countries from within- and between-subject designs – thus findings on this source can be considered both valid and reliable. Furthering this, De Bona and Paci (2020) compared time urgency cues to authority as a persuasion technique and found urgency cues resulted in even more people falling victim to phishing attacks than both authority and control conditions.

In the context of other research examining the roles of persuasion techniques (Cialdini, 2009) suggesting authority is a major contributor to increasing phishing susceptibility (Akbar, 2014; Butavicus et al., 2015; Zielinska et al., 2016), De Bona and Paci's (2020) findings would suggest time urgency could be an even greater threat to maladaptive behaviours. A reason for falling susceptible to phishing emails containing urgency cues could be due to a mechanism highlighted in Vishwanath et al. (2011) and Wang et al. (2012); whereby as attention to urgency cues increases, depth of processing emails reduced. Furthermore, if the presence of urgency cues results in people being less able to discriminate between phishing and genuine emails (Baryshevtsev & McGlynn, 2020) then these are risks which should be targeted to reduce the likelihood of responding to phishing. Cui et al. (2020) also predicted the likelihood of responding to phishing emails could be due to the likelihood of searching for relevant information within emails, moderated by the presence of urgency cues and sender information. However, findings conflicted with prior predictions – searching for relevant information was more likely when cues were no urgency cues or sender information was not present, but less likely when no urgency cues were present when sender formation was present. What can be concluded from this finding is limited due to only adopting self-report measures for likelihood of information searching. An improvement for future research examining the significance of information searching and urgency cues could be to use eye tracking, as used in McAlaney and Hills (2020) to measure perception and attention to amounts and types of information to provide a more accurate understanding of this mechanism.

The other two papers included in the analysis (Nthala & Flechais, 2017; Trang & Nastjuk, 2021) examined different sources of subjective time pressure, providing further insight into the mechanisms of subjective time pressure risks. Nthala and Flechais (2017) highlighted the importance of task context playing a role in urgency – namely if the importance of completing work under a time constraint is high, home users may be more likely to take cyber risks in order to get their work done. Although, there needs to be further investigation into subjective time pressure and cyber-security behaviours in home environments and blended work environments due to little data collected on this subject and in these domains detailing the precise nature of work arrangements and leisure activities involving cyber-security risks.

Trang and Nastjuk (2021) examined in greater detail how stress from subjective time perception, manipulated by hard time constraints, could influence time management and increase the likelihood of people not complying or finding workarounds to cyber behaviours policies. As this was the only study found to examine stress derived from the perception of manipulated time constraints, more exploration is needed to investigate the mechanisms of hard time constraints influencing stress derived from time perception as other studies have noted having hard time constraints can increase the likelihood of phishing susceptibility (Butavicius, Taib, & Han, 2022). One explanation for this susceptibility could be due to hard time constraints shifting the perceived utility of cues which could be utilised to detect phishing emails (Sturman et al., 2023); though more research on this mechanism is needed to further the understanding of risky decision making. Trang and Nastjuk (2021) also highlighted how only the punitive cyber policy helped reduce non-compliance – although it is worth nothing that whilst this was significant, the moderation effect was not large. Thus, when adopting cyber policies to guide cyber behaviours it is worth noting their efficacy could be limited by both likelihood and severity of punishments for non-compliance. Furthermore, due to the low moderation effects found, there is a clear need for other HCI measures to help moderate cyber risky behaviours due to subjective time pressure. Decision support tools used in intelligence analysis such as alternative hypothesis testing could be investigated further to reduce confirmation bias, though replications and tailoring to the context in further research is required with mixed findings being found on the efficacy of such methods in improving judgement accuracy (Mandel et al., 2018; Primer, 2009; Toniolo et al., 2023).

Findings are consistent with research investigating the role of objective time pressure in cyber-security decision-making (Acar et al., 2016; Kirlappos & Sasse., 2012; Vance et al. 2014), suggesting time pressure as a whole is of importance to account for when assessing cyber-security risks. With this in mind, it is necessary to design HCI, workplace, and immersive simulation studies based upon the clear distinction between objective and subjective time pressure in research to determine whether time pressure as a whole, individual components, or some components combined have more significant influence on cyber secure decisions and behaviour. It could be possible for people to engage in taking risky shortcuts due to hard time constraints (objective time pressure source – intrinsic cognitive load), inferred urgency to complete a task and stress derived from hard time constraints (subjective time pressure source – extraneous cognitive load) or meta-cognitive evaluation of the disparity between time limits and self-perception of performance (a combination of objective and subjective time pressure sources – germane cognitive load) – the latter of which could even be a guide for time constraints (self-imposed or otherwise) if time constraint is not present. For example, in Beautement et al. (2009), participants reported they felt justified in circumventing cyber-security measures intended to reduce cyber-attack risk if they believed they interfered with delivering work on time, particularly when a deadline was coming up. Whilst this is clearly a significant finding in relation to time pressure and cyber secure behaviours, it cannot be determined whether these behaviours, or intentions of behaviour, are contrived from their physical time constraints, self-evaluation of self-efficacy and internal body clock, or self-imposed deadlines.

Some research investigating psychological concepts which are linked to subjective time pressure in cyber-security such as impulsivity (e.g., Hu et al., 2015) should be furthered to understand these relationships. Self-control measures for screening such as the those used in Hu et al. (2015) whilst distinguishing between different concepts measurements in analyses – e.g., time urgency, impulsivity, risk-taking, motivation and decision-making styles – could aid with understanding how time urgency relates to other individual differences which predict cyber secure behaviour (Bishop et al., 2020; Raywood-Burke et al., 2021). The context of subjective time pressure sources may differ in directional relationships – e.g., time pressure at home is related to stress both at home and at work, but time pressure at work is not related to stress at home (Kleiner, 2014). With work and home blending in some fields, accelerated recently due to the global COVID-19 pandemic, understanding how time pressures may differ depending upon HCI contexts should be explored as evidence suggests subjective time pressure can be a consistently frequent occurrence across settings (Akdemir & Yenal, 2021; Atkins & Hueng, 2013).

Some limitations can be noted from the studies reviewed and the implications they have for at least some of the conclusions drawn. First, the only sources of subjective time pressure investigated within the studies was time urgency derived from email titles/content (eight papers) or subjective time stress derived from hard time constraints/deadlines (two papers). To date, this would mean we can only apply the significance of subjective time pressure relating to cyber behaviours to two different sources of subjective time pressure and specific cyber behaviours. Based on the findings of this systematic review, future research should expand upon the designs and findings from these studies with other potential sources such as environmental cues for time perception, further investigate the significance of internal body clocks/time management and explore interactions between subjective and objective sources of time pressure. Second, three quantitative papers measured intention of behaviour, six papers measured actual behaviour, and one paper detailed a qualitative study including intentions for, and actual, behaviour. None of the studies included in the present review adopted any neurophysiological measures to investigate this phenomenon, further limiting conclusions as these studies are reliant upon subjective measure or response behaviours.

Research in this field could benefit from adopting neurophysiological measures such as, but not limited to, EEG, heart rate monitors, eye tracking (including pupil dilation – e.g. to get an indication of levels of processing) measurement, and skin conductance responses. Other research using such measures have suggested how these applications within designs may compliment subjective self-report and response measures – EEG technology to identify significant neural pathways in depth of cognitive processing (Nicolae et al., 2017; Schreiter et al., 2019), eye tracking and pupil dilation measurements indicating attention and the depth of stimulus processing (Langer et al., 2017; McAlaney & Hills 2020), and heart rate monitors and skin conductance monitors (Can, Arnrich, & Ersoy, 2019).

Review Limitations

As with all systematic reviews, there is the potential for relevant published research to be missed from searches – e.g., due to noteworthy papers not being listed within databases searched or biases in the inclusion and exclusion of studies. The combination of specific search strings, databases searched, and specified inclusion/exclusion criteria may also have biased the literature output. However, to reduce this likelihood the search plan adopted a multifaceted approach for each stage of the systematic review which was pre-defined in the review protocol before the review commenced. First, to ensure maximum exploration and relevance, databases chosen for the search needed to be from a mixture of databases relevant to the area of research and multidisciplinary. Of the six databases targeted to be searched, two were multidisciplinary (Web of Science and SCOPUS), one was relevant to Psychology (psycINFO), one was relevant to business (EBSCO Business), and two were relevant to information technology and engineering (ACM and ABI/INFORM Proquest).

Second, the search strategy needed to be likely to identify relevant papers (if they existed) without being too broad in focus. To ensure this, the search strategy development involved testing of multiple variations of words, phrases, and combinations including MeSH/subject terms and narrowing down which were most likely to detect studies relevant to the review aims. Third, at the identification stage (see Figure 14) any relevant books, review papers and dissertations/theses were removed but searched to further reduce the risk of missing relevant papers. Potentially relevant full texts obtained were also pearl searched to reduce the likelihood of missing papers. With the potential for inclusion/exclusion bias, inclusion and exclusion criteria were clearly defined before the search was carried out to reduce this.

To further reduce bias, stage-by-stage inter-rater reliability checks were adopted between researchers using randomly selected references. If less than 95% of the sample resulted in the same outcome between researchers, then the level of consistency could not be deemed significant. Achieving sufficient agreement meant further screening could be completed with confidence in the inclusion/exclusion process being reliable. Of the studies deemed necessary to obtain the full text, one could not be obtained due to limited access – meaning this paper not included could be relevant and missed from analysis (Ayaburi & Andoh-Baidoo, 2019). However, we did attempt to seek sources of papers with limited access which was possible for some papers but was still restricted for this one paper. When determining whether a paper sufficiently met criteria to be included and reduce exclusion/inclusion bias, all initially identified studies were shortlisted and discussed with all researchers collectively and reached agreement on which studies were deemed to meet the criteria and which met criteria and demonstrated a clear relationship between variables to be included in data extraction and analysis.

2.5 - Chapter 2 Summary

From this systematic review it can be concluded that there is evidence – albeit limited in terms of the number of published studies to date – demonstrating that subjective time pressure can have a significant influence on decision-making in human-computer interaction (HCI) situations where cyber-security could be compromised. This should be considered in intervention development to, for example, reduce (and ideally eliminate) the risk of maladaptive behaviors occurring. However, the present review highlights the research to date on this topic has investigated relationships of only specific elements of subjective time pressure and cyber secure behavior (mainly time urgency cues in emails) – thus more research must be carried out in this area to address this research gap by exploring how other aspects of subjective time pressure could be significant factors to consider across a broader range of cyber behaviours. As noted above, there are more aspects and measures which could have been adopted in research designs to strengthen our knowledge of the significance of time pressure subjective components in conjunction with other aspects of time pressure. Therefore, key findings from this systematic review were utilized for the development of subsequent research within this thesis. First, there was a clear need to examine more sources of subjective time pressure across a broader range of cyber-security behaviours to investigate whether consistent findings were found across wider contexts, and how they may compare to other known predictors of behaviours (e.g., Raywood-Burke et al., 2021; Safa et al., 2015). Second, considering how time urgency may vary between individuals, there was a need to explore how accurately time can be perceived, whether measures exist which could be used to determine an individual's innate sense of urgency, and to what extent this may relate to engagement in maladaptive cyber behaviours. Third, despite consistent evidence being found to identify the threat time urgency cues pose in phishing susceptibility, the perceived consequences of replying/not replying to emails could be moderated by other key factors such as the email context – thus should be also considered to understand why the success of such persuasion techniques may vary. These research designs developed and presented in the next chapter, with the aim to aid development of HCI interventions to other aspects of cyber-security, could help users during work and leisure time to alter behaviours by reducing the influence of subjective time pressure sources for cyber breach risks.

Chapter 3: Individual Differences in Time Urgency and Cyber-Security: On the Significance of Relationships, Accuracy of Time Perception, and Improving Measurements

3.1 - Overview

As highlighted from the systematic review in Chapter 2, three main focus points were drawn from the findings:

1) There is a clear need to examine subjective time pressure across a broader range of cyber-security behaviours.

2) In order to evaluate how time perception and urgency may vary between individuals, it is important to consider to what extent variation in this individual differences may explain engagement in riskier cyber-security behaviours, and how this compared to other known predictors of cyber-security behaviours.

3) The wider context of phishing emails needs to be considered when evaluating the success of urgency as a persuasion technique.

This chapter addresses the first two points by examining the ability of individual differences to predict safe engagement in a range of cyber-security behaviours. This included focusing on how subjective time pressure could be treated as an individual difference, how it compares to other known predictors of behaviour (e.g., aspects of protection-motivation theory such as information security awareness – Raywood-Burke et al., 2021; Safa et al., 2015), and explore explanations for why patterns in time perception discovered in this chapter may have occurred. Furthermore, the chapter involves investigation of arguably a more suitable method of improving the validity of self-report individual difference measures – i.e., comparing the framing effects of traditional Likert scales (e.g., scales with fixed rating marks 1-5) to Visual

Analogue Scales (VAS – scales scored on a continuous slider/line, e.g., scored 0-100) - and demonstrate the capacity for reducing confounding framing effects. From this, implications are discussed for safer practice by utilising people's strengths and vulnerabilities, and potential directions for intervention developments in this research area.

3.2 - Measuring Urgency and Individual Differences in Cyber-Security

From a research perspective, people can be categorised according to similarities in individual differences to examine variation between groups in terms of factors such as demographic information including gender (Falk & Hermle, 2018), social-economic status (SES – Li, Xu, & Xia, 2020), education (Groot & van den Brink, 2010), age (Chen et al., 2018), and so on, as well as various psychological constructs such as personality (Indarti et al., 2017), impulsivity and risk-taking behaviour (Herman, Critchley, & Duka, 2018). Of these near infinite ways to differentiate, categorise individuals, and compare intersectionality of categories, measures used to collect this information can be used to examine relationships between individual differences and behaviours, values, and attitudes (e.g., Rudolph et al., 2017; Walumbwa, Lawler, & Avolio, 2007; Zajenkowski et al., 2020). From a human-centric perspective, these approaches and associated tools and methods could be useful in cyber-security as they hold the potential to identify trait strengths and vulnerabilities predictive of behaviour. For example, a tool for measuring cyber-security behaviours was developed recently at the global aerospace company Airbus (Morgan & Asquith, 2021) for personnel to accurately identify engagement in secure behaviour, with the aim to utilise such data to design targeted training (and other interventions – including decision support systems) to address clusters of vulnerabilities.

Currently, technologically driven tools in the field of cyber-security tend to assume a *one size fits all* approach. For example, system monitoring as a common risk mitigation driven by system anomalies used across all users within a business (e.g., Security Information and Event Management, SIEM, tools used by low-level security operation centre, SOC, analysts). In some instances, technological interventions may be the only appropriate type of intervention due to limited human involvement or capacity to control for human behaviour – for example recent research has demonstrated how AI could be utilised to correctly identify passwords with up to 95% accuracy through the typing sounds from keyboards (Harrison, Toreini, & Mehrnezhad, 2023). However, in instances where humans are more involved in a cyber-security process, technological interventions may be useful but used in isolation does not fully target human vulnerabilities; nor validate and promote strengths. By creating, refining, and deploying human-centric tools – perhaps informed by individual differences - in combination with technological interventions, maladaptive cyber-security behaviours could be better targeted and more effectively mitigated.

As highlighted in Chapter 2, time pressure (both objective and subjective) can increase the likelihood of humans engaging in maladaptive cyber-security behaviours. However, the presence of time pressure does not necessarily mean that there is a risk of maladaptive behaviour under all circumstances – with variability being noted in all studies found from the research previously reviewed, and in some instances improve productivity (e.g., Moore & Tenney, 2012). Some individuals may fall susceptible to the *planning fallacy*, whereby the estimation of how long a task takes to complete is systematically underestimated (Kahneman & Tversky, 1977), likely due to an *optimism bias* (Buehler, Griffin, & Ross, 1994) - the tendency to believe the future will be better than the past, therefore estimating that future tasks will not take as long as tasks already completed. Judgement of time could be moderated through other variables such as social influence (Fine & Vajsbaher, 2013) and workload factors (Baldauf, Burgard, & Wittmann, 2009) which may exaggerate the Kappa effect (whereby time duration between a series of consecutive stimuli used as temporal landmarks is thought to be shorter or longer than actual time passing – e.g., Kuroda et al., 2016). This exaggeration could mean an individual's urgency to complete a task within a given time could change depending upon their perception of time, and subsequently impact their performance. Furthermore, there is the potential for time perception and urgency to vary naturally between individuals – regardless of the circumstances; highlighting the need to evaluate individual differences in time pressure and time perception in the ability to predict engagement in a broad range of safer cyber-security behaviours (initial findings highlighted in Raywood-Burke et al., 2021).

Given this need, two different measures were adopted in Study 6 which utilised an observational design: the self-report Chronic Time Pressure Questionnaire (Denovan & Dagnall, 2019) indicating feelings of harriedness (i.e., feeling rushed) and awareness of deadlines, and a behavioural measure of time perception accuracy (Dougherty et al., 2005) consisting of the mean accuracy of time perception trials. Both have been previously evaluated (Alison et al., 2013; Corvi et al., 2012; Denovan et al., 2023; Dougherty et al., 2005; Dougherty & Hunter, 2003; Kim, Alison, & Christiansen, 2020), but not in relation to cyber-security behaviours – thus part of the novelty of this observational study was to note whether consistent findings were found for these measures as had been found in previous research. The Chronic Time Pressure Questionnaire, if indicating greater feelings of harriedness and cognitive awareness of deadlines with less safe cyber-security engagement as predicted, could be utilised as a diagnostic tool to highlight time management interventions which could be designed to support good cyber-security habits by reducing time urgency in conjunction with other known predictors of cyber behaviour.

The behavioural measure of time perception in particular was an important addition to compliment the self-report measure of subjective time pressure as from the research included in the Chapter 2 systematic review, none explicitly evaluated changes in the accuracy of time perception to predict cyber-security behaviours. An example of its use in another applied context is detailed in Alison et al. (2013) where differences were found in time perception moderated the influence of subjective time pressure upon the number of hypotheses generated for a simulated police investigation. Individuals were either told “As we are short of time today we have had to cut down on the amount of time we would normally like you to complete the scenario…” (p. 87) or were not told this before the task. In both conditions participants, were given the same amount of time. Alison et al. (2013) found specifically that for individuals who overestimated time in the low time pressure condition generated approximately the same number of hypotheses as those in the high time pressure condition. However, for individuals who underestimated time more hypotheses were generated in the low time pressure condition compared to the high time pressure condition.

Kim, Alison, and Christiansen (2020) furthered this finding by also investigating the impact of time pressure upon the quality of hypotheses generated in police investigation simulations and found not only did hypothesis generation decrease in quantity as time pressure increased for individuals who underestimated time passing, hypotheses generated also decreased in quality according to expert ratings. However, a critique of these examples is that the authors claim that this measure for time perception is a measurement of time urgency, though this is unclear. Whilst it is possible the accuracy of time perception could indicate time urgency, other factors which were not measured within these examples could influence the perception of time which are not related to urgency (e.g. age and cognition – Vasile, 2015). Other factors could also influence an individual’s sense of urgency which is not captured by the measurement of time perception accuracy (e.g., emotional modulation – Lake, LaBar, & Meck, 2016). Consequently, this behavioural measure of time perception will not be referred to as a measurement of urgency in this thesis. What these and other examples (e.g., Dougherty et al., 2005; Dougherty & Hunter, 2003) can still indicate, however, is that measuring an individual’s estimation of time passing could still be useful in predicting behaviour – specifically if underestimations of time passing resulted in poorer hypotheses being generated, this could suggest underestimations of time could also result in poorer decision-making in cyber-security. If the measure of time perception could predict engagement in cyber-security behaviours, with an underestimation of time perception hypothesised to be a predictor of engagement in riskier cyber behaviours, then this could account for more variance in explaining why individuals engage in certain cyber behaviours. Based upon these assessments of previous literature, research questions 1a, 1b, and 1c were adopted for Study 6 (detailed below) to evaluate the extent to which these measures for time perception and urgency could be used to predict cyber-security behaviours. It was expected that an underestimation of time passing, and given the evidence discussed in Chapter 2 (e.g., Cui et al., 2020; De Bona & Paci, 2020; Trang & Nastjuk, 2021; Vance et al., 2014), would be indicative of greater engagement in riskier cyber-security behaviours in the following study (Study 6); and that ratings for heightened feelings of Feeling Harried and Cognitive Awareness of Time Pressure in the Chronic Time Pressure Questionnaire would be predictive of engagement in riskier cyber behaviours.

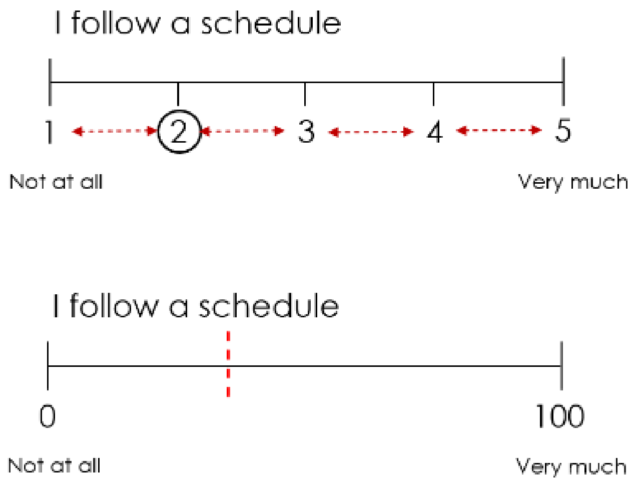
Several studies have attempted to examine how select individual differences measures could be used to examine the strength of relationships and ability to predict online cyber-security behaviours to estimate human cyber-security strengths and vulnerabilities. Cyber-security behaviours have frequently been researched using the SeBIS Online Security Behaviours Questionnaire (Egelman & Peer, 2015) which captures the engagement in updating behaviour, device securement, password generation and an individual’s proactive awareness to cyber risks. This measure, and to a lesser extent others such as the Employees’ Online Security Behaviour and Beliefs questionnaire (Anwar et al., 2017), have been used with potential individual difference predictors based upon well-researched psychological models of predicting behaviour, attitudes, and intentions including Protection Motivation Theory (PMT - Van Bavel et al., 2019) and Theory of Planned Behaviour (TPB - Ajzen, 2011). Using these above methods, gender has not always been found to be a significant predictor of cyber-security behaviour. For example, whilst men compared to women seem to be more likely to form stronger passwords, engage in updating software more regularly, and proactively search for cyber risk cues in Gratian et al. (2017), no significant gender differences were found in Branley-Bell et al. (2022). Branley-Bell et al. also found older participants were less likely to secure their devices compared to younger participants, but the opposite relationship was found for generating secure passwords, proactive awareness of risk, and software updating behaviour. Aspects of personality such as conscientiousness also arguably predict select cyber secure behaviours (Gratian et al., 2017; Shappie et al., 2020; Posey et al., 2015); and impulsivity, risk-taking attitudes, and some decision-making styles (rational, avoidant, and dependent) have also been found to be significantly related to cyber secure behaviours (Egelman & Peer, 2015).

Attempts have been made to refine predictive models of cyber-security behaviour engagement as some measures are highly correlated across frameworks (e.g., Egelman et al., 2015; Safa et al., 2015; Sommestad et al., 2015). However, there are notable differences in findings between studies that need to be addressed. For example, Gratian et al. (2017) found gender as a predictor of cyber secure behaviour, and higher impulsivity has been found to be significantly negatively correlated to cyber secure behaviours (Egelman et al, 2015). Shappie et al. (2020) found some personality aspects (conscientiousness, openness, and agreeableness) were significantly related to engaging in safer cyber-security behaviours. However, no significant relationships for personality components in the International Personality Item Pool (IPIP - Shappie, Dawson, & Debb, 2020) and Barrett's impulsivity scale (Stanford & Barrett, 1995) were found in Bishop et al. (2020). This could be in part due to different scales and measures used; therefore, there is a clear need to further evaluate these relationships - and in relation to the methodological aspects employed - to assess reliability and validity of findings. With these known predictors of cyber-security behaviour engagement having been thoroughly researched, it was necessary to form research question 2a as there needed to be a comparison of the extent to which time perception and urgency measures could explain behaviour variance when included into a model with known predictors of cyber-security behaviour. It was expected that the introduction of the time perception and self-reported urgency measures with other known predictors into a multiple regression model would explain a significant amount of variance which was not accounted for by the other predictors.

Whilst differences in findings noted in the research critiqued above could be due to variance of some predictors being attributed to other predictors, or low behaviour variance being accounted for in models potentially due to other known significant predictors not included, it is necessary to also consider how the framing of measurements could be having an impact. Previous research in this area (e.g., Bishop et al., 2020; Egelman & Peer, 2015) has involved using 5- or 7- point Likert scales used to collect rank ratings (known as ordinal data). These traditional self-report measures consist of fixed "landmarks" on a scale equally distributed across a scale with a neutral ratings (mid-points) and increments leaning to one extreme or the other (see Figure 15). The data collected using Likert scales can be useful in analysing the variation between participants' ratings. However, having a limited number of responses makes the comparison between the degree of rating extremities in variability less clear. Additionally, having fixed responses equally distributed across a scale could, theoretically, result in participants being more likely to form a central tendency (e.g., gravitating closer to neutral ratings) or provide more extreme ratings due to polarisation to the fixed responses – in turn potentially adding noise to the data set, shifting the data distribution, and impacting analysis findings. Furthermore, different individual difference predictors may have adopted Likert scales with a differing number of gradations (e.g., 5- or 7-points) which if used collectively could introduce bias to the analysis – data collected from scales with more points could be viewed in a greater resolution which too impacts the data distribution and analysis findings.

Figure 15.

An example of a 5-point Likert scale (top) highlighting how ratings may be polarised by fixed landmark responses using red dotted arrows, and an example of a Visual Analogue Scale (VAS – bottom) highlighting the lack of restrictions on ratings with only the extremities being labelled.



One potential solution to address these problems would be to adopt a scale which removes response limits, fixed "landmark" responses, and the resultant data that closer resembles that of interval data rather than ordinal properties – thus increasing freedom of choice. This has been demonstrated by Wu and Lueng (2017) whereby, using simulated data, they demonstrated noise from the data distribution had been reduced and was easier to interpret when there are 11-points on Likert scales compared to scales with fewer points. However, in this instance there still remains the issue of fixed "landmark" responses which could polarise ratings. A potential solution is to adopt the use of Visual Analogue Scales (VAS). VAS are similar in concept to Likert scales, although the only fixed ratings are at the poles of the scale (e.g., 0 to the left, 100 to the right) with a continuous line between (Figure 15) and no visual increments / gradations to subdivide the scale or to indicate the precise rating (i.e., lines to indicate half/quarter marks). Using a VAS, participants mark a point on the continuous line – thus significantly reducing the impact of the framing bias, and data collected would be close to that of interval-scale data (e.g., scales could be framed as 0-100 or at even greater detailed points with decimal points). Theoretically, therefore, the use of VAS, instead of Likert scales, for self-report measures could result in a more valid understanding of relationships between individual differences and cyber secure behaviours as noise from the data could be reduced, and a more accurate representation of ratings could be derived. Consequently, another key question needed to be addressed (RQ2b) to evaluate whether findings calculated from VAS data differed from previous research which used the same individual difference predictors but used Likert scales. Given that there was a possibility the distribution of data could differ depending upon the granularity and whether intermediary labels are utilised in scales, there was also a need to evaluate whether the distribution of data differed due to scale differences (RQ3).

To address the aims of this chapter to investigate the significance of subjective time pressure in comparison with other previously researched individual difference predictors, adopting VAS formats for self-report items, the following research questions were developed:

RQ1: a) Does a behavioural measure of time perception predict cyber secure behaviour?

b) Is a self-report measure of perceived time pressure a reliable predictor of cyber secure behaviour?

c) How do these time individual difference measures compare with each other?

RQ2: a) How do the time individual difference measures compare to

other individual difference predictors?

b) Are findings for individual difference predictors consistent – using VAS - with

previous research?

RQ3: Does the type of scale significantly influence data distribution?

Based upon previous research, it was predicted greater time urgency and underestimations of time passing would significantly predict engagement in riskier cyber behaviours (Alison et al., 2013; De Bona & Paci, 2020; Kim, Alison, & Christiansen, 2020; Trang & Nastjuk, 2021; Williams, Hinds, & Joinson, 2018). Individual difference predictor findings should be broadly similar to findings from previous research (Bishop et al., 2020; Egelman et al., 2015; Gratian et al., 2017), though there was potential for changes in significance due to the inclusion of time urgency and perception predictors for closely associated measures (e.g., impulsivity and conscientiousness) and given the use of VAS where the range of responses is far greater than when using Likert scales. Data collected from scales with more response points was predicted to be closer to being normally distributed (Wu & Lueng, 2017), and noted the significance of contributors to regression models could differ slightly due to changes in distribution as a result of scale type differences.

3.3 - Study 6: Methods

Participants

As G*Power (Faul et al., 2007; 2009) calculations for a medium to large effect size (f^2= 0.15 to 0.35) with a power of 0.8 indicated the minimum sample size required was 113 to 219 given the number of predictors included in analyses (detailed in subsections below), data was collected from 257 participants recruited at random online via Prolific online marketing tool. However, the included measures based upon protection-motivation theory/theory of planned behaviour required participants to be either in employment or education due to the wording of items (e.g., providing ratings in relation to attitudes involving a boss or organisation). Of these 257, therefore, data from 13 had to be excluded as they did not meet the criteria of having been either employed or in full-time education at the time of the study, previously in employment, or in education at the time of study completion. A further 32 datasets were excluded due to missing or incomplete data (i.e., >40% of data from at least one measure), and another 14 were excluded due to significant outlier responses (z-scores above/below +/- 3.29, $p < .001$). The total number of participants included in the analysis was 198 with age ranging from 18-48 years ($M = 24.96$, $SD = 5.96$). Table 5 includes all demographic information collected. All participants were highly proficient in English with it either being their first language or fluent as a second language, normal/corrected-to-normal vision, and completed the observational study on either a laptop or desktop computer. Informed consent was obtained from all participants and upon completion they were fully debriefed and compensated £7.50 for participation. This observational study was approved by the Cardiff University School of Psychology Research Ethics Committee (CU-SREC).

Table 5.

Demographic information for all participants included in the analysis for Study 6.

Demographic characteristic	***n***	**%**
Gender		
....Male	127	64.1
....Female	70	35.4
....Non-Binary	1	0.5
Country		
....Belgium	1	0.5
....Canada	1	0.5
....Chile	5	2.5
....Czech Republic	2	1.0
....Denmark	1	0.5
....UK	14	7.1
....Spain	9	4.5
....Estonia	4	2.0
....Finland	4	2.0
....France	1	0.5
....Germany	5	2.5
....Greece	12	6.1
....Hungary	10	5.1
....Ireland	2	1.0
....Israel	1	0.5
....Italy	19	9.6
....Latvia	1	0.5
....Mexico	7	3.5
....Netherlands	4	2.0
....Poland	39	19.7
....Portugal	42	21.2
....Slovenia	1	0.5
....South Africa	9	4.5
....USA	4	2.0
Education		
....GCSE or equivalent	12	6.1
....A-Levels or equivalent	66	33.3
....Undergraduate degree	74	37.4
....Master's degree	45	22.7
....Doctorate	1	0.5
Employment status		
....Employed	125	63.1
....In education	48	24.2
....Previously employed	20	10.1
....In education and employed	5	2.5
Employment/education category		
....Administration	8	4.0
....Beauty & wellbeing	2	1.0

....Business & finance	12	6.1
....Computing, technology and digital	39	19.7
....Construction & trades	2	1.0
....Creative & Media	10	5.1
....Delivery & storage	2	1.0
....Engineering & maintenance	11	5.6
....Environmental & land	1	0.5
....Government services	2	1.0
....Healthcare	9	4.5
....Home services	1	0.5
....Hospitality	7	3.5
....Law & legal	3	1.5
....Managerial	2	1.0
....Manufacturing	5	2.5
....Retail & sales	13	6.6
....Science & research	9	4.5
....Social care	1	0.5
....Teaching & education	9	4.5
....Transport	3	1.5
....Travel & tourism	4	2.0
....Other	43	21.7
Self-Reported *IT Skill*		
....Poor	4	2.0
....Below average	5	2.5
....Average	63	31.8
....Good	99	50.0
....Excellent	27	13.6
Self-Reported *Security* Training		
....None	45	22.7
....Beginner	68	34.3
....Intermediate	69	34.8
....Advanced	14	7.1
....Expert	2	1.0

Materials/Apparatus

A survey was created and complied online using Qualtrics, consisted first of a series of questions on demographic information: age, highest level of education achieved, gender, employment status, IT skill, cyber-security training, country currently living in, and employment area. The next section provided a link to a time perception behavioural measure (Corvi et al., 2012; Dougherty et al., 2005; Dougherty & Hunter, 2003) created in PsychoPy (Peirce et al., 2019). Once this was opened, the program would appear full screen and following instructions required the spacebar to be pressed when the participant believed 60 seconds had passed since a red flash occurred (lasting five seconds – the length of which was not known by the participants) - indicating the start of the trial. There were five time estimation trials in total, and no feedback was provided. Following sections in Qualtrics were all self-report measures using VAS for items with the same scales (0-100) with a slider to indicate responses. Only extreme responses - 0 and 100 - were labelled and no feedback was provided for which number the slider point responded to when participants moved it along the line, though participants were allowed to rate anywhere in between (and including) the extremities.

The first questionnaire was the SeBIS online security behaviour tool (Engelman & Peer, 2015) consisting of 16 statements divided into four subscales (Updating, Device Securement, Password Generation, and Proactive Awareness). Responses provided reflected how often participants exhibited these behaviours (0 = Never, 100 = Always). Second, participants completed the Chronic Time Pressure Questionnaire (Denovan & Dagnall, 2019) consisting of 13 statements from two subscales – Feeling Harried and Cognitive Awareness of Time Shortage – with ratings representing the thoughts or feelings of the participant for these two aspects of subjective time pressure (0 = Completely Disagree, 100 = Completely Agree).

Third was the International Personality Item Pool (IPIP) questionnaire (Shappie, Dawson, & Debb, 2020) consisting of 50 statements subdivided into five subscales (Extraversion, Openness, Conscientiousness, Neuroticism, and Agreeableness) with responses reflecting the extent to which participants agreed/disagreed statements applied to themselves (0 = Completely Disagree, 100 = Completely Agree). The fourth measure was the domain-specific risk-taking (DOSPERT) questionnaire (Blais & Weber, 2006 – Behaviour engagement only) consisting of 30 statements on risky behaviours subdivided into six subscales (Social, Recreational, Financial, Health/Safety, Ethical) with ratings reflecting participants' likelihood of engaging in these behaviours (0 = Never, 100 = Definitely).

Next was the General Decision Making Style (GDMS) questionnaire (Scott & Bruce, 1995) in which ratings were provided for 25 statements from five subscales (Intuitive, Dependant, Avoidant, Rational, Spontaneous) reflecting the extent to which participants agreed/disagreed with statements (0 = Completely Disagree, 100 = Completely Agree). The Barrett Impulsiveness Scale (Stanford & Barrett, 1995) consisted of 30 statements reflecting how regularly participants had experienced these statements (0 = Completely Disagree, 100 = Completely Agree), and the extended Unified Theory of Acceptance and Use of Technology (UTAUT2) used to assess the acceptance of the internet (Venkatash, Thong, & Xu, 2012) consisting of 30 statements from nine subscales (Performance Expectancy, Effort Expectancy, Social Influence, Trust, Facilitating Conditions, Hedonic Motivation, Price Value, Habit, and Behavioural Intention) with ratings reflecting the extent to which the participant agrees with each statement (0 = Completely Disagree, 100 = Completely Agree).

The final measure consisted of 43 statements relating to cyber-security behaviours, Protection-Motivation Theory (PMT), and Theory of Planned Behaviour (TPB) from nine subscales (McGill & Thompson, 2017; Posey, Roberts, & Lowry, 2015; Safa et al., 2015 – Information Security Awareness, Information Security Organisation Policy, Information Security Experience and Involvement, Attitude, Subjective Norms, Perceived Behavioural Control, Threat Appraisal, Information Security Self-efficacy, Information Security Conscious Care Behaviour) – each rating reflecting the extent of agreement with statements (0 = Completely Disagree, 100 = Completely Agree). Attention checks (e.g., To ensure you are paying attention please rate this as 0) were randomly placed across all measures to ensure attention to items was maintained throughout. Items for all measures were randomised in order, within their respective sections, to reduce inattentive ratings. All items for all measures were given the option to respond as “N/A” if they would not like to respond to a specific item, or if they believed the item was not applicable to them.

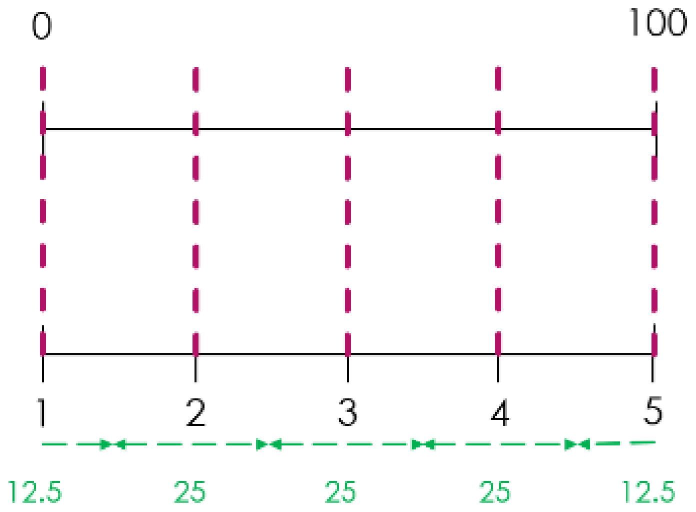
Design

This study adopted an observational design, whereby all categorical demographics (Gender, Education, Employment, IT Skill, Cyber-Security Training, Country Living In, Employment Category) were used to examine differences in ratings between groups for each subscale of cyber secure behaviour (Updating, Device Securement, Proactive Awareness, Password Generation). Age and subscales for all other predictors (Time Urgency, Chronic Time Pressure, Personality, Decision-making Style, Risk-Taking Preferences, Impulsivity, Acceptance of the Internet, Combined TPB/PMT questionnaire) were used in multiple linear regression models to evaluate their relationships with the four subscales for cyber secure behaviour. Mean substitution imputation was used in cases where data was missing for individual difference items to reduce bias.

To examine the differences in regression findings, data distribution, and data normality, a duplicate dataset was created whereby all data collected in VAS were converted into 5-, 7-, 9-, and 11-point Likert scales – see Figure 16 e.g., for VAS to 5-pt Likert 0 to 12.49 (VAS) = 1 (Likert), 12.5 to 37.49 (VAS) = 2 (Likert), 37.5 to 62.49 (VAS) = 3 (Likert), 62.5 to 87.49 (VAS) = 4 (Likert), and 87.5 to 100 (VAS) = 5 (Likert). Demographic comparisons and multiple regression analyses were carried out on the Likert data set. To evaluate normality of data, one-sample Kolmogorov-Smirnov tests were run on the VAS and Likert data sets respectively.

Figure 16.

Visualisation of the VAS (0-100, top) to 5-point Likert scale (1-5, bottom) conversion. Purple dotted lines between scale depict Likert scale ratings being mapped onto the VAS. Green dotted arrows and numbers depict the range of VAS ratings being converted to their Likert equivalents.



Procedure

Upon signing up to the study via Prolific online, participants were provided a link to the Qualtrics survey with instructions and consent form. After providing informed consent, and confirming they were completing the study on a laptop/desktop PC, participants had up to two hours' maximum to complete all measures (demographics, time perception accuracy, chronic time pressure, personality, decision-making style, risk-taking preferences, impulsivity, acceptance of the internet, combined PMT & TBP questionnaire, SeBIS). Average completion time was approximately 45 minutes, and it was not anticipated that participants would require more than one hour to complete the study, although the two-hour absolute limit was set given that it is an online study and participants may choose to take breaks that vary in duration. Once participants had completed all measures, they were provided with debrief information and a Prolific completion code used to receive payment.

3.4 - Study 6: Results

Time Perception Accuracy

To assess time accuracy from the behavioural measure, one-sample *t*-tests were utilised to determine whether the average perception of 60 seconds deviated significantly from 60 seconds passing in reality for each of the trials. From the average estimation of 60 seconds passing across five trials, means ranged from 27.3 seconds to 86.46 seconds (Figure 17). Using a one-sample *t* test, it was found participants significantly underestimated time passing (*t*(197) = -1.999, *p* = .047) by nearly 1.5 seconds when an average is calculated across the five trials (*M* = 58.61, *SD* = 9.81). On a trial-by-trial basis, one-sample *t*-tests indicate the estimation of time passing at trial one participants significantly underestimated time by 2.5 seconds on average (*t*(192) = -3.172, *p* = .002), and by 2.1 seconds in trial two (*t*(193) = -2.435, *p* = .016), but gradually became closer to accurate of 1.5 seconds under a minute at trial three (*t*(196) = -1.751, *p* = .081), one second under a minute at trial four (*t*(197) = -1.159, *p* = .248), and improved to the point of near perfect accuracy of time estimation – 60.04 seconds – by trial five (*t*(194)= .044, *p* = .965 - Figure 18).

Figure 17.

Mean estimation of 60 seconds averaged across five trials in Study 6.

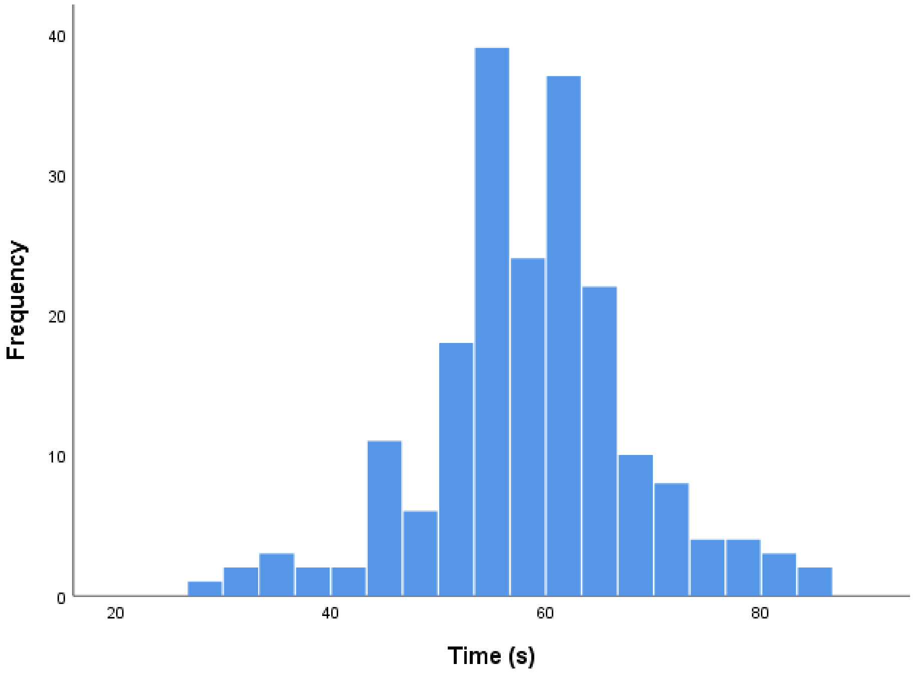
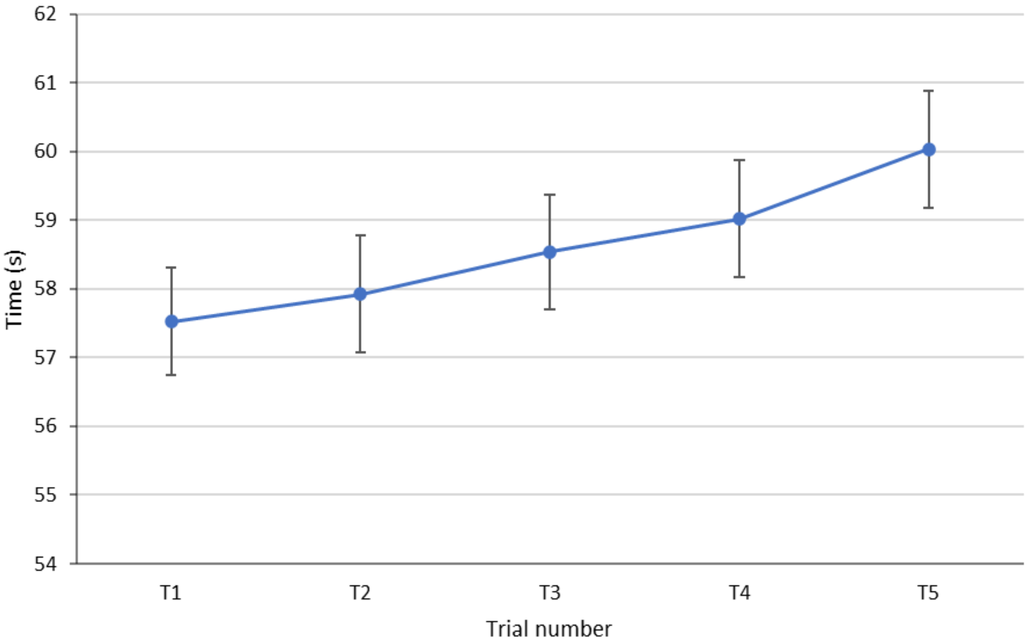


Figure 18.

Mean accuracy of 60 second time estimations over time perception trials in Study 6. Errors bars represent standard error +/-.



Individual Difference Predictors

When analysing for possible differences between demographic information (gender, country, education, employment status, employment category, IT skill, and cyber-security training) and cyber secure behaviours (device securement, updating, password generation, and proactive awareness) it was found proactive awareness was higher in those who were in employment, or in employment whilst a student, at the time of survey completion compared to those only in education or unemployed at time of survey completion, $F(3,194) = 2.69$, $p = .047$, and in those who rated themselves as having a higher IT skill ($F(4,193)= 3.474$, $p = .009$). Upon analysis of the whole sample, no significant differences between gender and cyber secure behaviours were found. However, to account for the imbalance in gender sampling (127 males vs 70 females vs 1 non-binary) 70 males were randomly selected to be compared with the 70 females and it was found there were marginally higher updating scores for men than women ($t(138)= 1.931$, $p = .056$), however the analyses did not reach statistical significance. No comparisons could be made with the non-binary category due to only one participant identifying as such. No other significant differences were found between demographic information and cyber secure behaviours.

Multiple linear regression analyses were employed to examine the significance of all individual difference predictors (age, time perception accuracy, chronic time pressure, personality, decision-making style, risk-taking preferences, impulsivity, acceptance of the internet, combined PMT and TPB questionnaire) in their ability to predict each group of cyber secure behaviours (device securement, updating, password generation, and proactive awareness). From enter regressions, a significant proportion of behaviour variance was accounted for, for all four categories of cyber secure behaviour - 27.5% for Device Securement ($r^2= .275$, $F(38, 159) = 1.587$, $p = .026$), 31.9% for Updating ($r^2= .319$, $F(38, 159) = 1.957$, $p = .002$), 37.5% for Password Generation ($r^2= .375$, $F(38, 159) = 2.512$, $p <$

.001), and 43.5% for Proactive Awareness (r^2= .435, *F*(38, 159) = 3.216, *p* < .001). However, only select subscales were found to be significant contributors to these enter regression models - see Table 6 for overview. Table 6 also demonstrates how regression models and significant contributors would appear if the same participants had theoretically completed the same measures on 5-, 7-, 9-, and 11-point Likert Scale equivalents of the same measures.

Device Securement - The Feeling Harried subscale of the self-report time pressure measure was a significant contributor in predicting Device Securement behaviour (β = .277, *t*(197) = 2.780, *p* = .006), though contributed to the opposite direction predicted – an increase in Feeling Harried predicted more secure cyber behaviour. Adopting a more avoidant decision-making style contributing to predicting riskier behaviour (β = -.183, *t*(197) = -2.561, *p* = .011). Unexpectedly, engaging in more risky health and safety-related behaviours contributed to predicting more secure cyber behaviour (β = .147, *t*(197) = 2.017, *p* = .045).

Proactive Awareness – Engaging in more risky recreational behaviours contributed to predicting less secure cyber behaviour (β = -.160, *t*(197) = -2.720, *p* = .007), whereas increases in performance expectancy in relation to internet use contributed to predicting more secure behaviour (β = .348, *t*(197) = 2.034, *p* = .044). Heightened information security awareness also significantly contributed to predicting more secure behaviour (β = .391, *t*(197) = 2.847, *p* = .005).

Updating – Only information security awareness significantly contributed to predicting more secure updating behaviour (β = .194, *t*(197) = 2.001, *p* = .047).

Password Generation - The Feeling Harried subscale of the self-report time pressure measure was also a significant contributor to predicting Password Generation behaviour (β = .214, *t*(197) = 1.977, *p* = .049); though again contributed to the opposite direction predicted – an increase in Feeling Harried predicted more secure cyber behaviour. Cognitive Awareness of Time Shortness was a significant contributor to the Password Generation regression model (β = -.127, *t*(197) = -2.076, *p* = .039), but in the direction which was predicted – increased awareness of time shortness predicted risker behaviour. Higher conscientiousness significantly contributed to predicting more secure behaviour (β = .171, *t*(197) = 2.522, *p* = .013), as did higher information security awareness (β = .327, *t*(197) = 2.368, *p* = .019) and more positive attitudes towards cyber behaviour (β = .349, *t*(197) = 2.062, *p* = .041).

Table 6.

Enter regression models for all SeBIS cyber-security behaviours across all individual difference measures – for each scale type - highlighting which measures were significant contributors in Study 6.

Scale Type	**Device Securement**	**Proactive Awareness**	**Updating**	**Password Generation**
VAS	**Model** - (r^2= .275, *F*(38, 159) = 1.587, *p* = .026) ***Feeling Harried*** *(β = .277, t(197) = 2.780, p = .006)* ***Avoidant*** *(β = -.183, t(197) = -2.561, p = .011)* ***Health Behaviour*** *(β = .147, t(197) = 2.017, p = .045)*	**Model** - (r^2= .435, *F*(38, 159) = 3.216, *p* < .001) ***Recreational Behaviour*** *(β = -.160, t(197) = -2.720, p = .007)* ***Performance*** *(β = .348, t(197) = 2.034, p = .044)* ***ISA*** *(β = .391, t(197) = 2.847, p = .005)*	**Model** – (r^2= .319, *F*(38, 159) = 1.957, *p* = .002) ***ISA*** *(β = .194, t(197) = 2.001, p = .047)*	**Model** - (r^2= .375, *F*(38, 159) = 2.512, *p* < .001) ***Feeling Harried*** *(β = .214, t(197) = 1.977, p = .049)* ***CAOTS*** *(β = -.127, t(197) = -2.076, p = .039)* ***Conscientiousness*** *(β = .171, t(197) = 2.522, p = .013)* ***ISA*** *(β = .327, t(197) = 2.368, p = .019)* ***Attitude*** *(β = .349, t(197) = 2.062, p = .041)*
11-point Likert	**Model** - (r^2 = .266, *F*(38,159), *p* = .041) ***Feeling Harried*** *(β = .265, t(197) = 2.658, p = .009)* ***Avoidant*** *(β = -.176, t(197) = -2.466, p = .015)*	**Model** - (r^2 = .443, *F*(38,159) = 3.330, *p* < .001) ***CAOTS*** *(β = .117, t(197) = 2.145, p = .033)* ***Recreational Behaviour*** *(β = -.119, t(197) = -2.482, p = .014)* ***Performance*** *(β = .4.01, t(197) = 2.597, p = .01)* ***ISA*** *(β = .294, t(197) = 2.406, p = .017)*	**Model** - (r^2 = .308, *F*(38. 159), *p* = .004)	**Model** - (r^2 = .362, *F*(38,159) = 2.374, *p* < .001) ***Conscientiousness*** *(β = .186, t(197) = 2.689, p = .008)*

9-point Likert	**Model** - (r^2 = .284, *F*(38,159) = 1.657, *p* = .017) ***Feeling Harried*** *(β = .258, t(197) = 2.625, p = .01)* ***Health Behaviour*** *(β = .149, t(197) = 2.036, p = .043* ***Avoidant*** *(β = -.198, t(197) = -2.777, p = .006)* ***Hedonic*** *(β = -.571, t(197) = -2.285, p = .024)*	**Model** - (r^2 = .428, *F*(38,159) = 3.133, *p* < .001) ***Recreational Behaviour*** *(β = -.118, t(197) = -2.446, p = .016)* ***Performance*** *(β = .345, t(197) = 2.268, p = .025)* ***ISA*** *(β = .313, t(197) = 2.531, p = .012)*	**Model** - (r^2 = .313, *F*(38,159) = 1.903, *p* = .003) ***ISA*** *(β = .200, t(197) = 2.048, p = .042)*	**Model** - (r^2 = .363, *F*(38,159) = 2.387, *p* < .001) ***Conscientiousness*** *(β = .163, t(197) = 2.384, p = .018)* ***Feeling Harried*** *(β = .212, t(197) = 1.986, p = .049)* ***CAOTS*** *(β = -.112, t(197) = -2.003, p = .047)* ***ISA*** *(β = .346, t(197) = 2.520, p = .013)* ***Attitude*** *(β = .333, t(197) = 2.007, p = .046)*
7-point Likert	**Model** - (r^2 = .288, *F*(38,159) = 1.689, *p* = .014) ***Feeling Harried*** *(β = .287, t(197) = 2.942, p = .004)* ***Health Behaviour*** *(β = .179, t(197) = 2.479, p = .014)* ***Avoidant*** *(β = -.163, t(197) = -2.374, p = .019)* ***Hedonic*** *(β = -.513, t(197) = -2.130, p = .035)*	**Model** - (r^2 = .419, *F*(38,159) = 3.022, *p* < .001) ***Recreational Behaviour*** *(β = -.119, t(197) = -2.446, p = .016)* ***Performance*** *(β = .331, t(197) = 2.188, p = .03)* ***ISA*** *(β = .277, t(197) = 2.253, p = .026)*	**Model** - (r^2 = .311, *F*(38,159) = 1.887, *p* = .004) ***ISA*** *(β = .193, t(197) = 2.005, p = .047)* ***Subjective Norms*** *(β = -.178, t(197) = -2.026, p = .044)*	**Model** - (r^2 = .365, F(38,159) = 2.405, p < .001) ***Conscientiousness*** *(β = .170, t(197) = 2.527, p = .012)* ***ISA*** *(β = .371, t(197) = 2.740, p = .007)*
5-point Likert	**Model** - (r^2 = .265, F(38,159) = 1.511, p = .042) ***Feeling Hurried*** *(β = .266, t(197) = 2.870, p = .005)* ***Avoidant*** *(β = -.162, t(197) = -2.353, p = .02)* ***ISA*** *(β = .237, t(197) = 1.985, p = .049)*	**Model** - (r^2 = .445, *F*(28,159) = 3.357, *p* < .001) ***CAOTS*** *(β = .123, t(197) = 2.296, p = .023)* ***Recreational Behaviour*** *(β = -.103, t(197) = -2.133. p = .034)* ***ISA*** *(β = .402, t(197) = 3.412, p = .001)*	**Model** - (r^2 = .336, F(38,159) = 2.118, p = .001) ***ISA*** *(β = .196, t(197) = 2.179, p = .031)*	**Model** - (r^2 = .369, *F*(38,159) = 2.443, *p* < .001) ***CAOTS*** *(β = -.130, t(197) = -2.154, p = .033)* ***Conscientiousness*** *(β = .148, t(197) = 2.306, p = .022)* ***ISA*** *(β = .266, t(197) = 2.019, p = .045)* ***Attitude*** *(β = .399, t(197) = 2.464, p = .015)*

Note. ISA = Information Security Awareness, CAOTS = Cognitive Awareness Of Time Stress.

VAS & Likert Scale Distribution Comparison

From running one-sample Kolmogorov-Smirnov tests, the number of self-report subscales found to be significantly normally distributed increasing as the number of points on the scale increases (Figure 19 and Table 7); therefore, indicating VAS data is closer to normally distributed data than Likert data.

Figure 19.

The number of self-report subscales (out of 40) which were found to be significantly normally distributed from Kolmogorov-Smirnov tests in Study 6 across 5-, 7-, 9-, 11-pt Likert and VAS scale types.

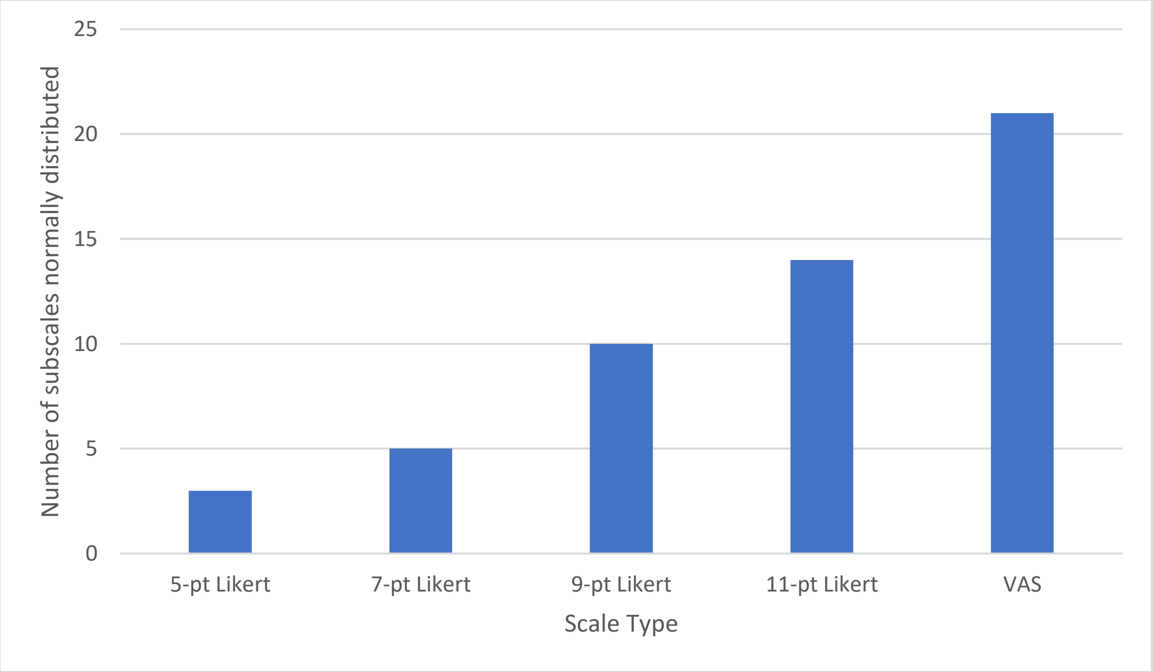


Table 7.

Indications of which self-report subscales were found to be significantly normally distributed in Study 6 from Kolmogorov-Smirnov tests across all scale types.

Scale	Subscale	5-pt Likert	7-pt Likert	9-pt Likert	11-pt Likert	VAS (0-100)
IPIP Personality	Extraversion	✘	✘	✘	✘	✓
	Agreeableness	✘	✓	✓	✓	✓
	Conscientiousness	✘	✘	✘	✘	✘
	Neuroticism	✓	✓	✓	✓	✓
	Openness	✘	✘	✘	✘	✘
Chronic Time Pressure	Cognitive Awareness of Time Stress	✘	✘	✘	✘	✘
	Feeling Harried	✘	✘	✘	✘	✘
DOSPERT	Social Behaviour	✘	✘	✓	✓	✓
	Recreational Behaviour	✘	✘	✓	✘	✓
	Financial Behaviour	✘	✘	✘	✘	✘
	Health Behaviour	✘	✓	✘	✓	✓
	Ethical Behaviour	✘	✘	✘	✘	✘
GDMS	Intuitive	✘	✘	✘	✘	✓
	Dependant	✘	✘	✘	✘	✘
	Avoidant	✓	✘	✓	✓	✓
	Rational	✘	✘	✘	✓	✓
	Spontaneous	✘	✘	✘	✘	✘
Barratt Impulsiveness Scale	BIS-11 Total	✓	✓	✓	✓	✓
UTAUT2	Performance	✘	✘	✘	✘	✘
	Effort	✘	✘	✘	✘	✘
	Social	✘	✘	✘	✘	✘
	Trust	✘	✘	✘	✘	✓
	Facilitating	✘	✘	✘	✘	✘
	Hedonic	✘	✘	✘	✘	✘
	Price	✘	✘	✘	✘	✘
	Habit	✘	✘	✘	✘	✘
	Behavioural	✘	✘	✘	✘	✘
Protection-Motivation Theory/Theory	Information Security Awareness	✘	✘	✘	✓	✓

of Planned Behaviour Questionnaire	Information Security Organisation Policy	✗	✗	✓	✓	✓
	Information Security Experience and Involvement	✗	✗	✓	✓	✓
	Attitude	✗	✗	✓	✓	✓
	Subjective Norms	✗	✗	✗	✗	✗
	Perceived Behavioural Control	✗	✗	✗	✗	✓
	Threat Appraisal	✗	✗	✗	✗	✗
	Information Security Self-efficacy	✗	✗	✗	✓	✓
	Information Security Conscious Care Behaviour	✗	✓	✓	✓	✓
SeBIS	Updating	✗	✗	✗	✗	✓
	Device Securement	✗	✗	✗	✗	✗
	Proactive Awareness	✗	✗	✗	✗	✓
	Password Generation	✗	✗	✗	✓	✓

3.5 - Study 6: Discussion

This observational study, largely consisting of questionnaires with a behavioural element, was designed and deployed to investigate three key research questions: can alternative measures of subjective time pressure be used to predict a broad range of cyber secure behaviours, how do these compare to other individual difference predictors, and does the type of scale self-report individual difference predictors significantly impact the validity of understanding the relationships between predictors and cyber secure behaviours. Some aspects of subjective time pressure measures contributed to predicting specific cyber secure behaviours – though not always in the predicted direction; with some similarities and differences in findings for individual differences and previous research; but also finding the type of scale does have a significant impact upon the normality of data distributions, suggesting Visual Analogue Scales (VAS) could be preferred over Likert scales to improve the validity of our understanding of relationships between individual differences and cyber secure behaviours. Below are detailed discussions for each of these aspects and explore future directions which need to be explored to address the impact of human strengths and vulnerabilities in cyber-security.

3.5.1 - Previously Evaluated Individual Difference Predictors

The role of motivation, measured using the combined TPB and PMT questionnaire (Safa et al., 2015), was noted with some similarities to previous research findings (Bishop et al., 2020). Information security awareness was a significant contributor to predicting proactive awareness, updating behaviour, and password generation. Attitudes to cyber-security was also a significant predictor for password generation, suggesting these specific aspects of motivation are key to understanding the strengths and risks of users in cyber-security compared to other motivation subscales. Despite the significant correlation between cyber secure behaviours and impulsivity noted in initial findings from Study 6 noted in Raywood-Burke et al. (2021) and Egelman et al. (2015), impulsivity was not a significant contributor to predicting any cyber secure behaviours in any of the regression models in Study 6. However, conscientiousness, which also had a significant correlation with select cyber secure behaviours (Raywood-Burke et al., 2021), was found to be a significant contributor to predicting password generation. Engagement in only health- or recreationally related risk-taking behaviours were significant contributors to predicting select cyber secure behaviour, compared to a wider selection of significant relationships found in initial findings (Raywood-Burke et al., 2021), as is observed for acceptance of the internet subscales. From the present study analysis (involving a subset of 70 men and the full sample of 70 women), men appeared to have marginally higher updating scores than women – suggesting gender may only have a small effect upon a specific cyber secure behaviour. This fits in some respects with some previous research that has also found mixed findings on the significance of gender on cyber-security behaviours (Bishop et al., 2020; Gratian et al., 2017; Raywood-Burke et al., 2021). Differences in findings between past research and the present study could be in part due to slight shifts in ratings due to scale differences (VAS vs Likert), and variance being potentially attributed to other measures used (i.e., subjective time pressure measures).

Data within Study 6 was collected from a more internationally diverse sample compared to previous research could also explain potential differences in findings compared to other similar studies (e.g., Bishop et al., 2020). This diversity might mean that findings are more generalisable across other national cultures. One limiting factor, however, of this study is that participants were from the general population rather than specific professions. As some professions may involve different requirements to cyber-security, and involve different work practices and cultures, these types of work cultures may be a further individual difference which was not accounted for within the design or subsequent regression models. When applying this type of research to specific work settings, further work would be needed to investigate the work-place differences including across different work departments within the same organisation(s).

3.5.2 - Likert and Visual Analogue Scales Validity

Building upon the initial findings presented in Raywood-Burke et al. (2021), not only can it be concluded Visual Analogue Scales (VAS) are a valid and reliable method of measuring relationships between individual differences and cyber secure behaviours, but VAS may be preferable over traditional Likert scales that have been used across many previous studies. Data was collected in VAS format and converted to 5-, 7-, 9- and 11-point Likert scale formats to consider how the same participants may have, theoretically, responded to the same measures on this form of scale to consider the significance of scale upon findings, distribution, and data normality. This was to control for the potential for noise to be added to data because of anchoring and adjustment bias when fewer points are provided on rating scales. From using tests of normality, it was found that more VAS scales were closer to normally distributed data than Likert data – with only three out of 40 self-report subscales being significantly normally distributed for 5-point Likert scale data, gradually increasing in number of subscales significant as points on scales increase: VAS having the highest at 21/40 (Figure 19). Whilst this is a theoretical comparison using converted data, this furthers previous research on improving self-report scales (Wu & Lueng, 2017) as it suggests strong evidence for the potential to reduce anchoring and adjustment bias in self-report data; thus, VAS may be more appropriate when adopting self-report measures as it allowed for a finer grained analysis of relationships. Of those subscales which remained not normally distributed regardless of the scale type, this could indicate a natural skewness to those specific psychological concepts, and the manner in which they are being measured. For example, one of the items for device securement – *I use a PIN or passcode to unlock my mobile phone* – on average was rated to be very highly agreed with (*M* = 94.31, *SD* = 19.42); thus, suggesting on average most people engage with this action which makes sense given that the data were collected in 2021 and assuming that such a secure behaviour was engaged in to a lesser extent in the years prior.

It should be acknowledged, however, that both granularity was increased from adopting VAS scales and the removal intermediary labels (i.e., “landmarks”) were adopted for all self-report measures. Therefore, what still remains unclear is whether it is just one or both of these changes which is driving the observed differences. Furthermore, the simulation of grouping VAS data to form Likert scale comparisons does not necessarily reflect how the same participants may have provided ratings for different scales – but only give an indication of what they could potentially do. Further research evaluating the benefits of VAS compared to Likert scales should follow up on these limitations by manipulating granularity and the presence of intermediary labels independently for the same participants to consider what differences may occur in practice.

3.5.3 - Time Perception, Chronic Time Pressure, and Cyber Secure Behaviour

To build upon the gap in research examining the relationship between cyber secure behaviour and subjective time pressure (Chapter 2), the present study included two different methods to assess subjective time pressure to evaluate whether they could be used to predict cyber secure behaviour – a behavioural measure for time perception accuracy (Alison et al., 2013; Dougherty et al., 2005; Kim, Alison, & Christiansen, 2020) and a self-report measure capturing heuristic and cognitive elements of subjective time pressure (Denovan & Dagnell, 2019; Denovan et al., 2023). The regression modelling using data collected in VAS found the cognitive awareness of the shortage of time was a significant contributor in predicting password generation. Whilst this subscale finding supports the hypothesis that increased subjective time pressure would predict riskier cyber behaviour, it only suggests this measure could be a significant contributor to predicting one specific behaviour. In the instance it was a significant contributor – the password generation regression model – the size of the effect was small. Furthermore, the Feeling Harried subscale of the chronic time pressure questionnaire was a significant contributor to password generation and device securement, though in the opposite direction to which was predicted; suggesting the more anxiety and stress derived from subjective time pressure is related to more cyber safe behaviours. These findings for the self-report chronic time pressure questionnaire appear to support very mixed conclusions on the extent to which subjective time pressure could be treated as an individual difference measure to predict cyber behaviours, but there could be at least a couple of explanations for this result.

First, the items in the feeling harried subscale apply to a general/vague scale of time (i.e., could be applied to time management on any day/hour etc.) – meaning responses could more accurately reflect an individual’s reflection of time management overall rather than to a specific time frame or situation. Second, due to the lack of specificity, ratings from both subscales could be more reflective of an individual’s attitudes, values, and self-confidence in relation to time management in general. It could be the case that there is an indirect mediating variable in the relationship between the Feeling Harried ratings and engagement in these cyber behaviours. Feeling Harried ratings could reflect a self-reflection that on average individuals recognise frequent occurrence of feeling of urgency, thus a mediating variable could be individuals may be inclined to anticipate urgency as a result, and subsequently would wish to act in a more conservative, risk averse, manner (concurrent with prospect theory and decision by sampling discussed within Chapter 1). A future line of research into this would be required to evaluate whether this is the case by measuring Chronic Time Pressure ratings, recording expectancy of urgency, and actual behaviour to investigate what exactly might be mechanism between attitudes and behaviour (whilst controlling for confounding variables such as social support in group settings – Nordqvist, Hovmark, & Zika-Viktorsson, 2004).

Regarding the behavioural measure for time perception, it was found that when individuals are asked to estimate when they believe 60 seconds has passed, they tend to underestimate, on average, how much time has passed. This finding appears to align with some previous research in which participants on average would underestimate how much time is needed to complete a task (Roy et al., 2005). There is some research to suggest that individuals overestimate time (e.g., Burt & Kemp, 1994). However, a notable difference is this previous research has examined the estimation of time needed to complete a task prospectively or retrospectively, whereas the present study has examined time estimation in which the only goal was to estimate time passed in real time. Therefore, it is possible findings in previous research differ based on differences in time scale and tasks. In this measure's ability to predicted cyber-security behaviour engagement, however, no significant contributions were found for any of the regression models. Despite this not supporting the hypothesis that an underestimation of time would predict riskier cyber behaviour engagement, contrasting previous research discussed in Chapter 2, the reason why this is may be due to the nature of this measurement of time perception – and by extension the nature of time perception itself.

The current study noted participants began to underestimate how much time had passed by nearly 2.5 seconds on average in the first trial, but by trial 5 they were almost (on average) accurate in predicting when 60 seconds had passed (Figure 18). This suggests that participants may be more time urgent at first, but gradually become less time urgent over subsequent minutes. Though, this uneven pattern of time perception could in part be questioned due to the lack of control from online data collection for known factors which could moderate time perception across much shorter periods of time (e.g., prior exercise and sympathetic nervous system activity – Behm & Carter, 2020, Ogden et al., 2022; exposure to highly arousing negative stimuli – Ogden et al., 2019; perception of speed in the environment – Allingham, Hammerschmidt, & Wollner, 2021; sound and emotive distractions – Symons, Dick, & Tierney, 2023) as well as uncontrolled access to clocks outside of the research programme, therefore explaining why the baseline behavioural time perception measure was not predictive of cyber-security behaviour as the baseline was derived from an average of all five trials. Figure 18 also appears highlight a possible ceiling effect due to the number of trails included, whereby it appears from the pattern across the five trials time perception is gradually dilating but it is unclear whether after trial five people would continue to experience further time dilation to the point of significantly overestimating time perception, or consistently judge time perception more accurately.

Despite these possible limitations there is the possibility this pattern of time perception accuracy is an accurate reflection of time perception over this time period, and thus explain why the behavioural measure used in Study 6 may not be a suitable predictor for cyber secure behaviour engagement. As a result, there was a clear need to evaluate this behavioural time perception measure further to address these limitations using in-person data collection when COVID-19 lockdown restrictions were relaxed (noting again that Study 6 was conducted during a period when restrictions meant that in-person testing was impossible / almost impossible to justify from a risk assessment perspective). The following subsection therefore details the follow up observational study – Study 7 – with discussion around key findings and their relevance to time perception in cyber-security decision making.

3.6 - Accuracy in Time Perception

As outlined in Chapter 2, the subjective perception of time can significantly influence cyber-security behaviour for the worse – likely due to the perception of time passing quicker from environmental cues, or from instilling a heightened sense of urgency to achieve a particular goal through action. This was partially demonstrated in Trang and Nastjuk (2021), whereby an increase in objective time constraint (i.e., reducing the amount of time available to complete a task) lead to heightened ratings of reported time stress – which in turn was related to increases in deviation from cyber-security policies. However, none of the studies in the Chapter 2 systematic review explicitly evaluated how the perception of time lead to an increase in subjective time pressure. This in part is why a behavioural measure of time perception was included in Study 6 in addition to a self-report measure for subjective time pressure. Although, as was detailed from the Study 6 findings, this measure appeared to not be a significant predictor of cyber secure behaviour engagement. In order to address the limitations highlighted in the previous subsection, one must first consider the wider nature of time perception.:

Time passing (the criterion in this instance) consists of intervals following one another moving in a forward linear manner. These intervals could be broken down into measurable units of time (e.g., years, months, days, hours, minutes, seconds, milliseconds) – which, if suitable tools were available and actively utilised, could be used as cues to form a judgement on how quickly time is passing. However, even in instances where suitable tools are available and utilised, other cues can be used as measurements of time intervals. For example, memories can be associated with points in time; and when compared with each other can be used to judge distances in time passing between said events. Though, evidence suggests more often than not the accuracy of time perception judgements in such instances is highly influenced by attention biases attending to environmental cues. For example, in Faro et al. (2005) participants judged the time between presented historical events (e.g., the launch of Sputnik 1, Armstrong's first step on the moon, and the Woodstock Music Festival in 1969), depending upon the perceived causal relations between said events, and found events which were believed to be causally related occurred closer together than non-related events – despite in reality the time distance being the same between presented events. This phenomenon is known as temporal binding – where "the temporal interval between one event and another, occurring sometime later, is subjectively compressed" (Hoerl et al., 2020, p. 1).

On a more granular level (whilst judging events across the space of a few seconds at most), Fereday, Buehner and Rushton (2019) explored time interval estimations between causal and non-causal events and found judgements of time passing to be slower for perceived causal events – with the size of the difference growing with an increase in reference duration (i.e., the duration between the start and end of each trial). Distortions to memories of speed judgements can occur through language manipulation in descriptions of events in instances of memory recollection – so, for example, in cases where the speed of moving vehicles before a witnessed accident is being judged verbs (e.g., crashed, smashed, hit) being used to describe the recollection of the event can impact the estimation of speed of the vehicle (Loftus & Palmer, 1974). When perceiving faster movement in dance recording, participants in Allingham, Hammerschmidt, and Wollner (2021) were more likely to rate the duration of the recordings as lasting longer than recordings of slower movements. However, this was moderated by whether the participants had watched a recording of themselves versus another person, and by watching recordings after acting out the movements compared to just watching the recordings. These findings suggest that experience of movement, and observation of movement can distort perceived duration between time intervals. Exercise and increases in arousal in the sympathetic nervous system has also been found to have small, but significant, reduction in the estimation of time passing (i.e., time appears to pass quicker – Behm & Carter, 2020; Ogden et al., 2022).

Wearden and Ogden (2021) have reviewed research on filled-duration illusions – whereby the frequency and complexity of landmark points between time intervals are being judged can influence perceived duration. The theory behind this research suggested that when there are more landmarks, or more complex occurrences, between time intervals being judged, the longer the duration is perceived to be. Within the review, they outline two different approaches research has adopted to explore this illusion theory – divided-time studies and filled-interval studies. When investigating perceived duration between point A (occurring as the first point in time) and point B (second point in time), divided-time studies would compare and contrast the number of landmarks in between point A and B which could be used to divide up the time. Buffardi (1971), for example, divided up a time interval with up to five dividers using a 1200Hz tone, red light, or stimulation of the participants' finger and found an increase in the number of dividers also lead to an increase in perceived duration: with no significant differences between auditory, visual, or tactile modalities. Filled-interval studies would broadly consist of a comparison of a filled period between time intervals A and B with an empty period. A simple example of this is seen in Meumann's (1896) experimental series four, whereby a continuous sound between two points in time would result in an increased perceived duration compared with two brief sounds indicating the start and end of a time interval of the same period. The broad range of the studies included in the Wearden and Ogden review appear to demonstrate how time perception could be altered over short periods of time.

In summary, along with the other literature discussed above, it is clear a range of variables could influence perceived duration across different contexts and time scales. In Study 6, the behavioural measure for time perception was adopted based up previous literature (Alison et al., 2013; Dougherty et al., 2005; Dougherty & Hunter, 2003; Kim, Alison, & Christiansen, 2020) to calculate and assess time perception accuracy. Participants would be required to estimate the passing of 60 seconds five times, then an average would be calculated to assess whether overall individuals were underestimating, overestimating, or accurate in perceiving time passing. Whilst it was found the average taken from all five trials indicated participants significantly underestimated time passing by 1.5 seconds, one-sample *t* tests utilised on a trial-by-trial basis indicated that the accuracy of time perception changed over time. Consequently, this change in time perception over time could be the reason why an overall average perception of time accuracy may not be a suitable measure for time perception when predicting behaviour.

To address these potential limitations highlighted from the behavioural measure for time perception adopted in Study 6 where data was collected online, and to control for a number of the factors detailed above, a new study was developed. Given the easing of COVID-19 restrictions at the time of development – an in-person testing protocol was possible. The purpose of Study 7 was to investigate whether the accuracy of time perception naturally changes over time, controlling for variables which could influence accuracy: distracting sounds, movements, and activities during estimations of time duration. By controlling for distractions between time estimations, this would also control for the filled-interval illusion. As there is some evidence increased consumption of alcohol (Nuyens, Billiuex, & Maurage, 2021), other recreational drugs (Ogden & Faulkner, 2022), increased sleep deprivation (Sen, Kurtaran, & Ozturk, 2023), and caffeine consumption (Arushanyan et al., 2002) can also significantly alter time perception accuracy; these were also accounted for during data collection. Arushanyan et al. (2002) also noted the time of day could also influence time perception accuracy, thus the study was carried out at the same time of day. A replication the following day at the same time, with the same participants, was also carried out to account for extraneous priming variables, and to assess whether accuracy was maintained after a day.

Based upon the pattern of time perception accuracy from Study 6, it was hypothesised that, when controlling for potential extraneous variables, perceived duration would be underestimated in the first trial but gradually become increasingly accurate over time. If it were found time perception does change over time, then this would imply a behavioural measure using the mean estimation of time perception using multiple 60 second intervals would not be a good predictor of cyber-security behaviours. Subsequently, such implications would suggest research into predicting cyber-security behaviour engagement with time perception should investigate different scales of time, or other measures of stress derived from time (e.g., using heart rate monitoring and skin conductance responses, Ogden et al. 2022). If it were found after controlling for extraneous variables time perception accuracy did not change over time, then this could explain to some extent why the measure was not a good predictor of cyber-security behaviour in Study 6.

3.7 - Study 7: Methods

Participants

Data was collected from 77 Cardiff University Psychology undergraduate students via the School of Psychology Experimental Management System (EMS). Data from five had to be excluded due to unexpected extraneous variables such as sound distractions being present during the study, and a further three were excluded due to invalid responses to the task in session one. A full data set was collected from the remaining 69 participants for the first session, though for the second session the following day four participants did not attend, two were removed due to invalid responses (i.e., skipped through the first trial by mistake), and a further three data sets for session two were removed due to participants having reported consumed significant amounts of alcohol prior to the session. Therefore, 69 data sets were included in the final analysis for session one, and 60 for session two – above the minimum sample size required (n = 34) from G*Power (Faul et al., 2007; 2009) calculations for a medium effect size or greater (Cohen's *d* > 0.5) with a power of 0.8. No other data sets were excluded due to the consumption of caffeine or other recreational/prescribed drugs as there were no significant differences in these variables. No alcohol or other recreational drugs were reported to have been consumed in either session by those included in the final analysis, but caffeine intake calculated from self-reported consumption of caffeine indicated on average consumption was low (session 1: *M* = 14.48 mg, *SD* = 17.10; session 2: *M* = 14.55 mg, *SD* = 18.61). Twelve participants reported having taken prescribed drugs, however these consisted of medications for which there is no previous indication they could influence time perception (e.g., for hay-fever, and antibiotics) so this variable was not considered for analysis. Of the 69 participants which were included in the final analysis, 61 were female (seven male, one prefer not to say), and the mean age was 19.67 years (*SD* = 2.312, Range = 18-36). All participants were highly proficient in the English language with it either being their first language or fluent as a second language, normal/corrected-to-normal vision, and completed the sessions on a desktop computer in a cognitive laboratory. Informed consent was obtained from all participants and upon completion they were fully debriefed after the second session and compensated with course credits (one per 15 minutes of study time) for participation. This study was approved by Cardiff University School of Psychology Research Ethics Committee (CU-SREC).

Materials/Apparatus

A Qualtrics survey was used to collect basic demographic information (age and sex), and self-reported consumption of caffeine, recreational and prescribed drugs. A link to the behavioural time perception measure was included within the Qualtrics survey which took participants to an extended version of the behavioural time perception measure created in Psychopy. This measure was identical to that used in Study 6, with the exception that the version in this study consisted of 10 trials of 60 seconds rather than five. A debrief slide was then included at the end of the Qualtrics survey for the second session only.

Design and Procedure

Participants who had signed up to the within-participants observational study via the EMS were invited to a cognitive psychology laboratory within the School of Psychology at Cardiff University. The laboratory was a quiet computer-based environment, to which only one participant would be tested at a time to avoid distractions to time estimations. Timeslots to sign up to the study session one were consistently made available between 10am and 12pm, with session two occurring the following day at the same time they had signed up for session one. Prior to taking part, all participants were informed they should avoid any significant consumption of caffeine or recreational drugs. In session one, participants were asked to open the Qualtrics survey to provide basic demographic information, and details of caffeine and recreational drug consumption, and to note any prescribed medications they may have taken (to note any which could influence time perception). Participants were then provided with instructions and a link to the behavioural time perception measure to complete in their own time. After completing the time perception task, participants were instructed to come back the following day for session two of the study. In session two, participants reported any consumption of caffeine, recreational drugs, and prescribed drugs, then repeated the behavioural time perception measure, and were then fully debriefed.

3.8 - Study 7: Results

As with Study 6, to assess time accuracy from the behavioural measure, one-sample *t*-tests were utilised to determine whether the average perception of 60 seconds deviated significantly from 60 seconds passing within each of the trials. Analyses for the differences in the accuracy of perceived durations for each trial were carried out for both sessions one and two. In session one, on average no significant deviations (all *p*s > .05) from accuracy for any of the 10 trials were found (Figure 20). However, in session two in the first trial it was found participants would on average underestimate perceived duration significantly by 3.67 seconds (*t*(59) = -2.142, *p* = .036) – significantly lower than trial one in session one as noted by a paired-samples t-test (*t*(59) = 2.074, *p* = .042) - with no significant deviations from accuracy found for the other trials (Figure 21). No other significant differences were observed for perceived direction within trials, or between session one and two.

To account for the amount of sleep (session 1: *M* = 6.86 hours, *sd* = 1.67; session 2: *M* = 6.91, *sd* = 1.60) or caffeine intake potentially influencing time perception accuracy, linear regressions were run for both sessions on a trial-by-trial basis (as well as for the averages across all trials) to evaluate the extent to which amount of sleep might predict time perception accuracy. However, it was found for comparisons that the amount of sleep or caffeine intake did not significantly predict time perception accuracy in any instances (*p* > .05).

Figure 20.

Mean accuracy of 60 second time estimations over 10 time perception trials in Study 7 session one. Errors bars represent standard error +/-.

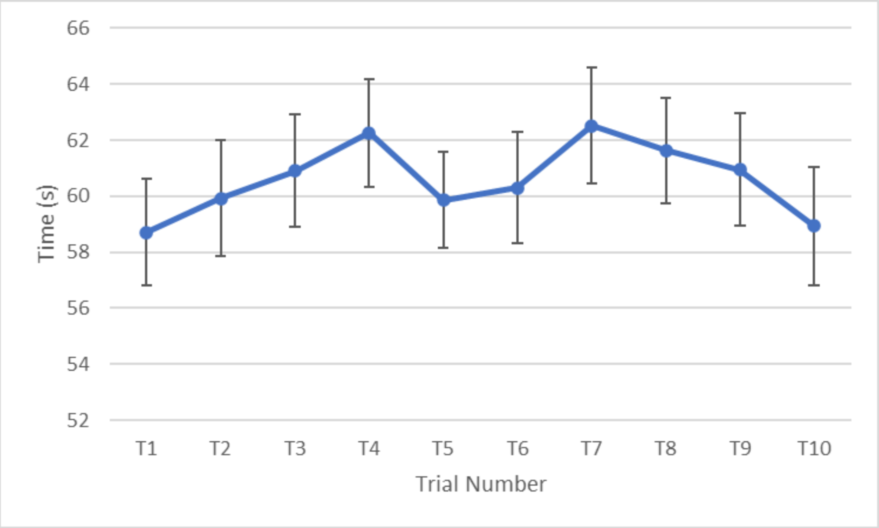
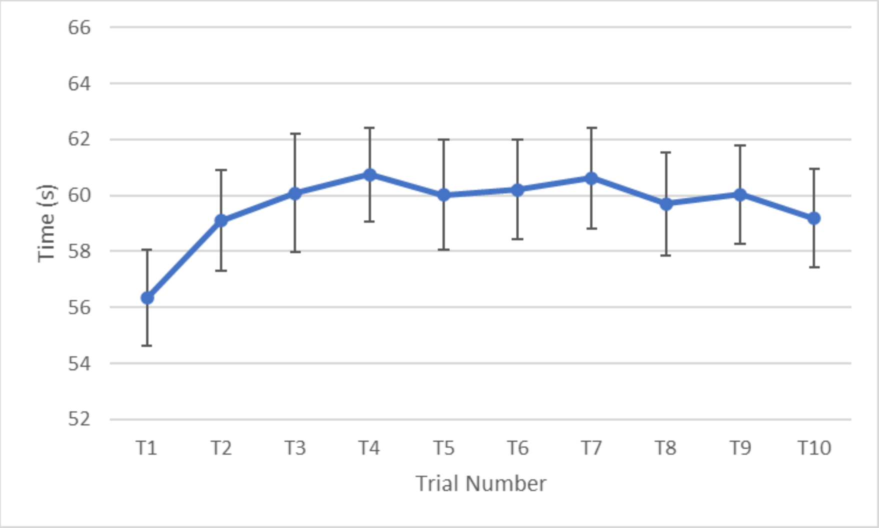


Figure 21.

Mean accuracy of 60 second time estimations over 10 time perception trials in Study 7 session two. Errors bars represent standard error +/-.



3.9 - Study 7: Discussion

The main purpose of Study 7 was to examine the accuracy of time perception estimations when controlling for extraneous variables from an in-person sample compared to the online data set from Study 6 for the same measure (Alison et al., 2013; Dougherty & Hunter, 2003; Dougherty et al., 2005; Kim, Alison, & Christiansen, 2020) which was deployed online. In Study 6, a behavioural measure for time perception accuracy was adopted to investigate the extent to which it could be used to predict a broad range of cyber secure behaviours. In that study, it was found the behaviour measure was not a significant predictor of any behaviours, but one of the reasons for this could be because of the nature of time perception. As the main output of this measure was the mean estimate of time perception from five trials, the mean estimation would be dependent on the performance for each trial. The analyses on each of those trials indicated that participants would significantly underestimate time passing by approximately 2.5 seconds in the first attempt at judging 60 seconds but would gradually becoming more accurate by trial five. This pattern of time perception change over time could explain, therefore, why the mean performance from such a measure might not be a reliable predictor of cyber secure behaviours and that a more granular measure focusing on earlier time estimations of time perception could be better suited.

However, data from Study 6 was collected from an online sample recruited via Prolific; thus, multiple uncontrolled variables (e.g. distractions, consumption of caffeine, alcohol etc.) could have influenced the accuracy of time perception such as the filled-interval illusion (Wearden & Ogden, 2021) whereby intervals such as sound could not only distract but be used to judge the speed of time passing (Symons, Dick, & Tierney, 2023). Study 7, subsequently, was conducted in-person (made possible due to a significant reduction in COVID-19 social distancing conditions) in a controlled environment in two sessions to evaluate whether there was a natural change in time perception over time when accounting for potential moderating variables to explain why such a measure may not be suitable in predicting cyber secure behaviours. Furthermore, the number of time estimations were doubled to account for a potential ceiling effect observed in Study 6 – whereby trial five participants were near perfect on average in estimating 60 seconds passing.

Results from Study 7 indicated that in session one, on average, there were no significant deviations in accuracy estimations of 60-seconds (different to the findings for trials 1 and 2 in Study 6), but in session two, there was a significant underestimation of time passing by 3.67 seconds, although for the first trial of that session only. Time estimations, on average, were closer to 60-seconds in later trials of the second session. Findings from Study 7 provide insight into a few aspects for which answers were sought. First, from extending the number of trials to account for the possible ceiling effect noted in Study 6, it is clear that participants on average maintain consistent accurate estimations of 60 seconds both when tested online (Study 6) and in person (Study 7). Second, the pattern of significance found in session two is coherent, though only for the first trial, with the findings from Study 6. Although, despite some observed underestimation in trial one of session one, no significant differences in accuracy were found. Whilst this only in part supports the hypothesis that time perception is underestimated to begin with but becomes more accurate over time, part of the explanation for these mixed findings could be due to the high level of variance noted in this study.

In Study 7, the amount of variability in estimations of time across all trials, for both sessions, was on average significantly greater than that of the perceived duration estimations for the same measure in Study 6 (*F*(22) = 44.561, *p* < .001 - Appendix D). With greater variability in data, this means that it is harder to determine the significance of differences in perceived duration which on average may be small – thus to some extent explain why observed over/underestimations of perceived duration in session one of up to approximately 2 seconds were not found to be significantly different on average from accurate (sizes of deviations which were found to be significant in Study 6), and why a much larger difference noted in trial one of session two than trial one in Study 6 was significant. With double the variance observed in Study 7 compared to Study 6, this is likely reflective of the differences in online vs in-person data collection as some participants online may have had access to timers/clocks and some may have used these to provide on average more accurate estimations of time.

With this variability in mind – there may be some evidence to suggest that the accuracy of time perception, when controlling for variables which could influence accuracy, changes in the first estimations of time. Subsequently, this could imply that natural differences in time perception over time may indicate why the mean estimation from multiple trials may not be a reliable predictor of cyber secure behaviours. Although, as mixed findings were found between both sessions, future research on this topic could explore the changes in time perception accuracy over first estimations, on a smaller time scale, to evaluate how long it takes to change from underestimating time to accurate perception on average. When examining the extent to which this behavioural measure of time perception could predict cyber secure behaviour, the average estimation across all trials was not a significant predictor. However, in follow-up analyses of data in Study 6 replacing the mean perceived duration estimations with individual trials into regression models, it was found the first estimation of time perception was a significant predictor of password generation (β = 1.688, t(197) = 2.554, p = .012) – indicating people underestimated time perception were less likely to engage in safer password generation behaviours, and those who were more accurate/overestimated time perception were more likely to engage in safer password generation. However, all later time estimation trials were not significant contributors to predicting any behaviours. If this is the case, given that on average it appears there may be some underestimation to begin with, another future direction of this phenomenon could examine whether interruptions and distractions at certain intervals interrupt the pattern of time accuracy of estimations over time (i.e., does time estimations *reset* to underestimation after an interruption/distraction? – Zijlstra et al., 1999). Additionally, if on average underestimation was found due to these interruptions/distractions, would each time estimation for each trial after interruptions/distractions be a significant predictor of cyber secure behaviour engagement?

Although carrying out Study 7 in-person allowed for the control of multiple possible confounding variables such as sleep quantity (Sen, Kurtaran, & Ozturk, 2023) – further research could be done in this area to investigated factors which still could not be controlled in the paradigm adopted. Whilst no significant differences were found between the amount of sleep participants had between sessions, sleep quality could not be controlled for. The use of a polysomnogram – the systematic process of collecting physiologic parameters of sleep such as EEG activity and electric-oculograms (Rundo & Downey, 2019) - in future research examining time perception and sleep quality could be adopted to measure whether differences in quality predict time perception differences. However, practical limitations (i.e., increased time of study length, extra costs) of such methods mean only smaller sample sizes could be realistically recruited.

A final, but critical, limitation to highlight is the extent to which the behavioural measure of time perception accuracy (Alison et al., 2013; Dougherty & Hunter, 2003; Dougherty et al., 2005; Kim, Alison, and Christiansen (2020) reflected *urgency* as claimed by these authors. There is not a clear understanding from using this measure alone on the mechanisms behind time estimations. It could be the case that if an individual is feeling more urgent, they may be more eager in any decision-making scenario to make an earlier response to a decision (or chain of) – but what comes first: the underestimation of time passing, or the motivation for urgency? Would an individual feel motivated to respond urgently, and as a result underestimate time passing as an outcome, or might an individual initially underestimate time passing, and this subsequently motivates a greater sense of urgency? Whilst the measure of time perception could still be a measure of time urgency (i.e., extraneous cognitive load), this lack of mechanism clarity means it is not sure whether the data output is an input or an output of the decision-making process. Consequently, it may be more accurate to describe this as a measure of time accuracy rather than one of urgency.

To conclude, as it is unclear from the findings of Study 6 and 7 that this behavioural measure for time perception can predict cyber secure behaviour, future research could explore whether there is a unidirectional or bidirectional relationship in time perception and urgency. A suggestion for this topic of research could be to determine ways of manipulating known variables to influence time perception (e.g., sleep deprivation - Sen, Kurtaran, & Ozturk, 2023) and urgency (e.g., use of time urgency cues in emails – De Bona & Paci, 2020) and record changes. In other words, from manipulating time urgency and recording changes in feelings of urgency, and vice versa, the significance of outputs could give an indication on the directionality of relationships between these two factors. As this suggestion would not directly address the key aims of the thesis, i.e., to examine the impact of cognitive load and time in cyber-security decision making and find ways to reduce risk, the final chapter direction explored the previously unaddressed significance of context and methods of measuring risk in cyber-security decision making highlighted in Chapter 2.

3.10 - Chapter 3 Summary

This chapter focussed on a need to examine the relationship of subjective time pressure with a broader range of cyber secure behaviours and evaluate the extent to which variance in time perception and urgency could explain cyber secure behaviour engagement established in the systematic review from Chapter 2. Time perception and urgency measures were compared a) with each other, and b) with other known cyber secure behaviour predictors in Study 6 across a range of behaviours to address this. Study 6, largely reliant upon self-report Likert measurements, also provided the opportunity to investigate the use of VAS and their potential to improve the validity of findings through ratings being theoretically less susceptible to anchoring and adjustment bias.

From the research reported within this chapter, several novel findings have been noted. First, that even though models used to predict a range of cyber secure behaviours account for significant proportions of behaviour variance – there was only a limited contribution from subjective time pressure measurements to these regression models. For the self-report measure from the Chronic Time Pressure Questionnaire, findings conflicted in the direction of significance (with cognitive awareness of time pressure being associated with riskier password generation behaviour but feeling harried being associated with safer password generation and device securement behaviour) could be due to a lack of reference to a particular time scale.

Second, the mean perceived estimations from the measure of time perception accuracy, estimating 60 seconds passing several times, was found not to be a significant contributor to predicting any cyber secure behaviour. However, from examining the nature of time perception accuracy on a trial-by-trial basis in Study 6, and the follow up of time perception accuracy in Study 7, the reason this could be is because of how time perception may change over time for first estimations – with perceived duration estimations in Study 6 and session two of Study 7 indicating significant underestimation of time in the first trial, but become closer to accuracy on average over time. These findings, as discussed in previous subsections, would suggest that these measures may not be suitable as a way of examining individual differences in subjective time pressure. Consequently, future investigations of individual differences in subjective time pressure and cyber secure behaviour needs to include measures which are in reference to a particular time scale and consisting of initial estimations of time passing in conjunction with distracting/interrupting variables in a cyber-security context.

Third, theoretically, if the same participants who provided VAS ratings for all self-report questionnaire subscales in Study 6 theoretically were to provide answers on Likert scales, it was suggested through converting data that scales with fewer rating points would have greater noise. This increase in the noise within the data would result in more subscales not being normally distributed, and that responses limited to fewer points on a scale could introduce more anchoring and adjustment bias to responses – thus findings would be less representative of the relationships in reality between individual differences and cyber secure behaviours. It is worth noting, however, that as this was a theoretical comparison between scale types rather than comparing real participants' data across all scale types that this simulated scale comparison indicates the worst-case scenario of anchoring and adjustment bias. Future work investigating the influence of anchoring and adjustment bias in scale types should compare and contrast how in reality the same participants might provide responses to self-report items which have either VAS or Likert scales to determine the precise extent to which anchoring and adjustment can alter responses being provided.

Fourth, regression models in Study 6 indicated a significant proportion of cyber secure behaviour variance can be accounted for (from 27.5% for device securement to 43.5% for proactive awareness). Whilst these overall models are significant, only select subscales appear to be significant contributors (notably information security awareness from the combined PMT/TPB questionnaire). Combined with the knowledge that between 56.5% and 72.5% of behaviour variance was not accounted for (depending upon the cyber behaviour in question), there may be many more significant variables which could predict behaviour need to be accounted for. Furthermore, as the self-report ratings for individual differences predictors were being compared with self-report ratings for engagement with cyber secure behaviours – what is ultimately being examined is how prior attitudes and intentions can predict intentions of behaviour. Whilst these findings are useful in indicating which attitudes and intentions may be noteworthy in attempts to develop personas (i.e., groupings of significantly related strengths and vulnerabilities) which could be created for organisations, helping better target human factors cyber-security support interventions for particular types of people, actual behaviour may differ in reality. In the next chapter, therefore, the main focus returns to investigating actual behaviour change, but in the context of cyber-security, due to subjective time pressure to address the third and final outcome from the Chapter 2 systematic review: phishing email context needs to be considered in investigating the success of urgency as a persuasion technique.

Chapter 4: Urgency and Persuasion in Phishing Susceptibility – Why Context Matters

4.1 - Overview

As was highlighted from the systematic review into the role of subjective time pressure in cyber-security (Chapter 2), a significant proportion of research on this topic has focused on the significance of time urgency cues within emails – e.g., text within email indicating the need to respond within the next 24 hours. Eight behavioural studies such as De Bona and Paci (2020) and Cui et al. (2020) demonstrated that when these cues were included within phishing emails, people were significantly more likely to respond to them. However, the degree of phishing susceptibility appears to vary between studies when time urgency was compared with other persuasion techniques (e.g., pretending to come from a source of authority – Bishop, Asquith, and Morgan, 2022).

To be able to more precisely pinpoint where susceptibility may lie regarding the success of phishing email techniques, this chapter will describe the extent to which phishing emails pose a threat to cyber-security, how persuasion techniques (with a focus on subjective time pressure) can be adopted within phishing emails to increase phishing susceptibility, and how decision-making biases relating to attention to context can be exploited to increase phishing susceptibility. A novel experimental paradigm was created for three experiments (Study 8, 9 and 10) adopting a mixture of self-reported utility of outcomes, phishing estimations, and behavioural measurements of phishing susceptibility to broaden the understanding of how context can significantly influence the success of phishing email techniques – and how a tool from this data could be developed to support phishing simulations. However, in order to account for the complexities of persuasion techniques, and the context of the email in which they are in, the novel paradigm needed to account for both the significance of both of these factors combined based upon the extensive research to date on persuasion in phishing susceptibility. Through capturing data more than just behavioural responses to emails, this could highlight where the weight of cyber-security risk may lie within the decision-making process to respond/not respond to emails, and therefore guide the focus on phishing susceptibility training. The following subsections review of the threats both persuasion and context pose the phishing susceptibility, providing a justification for why a complex, but informative, experimental design was necessary to account for both factors simultaneously.

4.2 - Phishing Email Risks in Cyber-Security - and The Art of Persuasion

To understand the risks to cyber-security through phishing email attacks, first it is important to note how phishing tactics have changed over time to explore why people may be falling susceptible to this type of cyber threat in the present. One tactic cyber criminals may choose to adopt is that of mass phishing, whereby phishing emails are designed to be sent to as many people as possible. However, in more recent years Proofpoint (2020) has noted more of a tendency for phishing emails to focus more on the quality of phishing emails rather than the quantity. This quality approach to email phishing is known as spear phishing where the email is tailored and targeted towards specific individuals, businesses, or organisations which has been found to have been increasingly reported in recent years (Griffiths, 2023). Although reports such as Valimail (2021) indicate only approximately 1% of global emails are malicious, phishing accounted for almost 40% of all breaches – and approximately 94% of malware being delivered through email (Verizon, 2022). Despite Verizon detailing that reporting of phishing emails has risen from about 4% in 2016 were being not clicked, rising to roughly 12.5% in 2021, the percentage of people who click on phishing emails has also risen from approximately 3% in 2016 to almost 10% in 2021.

Whilst tools such as Domain Message Authentication Reporting and Conformance (DMARC) can be adopted to reduce the number of spoofed emails by restricting where emails can be received from (Stilgherrian, 2018), such tools still have limitations in their ability to prevent successful phishing email attempts. First, tools which screen emails require criteria on which emails should be allowed to come through – thus despite some learning and altering of protocols occurring, it is still possible for phishing emails to slip through the filter process. Second, even the most extreme protocols which can prevent all external emails from a domain cannot rule out insider threat. Third, once a user has received an email there are a multitude of variables which can influence the likelihood of choosing to respond/not respond which are not good indicators of whether the email is genuine or phishing – some of which are the focus of the current chapter.

As discussed in Chapter 1, the quality of a decision could be determined by the framework of decision making in the given circumstances, the perceived probability of producing the most desirable perceived outcome, and the quality of the information available being utilised within the decision-making framework. However – to what extent is good decision-making within the control of the decision maker, and how much is due to the environmental context? The weighting of these points could determine where the most appropriate intervention is needed. In the context of phishing emails, language use could be significant factor in the decision to respond to emails. Greeno et al. (2022) is an example of an attempt to create a cyber-security language repository to aid the mutual understanding of commonly used terms. The researchers conducted two studies (one with the general population and another with people who reported to work within technology driven areas) where participants rated cyber-security words and phrases across a number of dimensions from familiarity to semantic properties, with the outcome being a normed database with over 700 words and a number of phrases. A better understanding of cyber-security language could in part help aid the quality of communication between individuals over email, but how language can be crafted to appear authentically written could also increase the risky likelihood of replying to phishing emails on the basis they appear more appealing (as has been noted in the visual appeal of websites – Stojmenovic et al., 2022). Subsequently, persuasion techniques adopted within the text of spear phishing emails pose a serious threat to cyber-security This final point relates to a particular threat in recent years with the capacity to use artificial intelligence (AI) to generate targeted phishing emails much faster than before. Whilst there are current methods underpinned by machine learning being developed to analyse and prevent AI-based phishing attacks (e.g., Eze & Shamir, 2024), subtle and more nuanced tactics which adopt persuasive techniques may be less easy to detect.

Cialdini (2009) has extensively defined and researched major persuasion techniques: *Authority* (people perceived to have perceived authority/expertise, or use authoritative language), *Scarcity* (the less there is of something the more people tend to want it), Reciprocity (if it is believed something is owed, there is a social obligation to return something to achieve balance), *Commitment and Consistency* (the need to behave consistently with one’s sense of self-image), *Liking* (people tend to believe likeable others compared to those they do not like), and *Social Proof* (the need to confirm with norms of the context). These persuasion techniques have often been utilised by phishers to increase the likelihood of users responding to malicious email content, though some persuasion techniques have been found to be more successful in increasing responses than others. Authority, for example, has been indicated to be one of the more successful techniques consistently (Akbar, 2014; Butavicus et al., 2015; Williams, Hinds, & Joinson, 2018) – yet one of the most reported for phishing by Airbus employees (Bishop, Asquith, and Morgan, 2022). Scarcity, on the other hand, has had inconsistent findings – with Bishop, Asquith and Morgan finding scarcity was the second most successful persuasion technique when students were asked to indicate whether they would respond to emails; but in other instances, it has been found to be one of the least successful (Lin et al., 2019; Parsons et al., 2019). Bishop, Asquith, and Morgan (2022) also indicated all other persuasion techniques were less successful than emails which did not contain any other persuasion technique.

There are a few things to note here. One reason inconsistencies in the success rate of the scarcity persuasion technique could be due to it being very broadly defined – scarcity through the lack of information, a limited offer, or a restriction on perceived time instilling a sense of urgency could all differ significantly. De Bona and Paci (2020) investigated the response rates to emails which contained authority or time urgency cues in attempts to increase response rates, and found not only did phishing emails with authority have high response rates, but emails containing time urgency cues (i.e., detailing the need to respond within a fixed period of time) had even higher response rates than authority emails. Why, therefore, might the success rates of phishing email techniques vary? This could be in part due to the context of the email – i.e., the subjective utility of replying or not replying to an email could depend upon the perceived potential outcomes for said email. The utility of replying/not replying to an invitation to attend an academic or industrial conference may not be equal to that of an email describing the need to change a password to avoid losing access to work-related folders in a shared online area. In turn, the utility of these decisions may not be the same as an email requesting for the review of payroll details to check for errors. As the weighting of perceived outcomes could vary due to the nature of the email – not just the adoption of persuasive language – this could explain the difference in success rates across previous literature. This is why an experimental approach, as utilised in the literature discussed above, to evaluate these factors was deemed to be the most appropriate for the studies in this chapter. As causal relationships can establish more definitive conclusions, these could better inform how email phishing susceptibility could be targeted in more granular detail to improve decision making quality. These comparisons could then be easily reflected upon previous literature to clearly indicate overlaps in findings.

Given that the significance of how the context of emails, specifically their associated subjective utility of outcomes (e.g., from choosing to respond or not respond to them), could influence phishing susceptibility had not been previously considered thoroughly in the literature to date, this needed to be a clear focus reflected within the design of the next studies. However, examining different contexts of email, and how they may differ in outcome, as a single manipulation is not enough to consider when trying to address phishing susceptibility. Given the literature on phishing susceptibility discussed above, and from Chapter 2, there is overwhelming evidence that the use of persuasion techniques are both common and successful in increasing phishing susceptibility. Examining either persuasion technique or email context in isolation ignores how these two factors may simultaneously cause differences to phishing susceptibility. Both factors could influence the quality of decision making in the similar fashion because in both cases contextual information is being manipulated. Persuasion techniques could enhance or diminish the perception of the outcomes to responding or not responding to emails, but the extent to which they can do this could be specific to different contexts. The differences and variance in the success of persuasion techniques in previous phishing literature (Akbar, 2014; Bishop, Asquith, and Morgan, 2022; Butavicus et al., 2015; Lin et al., 2019; Parsons et al., 2019; Williams, Hinds, & Joinson, 2018), therefore, could also be a reflection of the multitude of email contexts across studies in which persuasion cues are embedded. Consequently, in order to provide a more granular understanding of the threats phishing susceptibility can pose, the experimental paradigm needed to assess both the manipulation of persuasion techniques and wider email contexts which may differ in decision outcome utility.

Reflecting upon this discussion in light of Brunwik's lens model (1956) discussed in Chapter 1 (see Figure 2), how could the inclusion of persuasion techniques and the subjective utility of perceived outcomes influence the quality of decision making? First, the perceived pressure to respond more urgently could alter the framework adopted to form judgements (e.g., a simplified quick and easy assessment of limited information rather than a slower but more complex, thorough analysis of information available). Second, text content to emails could bias attention to variables which could influence judgement but are not valid or reliable indicators of whether the email presented is genuine or phishing – thus the quality of information included in a decision analytical framework could be compromised. Third, because of attention bias on some cues to determine whether an email is genuine or phishing in light of the perceived subjective utility of responding/not responding to the email, this could influence the desirability of different outcomes – and subsequently could result in different behaviours. For example, an individual views an email requesting the need to update a password for a work account to maintain access to it, but is requested to change it before the end of the day: In this instance there could be a risk the link indicated to click on to change the password is malicious, but if attention and value is placed upon the need to respond urgently in order to maintain a perceived priority (i.e., maintain access to the work account) the judgements formed when viewing this email could skew the perception of safety, and consequently could be inclined to engage in the request.

Considering previous literature from the Chapter 2 systematic review and broader literature around persuasion in phishing has not thoroughly investigated (to the researcher's knowledge) the expected utilities of outcomes when controlling for subjective risk probabilities – these dependant variables are precisely what the following final studies aimed to include. As discussed in Chapter 1, behaviour is not the only aspect of whether a decision is a good or bad decision – it is necessary to consider the prior motivations, attitudes, and beliefs which can lead to the behaviour. Many phishing email simulations – such as MetaCompliance (2023) and TitanHQ (2023) – are behavioural intervention tools, indicating click rates in phishing simulations, which depend upon behavioural input to address through repeated use to indicate to users how to identify phishing emails. However, Brunken et al. (2023) highlights that there needs to be an effective balance of simulation support tools and productivity, with their example indicating the hidden costs such as the effort for different stakeholders taking part in simulations costing at least €50,000 in person hours. A tool, framework, or paradigm which could account for key aspects of the beliefs and values which may motivate behaviour could have to potential to better highlight, or diagnose, where risk may lie within phishing susceptibility decision making – but also needs to maintain the optimal balanced between practicality and productivity.

Bax, McGill, and Hobbs (2021) attempted to address this issue by investigating how rewards and response costs can influence phishing email response behaviour in the context of Protection-Motivation Theory (PMT). This theory (Rogers, 1983) suggested that an individual's response to a potentially threatening situation will likely depend upon an evaluation of the perceived threat to themselves (threat appraisal) and their perceived ability to manage the threat (coping appraisal). Bax, McGill and Hobbs' (2021) hypothesis to the applied model of PMT was that the costs to responding to potential phishing emails and the perceived rewards could not only motivate people to engage in behaviour designed to protect the individual but could also result in maladaptive behaviour (whereby a reduction in fear is reduced but the danger posed by the threat is not). They assessed these hypotheses (H7 and H9 within the paper) by providing a list of items, the majority of which were developed by the researchers, to measure different aspects of PMT – namely perceived severity of the threat, perceived vulnerability of oneself, perceived rewards, perceived response costs (e.g., monetary, time, effort). Response efficacy - an individual's assessment of the efficacy of the recommended response to the threat, and self-efficacy -an individual's beliefs on how successfully they will be able to execute the recommended protective behaviours. The researchers were able to establish higher perceived rewards and response costs self-report ratings were predictive of higher self-reported maladaptive phishing email behaviour engagement. However, whilst motivations and beliefs are clearly being evaluated within this study, self-reported motivations are being assessed against self-reported behaviour engagement which is not specific to an email context – i.e., items for maladaptive behaviour indicate motivations for engaging in behaviour with no specification on the type of email. This limits conclusions because there is not a clear link between motivation had behaviour engagement on the basis of differences in perceived utility of responding/not responding to specific types of emails.

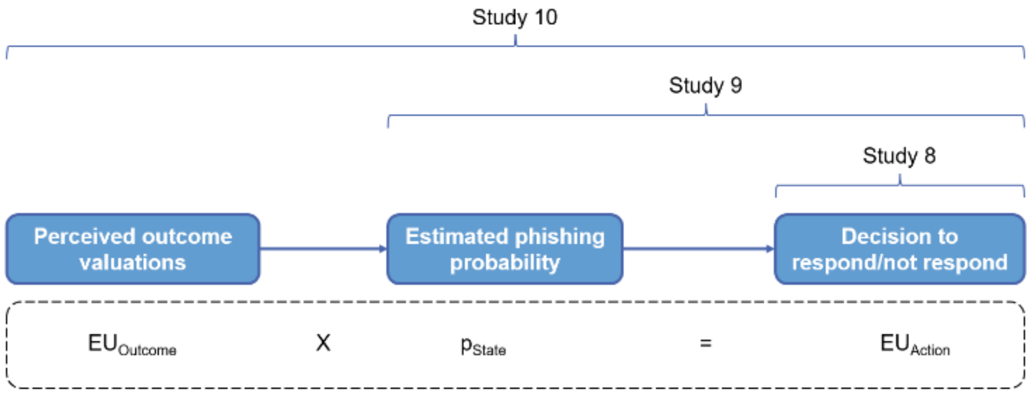
A novel application of the Expected Utility Theory (EUT - Von Neumann and Morgenstern, 1953), therefore, was explored which incorporated the perceived utility of outcomes and the likelihood of risks occurring to indicate the utility of decision-making options. As discussed in Chapter 1, the original intention of the framework to indicate how people should make *rational* decisions was flawed as outputs would not accurately reflect *actual* decision making due to assumption violations (e.g., transitivity). However, from collecting both estimations of outcome utilities and perceived probabilities prior to actual behaviour, comparisons could be made to evaluate the extent to which the EUT framework using subjectively derived data would explain actual behaviour. Alternative to suggesting how people *should* make *rational* decisions for decisions which have not yet been made, this retrospective adoption, if accurate, could act as a tool to aid metacognitive reflection – i.e. to encourage reflection upon where the weight of risk comes from within judgement formation for decisions which have already been made.

4.3 - Evaluating Phishing Susceptibility: How Email Context Influences the Impact of Persuasion Techniques

To address the issues discussed above, a newly developed paradigm was adopted for the final three experiments (Studies 8, 9 and 10) to incorporate the combination of perceived outcome utilities, judgements of risk probability, and actual behaviour to evaluate where the weight of phishing susceptibility lies as a result of persuasion techniques and email context (see Figure 22 for an overview). The purpose of developing these experimental studies was threefold: First, to provide insight into how persuasion techniques within differing email contexts may interact simultaneously in influencing phishing susceptibility on a more granular level. Specifically, this would involve evaluating whether differences exist for both persuasion technique and email context. Second, to evaluate whether prior beliefs and values prior to decision making are useful additions to behavioural measurements in assessing phishing susceptibility. Third, from a combination of expected utilities of decision outcomes and estimations of phishing probabilities, the extent to which the Expected Utility Theory (EUT) framework could provide a successful basis to predict actual behaviour was assessed to understand to its potential to highlight where decision making risks may lie in phishing susceptibility.

Figure 22.

Overview of Studies 8, 9, and 10 – and how data collected forms an expected utility (EU) framework for evaluating user susceptibility to phishing.


Study 10
Study 9
Study 8
Perceived outcome valuations
Estimated phishing probability
Decision to respond/not respond
$EU_{Outcome}$
X
p_{State}
=
EU_{Action}

Note. *$EU_{Outcome}$ = Expected Utility to specific outcome. P_{State} = Probability estimation to specific state – i.e., whether an email is genuine/phishing. EU_{Action} = Expected Utility value for a specific action – i.e., respond or not respond to an email.*

Study 8 consisted of an experiment whereby participants would be expected to choose to respond or not respond to presented emails containing different persuasion cues across a variety of wider email contexts. This was to assess, from a behavioural perspective, whether behavioural differences may occur due to both manipulations in persuasion technique and email context. Study 9 expanded upon this by requiring participants, prior to making a decision, to estimate the likelihood the presented email is genuine or phishing. The introduction of this additional measure was to indicate what benefit estimations of risk probability could have when assessing phishing susceptibility for the study manipulations; with the addition of comparing whether repeated prior measurements impacted behaviour when compared with findings from Study 8. As highlighted by the discussion in the previous subsection in relation to Brunken et al. (2023), there was a need to assess this potential impact as to whether this approach would indicate the optimal balance between the usefulness and productivity cost to completing more measures, or whether more measures might be counterproductive both in burden to complete, and the influence repeated measures have on behaviour. Due to the increase in risk salience from including more repeated measures prior to decisions, it was predicted this could alter the perception of risk, resulting in a changes to the likelihood of choosing to respond across all conditions.

Study 10 then built even further upon Study 8 and 9 by included measures of expected utility to indicate the extent to which individuals would subjectively value the positive (or negative) consequences of replying (or not replying) to a particular type of email on the belief that it was genuine (or phishing). As the systematic review (Chapter 2) revealed a lack of research examining the relationship between objective and subjective time pressure in cyber-security contexts – with Trang and Nastjuk (2021) being the only example to demonstrate this relationship in information security non-compliance – objective time pressure was considered as a third manipulation in Study 10. Whilst this added an additional level of complexity to an already complex experimental paradigm, it was also an opportunity to evaluate how objective time pressure may compare to subjective sources of time pressure in the context of email phishing (i.e., urgency cues) – previously unexplored as highlighted above. Based upon the literature reviewed in Chapter 2 and other works (e.g., Chowdhury et al., 2019), it was expected that as the amount of time allowed to decide to respond or not respond to an email became more limited, participants may be more likely to make riskier decisions – which in this case would consist of choosing to respond to presented emails. If differences were found between levels of objective time pressure, then comparisons were planned to investigate whether differences in objective time pressure also interacted with the persuasion techniques included within different emails contexts. Specifically, it was of interest to see whether time urgency as a persuasion technique increased phishing susceptibility to the same extent that objective time pressure might. With the dependant variables consisting of data which could fit into the EUT framework, and actual behaviour also being collected, the main focus of Study 10, however, was to see the extent to which the framework could be used to predict actual behaviour and form the basis for a phishing susceptibility tool.

As authority and scarcity have been noted to be the more successful on average (Akbar, 2014; Bishop, Asquith, and Morgan, 2022; Butavicus et al., 2015; Lin et al., 2019; Parsons et al., 2019; Williams, Hinds, & Joinson, 2018), the success of these persuasion techniques was focused upon across a broad range of email contexts. However, as scarcity has been defined too broadly in the context of phishing email research (and subsequently a potential reason why inconsistent findings have been found previously), for the purposes of the final three studies, scarcity was divided into two separate persuasion techniques: time urgency (i.e., scarcity of perceived time available) and scarcity of quantity (i.e., the less there is of something, the more people want it – such as a limit offer).

Across Studies 8, 9, and 10, it was predicted participants would be more likely to respond when presented emails contained at least one persuasion technique investigated and become even more likely if more than one technique was used. Although, it was expected there could be differences between response rates to persuasion depending upon the email context. As these studies, to the researcher's knowledge, appeared to be the first of their kind to consider a range of persuasion techniques across multiple email contexts in a controlled setting, there was little basis to determine the direction of differences between expected utility and probability ratings – but what differences may have occurred due to these manipulations of persuasion technique and email context were explored. Ratings of expected utility and phishing probability would be collected and calculated to evaluate the extent to which these measures equated to actual behaviour. The below subsections detail the variations in the experimental paradigm across the three studies, including a breakdown of key findings and collective discussion. The key research questions, developed considering the key purposes of these studies, were as follows:

1) **How successful are known persuasion techniques across different types of emails contexts?**
2) It was predicted that behavioural responses in Studies 8, 9, and 10 (i.e., choosing to respond/not respond) and probability estimations in Studies 9 and 10 (i.e., the extent to which emails were judged to be genuine/phishing) would differ significantly depending upon which persuasion techniques were adopted in different contexts. However, as these two manipulations combined had not previously been researched, to the researcher's knowledge, there was no clear justification for a specific direction of differences to be predicted. **Would participants be more likely to judge emails which contained a persuasion technique as genuine compared to passively written emails?**

   Based upon the literature discussed in Chapter 2 and the introduction above indicating authority, scarcity, and time urgency have successfully increased response likelihoods to phishing emails, it could be expected that the inclusion of persuasion cues would increase the belief it was genuine. Although, as email context could be a moderating variable with little to no previous evidence indicating directional influence – a non-directional prediction was adopted indicating that differences were expected in the analyses from Study 9, but the direction may vary within persuasion manipulations due to email context.
3) **Are participants who are more likely to judge an email as being genuine more likely to respond?**

   It was predicted in Studies 9 and 10 those who believed an email was more likely to be genuine that they would also have been more likely to have chosen to respond.

4) **Does an increase in risk salience reduce the likelihood of responding to emails?**

   It was predicted that by asking questions to consider the likelihood of risk prior, participants would be less likely to respond to emails in Study 9 than in Study 8 (where no prior risk questions were asked) as an increase in risk salience could encourage greater need to avoid risks (Dertwinkle-Kalt & Koster, 2019).

5) **Do hard time constraints increase the likelihood of phishing susceptibility?**

   It was predicted in line with the research discussed in Chapter 2 (e.g., Chowdhury et al., 2019) that higher time constraints in Study 10 would result in an increase in responses to emails.

6) **Can the Expected Utility Framework be utilised retrospectively to highlight risks in phishing susceptibility?**

   As this is a novel application, it was not known the extent to which actual behaviour could be explained by subjective estimations of outcome utility and probability. However, calculations were made using the EU formula for the data collected in Study 10 and comparisons were made to indicate what percentage of EU predictions equated to actual behaviour. For expected utility outcome ratings for different email contexts, it was predicted that there would be differences between email contexts, though the direction of differences could not be predicted as there is little to no indication from previous research how outcome utilities could differ for the email contexts evaluated in these studies.

4.4 - Studies 8, 9, & 10: Methods

Participants

Study 8 - Data was sought to be collected from 300 participants through a UK representative sampling recruiting method to get a gender-balanced sample online via Prolific online marketing tool. Two-hundred and ninety Prolific users had signed up to take part in the experiment, though of these 290, twenty-five datasets had to be excluded due to missing or incomplete data (i.e., >40% of data from at least one measure), and another 10 were not included as main task data (collected in a Psychopy program) could not be paired with the rest of their data (collected via Qualtrics). The total number of participants included in the analysis was therefore 255 - above the minimum sample size required (n = 143 – as was the case for Studies 9 and 10) from G*Power (Faul et al., 2007; 2009) calculations for a medium effect size or greater based upon previous literature discussed (*w* > 0.3) with a power of 0.8. Ages ranged from 19-80 years old (*M* = 45.49, *SD* = 15.45), with 132 females (122 males, one other), and the majority having obtained at least A-levels or equivalent (86.3%) and 66.3% having obtained at least undergraduate degrees or equivalent.

For self-reported IT skill, 0.4% reported having poor IT skills, 3.5% were below average, 34.1% average, 44.7% good, and 17.3% excellent. For self-reported level of cyber-security training received, 19.6% reported having received no training, 36.9% received beginner level training, 36.1% received intermediate training, 6.3% advanced, and only 1.2% reported to have received expert level training. The average amount of time (hours and minutes) spent online per day was 6.11 hours (*SD* = 4.21). Regarding previous phishing email experience, 81.6% of included participants reported to have previously experienced phishing emails (with 10.6% reporting they have not, and 7.8% being unsure). When asked to report one they had previously suspected an email to have been phishing prior to taking part in the experiment, 6.3% of participants reported they suspected an email to be phishing on the day of the study, 27.1% reported suspicion within the last week prior to participation, 17.3% within the past fortnight, 27.8% within the last month, 8.2% longer than a month, 12.2% reporting they were unsure, and 1.2% had never suspected an email to be phishing.

Study 9 – As above, data was sought to be collected from 300 participants through a UK representative sampling recruiting method online via Prolific online marketing tool. Twenty-nine datasets had to be excluded due to missing or incomplete data, meaning the total number of participants included in the analysis was 271. Ages ranged from 18-89 years old (*M* = 45.91, *SD* = 16.10), with 137 females (133 males, one preferred not to say), and the majority having obtained at least A-levels or equivalent (85.3%) and 60.9% having obtained at least undergraduate degrees or equivalent.

For self-reported IT skill, 0.7% reported having poor IT skills, 2.2% below average, 35.4% average, 44.6% good, and 17.0% excellent. For self-reported level of cyber-security training received, 22.9% reported having received no training, 34.3% received beginner level training, 34.3% received intermediate training, 7.0% advanced, and only 1.5% reported to have received expert level training. The average amount of time spent online per day was 5.98 hours (*SD* = 3.11). Regarding previous phishing email experience, 85.1% of included participants reported to have previously experienced phishing emails (with 6.6% reporting they have not, and 8.1% being unsure). When asked to report when one had previously suspected an email to have been phishing prior to taking part in the experiment, 9.4% reported as suspected an email to be phishing on the day of the study, 31.8% reported suspicion within the last week prior to participation, 9.4% within the past fortnight, 28.1% within the last month, 9.4% longer than a month, 9.7% reporting they were unsure, and 2.2% reporting to never have suspected an email to be phishing.

Study 10 – Three-hundred participants were sought to be recruited through a UK representative sampling recruiting method online via Prolific. Thirty datasets had to be excluded due to missing/incomplete data (i.e., not completed the full study), resulting in a total number of 270 participants being included in the final analysis. Ages ranged from 18-76 years old (*M* = 45.39, *SD* = 15.15), with a balanced sample by sex (135 females and males), and the majority having obtained at least A-levels or equivalent (87%) and 66.6% having obtained at least undergraduate degrees or equivalent.

For self-reported IT skill, 0.7% reported having poor IT skills, 1.1% below average, 35.2% average, 43.7% good, and 19.3% excellent. For self-reported level of cyber-security training received, 24.4% reported having received no training, 33.7% received beginner level training, 33.3% received intermediate training, 7.8% advanced, and only 0.7% reported to have received expert level training. The average amount of time spent online per day was 6.28 hours (*SD* = 3.22). Regarding previous phishing email experience, 84.6% of included participants reported to have previously experienced phishing emails (with 7.1% reporting they have not, and 8.3% being unsure). When asked to report when one had previously suspected an email to have been phishing prior to taking part in the experiment, 10.2% reported as suspected an email to be phishing on the day of the study, 35.3% reported suspicion within the last week prior to participation, 12.4% within the past fortnight, 22.6% within the last month, 7.9% longer than a month, 10.5% reporting they were unsure, and 1.1% never suspecting an email to be phishing.

These three studies were approved by the Cardiff University School of Psychology Research Ethics Committee (CU-SREC). All participants across these three experiments were highly proficient in the English language with it either being their first language or fluent as a second language, normal/corrected-to-normal vision, and completed their respective experiments on either a laptop or desktop computer. Informed consent was obtained from all participants and upon completion they were fully debriefed and compensated £8 for participation (average completion approximately 40 minutes).

Materials/Apparatus and Design

A 5x6 repeated measures experimental design (persuasion technique x email context) was adopted for Studies 8 and 9, and a 5x5x6 mixed experimental design (persuasion technique x email context x time constraint) was adopted for Study 10. One repeated measures independent variable for all three experiments was email context consisting of five levels: confidence (i.e., an invitation to a conference), invoice (a request to confirm or review a purchase order), personal finance (a notification of being at risk of losing leave days or incurring loss of payment due to errors), loss of access (a notification alerting the risk of losing access to a work-related computer account or shared folders), and survey (a request to complete a survey which may consist of providing personal information or feedback). The second repeated measures independent variable adopted across all three experiments was the persuasion technique adopted within emails, consisting of six variations: authority (consisting of the inclusion of authoritative language and cues such as titles indicated sender authority), time urgency (calls for the need to reply within a limited time), scarcity of quantity (including details of the potential for limited quantities of something desirable), a combination of time urgency with authority, time urgency with scarcity of quantity, and no persuasion technique (whereby emails were passively written with no cues to indicate any degree of malevolence).

The third independent variable, a between-subjects manipulation only included in Study 10, was the amount of time permitted to make decisions (i.e., when requested to provide judgement ratings described below and indicate what action should be taken) which consisted of five levels which participants were randomly assigned whilst ensuring as close to an even distribution across each level: 13s (*n* = 50), 19.5s (*n* = 55), 26s (*n* = 54), 32.5s (*n* = 55), and

39s (*n* = 56). These objective time pressure levels were determined by the average response times from participants who took part in Study 9. The average response time for providing a probability judgement and behavioural response per email in Study 9 was 26s, forming the middle point of the objective time constraint conditions in Study 10, and the other conditions being 25% and 50% above and below the average.

A Qualtrics survey was developed for each study which consisted of the following sections in chronological order:

- An introduction providing an overview of the study and a consent form.
- A list of demographics questions consisting of - their Prolific ID so their data can be matched with Prolific to provide participation payments after the study, information on their age, sex, highest level of education achieved (GCSE or equivalent, A-levels or equivalent, undergraduate degree or equivalent, master’s degree or equivalent, doctorate, or other), subjective rating on a 5-point scale for current level of information technology skill (1 = poor, 5 = excellent), subjective rating on a 5-point scale for current level of cyber-security education (1 = none, 5 = expert), and average number of hours spent online per day.
- A description of the hypothetical context to the email task described below.
- (Study 10 only) Ratings for expected utility ratings in relation to each different email context type – detailed below.
- A link to the email task created in Psychopy and instructions on how to complete the task.
- A full debrief for the study.

For the expected utility ratings – novel scales were created in order to evaluate the subjective perception of outcomes to responding, or not responding, to different email contexts. With the actions to the decision being to respond or not respond, each action has a possible state of the world – i.e., the email could be genuine or phishing. As this was the case, participants would need to report the utility specifically for replying and not replying to an email which they believe to be genuine or phishing. Furthermore, each possible state may also be subject to both perceived negative and positive consequences. As a result, eight questions were formed to reflect the negative or positive utility to respond/not respond on the assumption that an email is genuine or phishing. With five different email contexts were considered in the experimental design, the eight questions were formulated for each of the specific email contexts – resulting in a total of 40 statements (used in study 10 only). For each statement, participants would be asked to indicate on a VAS the extent to which they valued the positive/negative consequences of replying/not replying to an email of a specific nature on the belief the email was genuine/phishing (scaled 0 = do not value to 100 = completely value). For example, for the context of a conference invitation, one of the questions was "How much would you value the positive consequences of replying to a genuine email invitation to attend a conference?". The full list of questions and scales used can be found in Appendix E. A definition of the email context was provided with each set of questions (also in Appendix E).

The decision to ask participants to judge positive or negative consequences was made as the researcher did not wish to restrict what participants could use to inform their subjective perception of outcomes. Whilst this can be noted in part as a limitation, as it would not be possible to clearly indicate specific examples of what informed values, the benefit was that it meant participants were not restricted in what could be used to inform decisions compared to categories imposed by the researcher – with positive and negative values still capable of indicating differences in perceived outcome utilities. Instructions were also provided asking participants if they could not think of anything to inform their judgement then they should provide a rating of zero – as if nothing can be thought of to inform their judgement then no weighting should be assigned to the valuation.

For the email task - Very realistic representations of 30 emails were created (See Appendix F for examples) – one for each combination of persuasion condition with context condition which were used for all three experiments. Each email consisted of only text content (no email addresses, links, attachments, images etc.), and would always refer to the need to click on a link or attachment within the text; however, referenced links/attachments could not be viewed (e.g., to see a contents preview or full link). The word count for each email was constrained to between 100-150 words and followed a uniform structure (introduction – e.g., greeting, main content, email signature – see Appendix F). Images were then presented to participants across all three experiments in a program developed in Psychopy one at a time in the centre of the screen, though in Study 10 participants were also shown a timer in the top-right of the screen to indicate how much time remained to make a judgement and decision regarding the presented email which differed depending on which time constraint level the participant had been randomly assigned to (13s, 19.5s, 26s, 32.5s, or 39s). When each email was presented, below the email, participants would be first asked to judge what the probability was for the email presented being genuine or phishing (Studies 9 and 10 only) on a VAS (Definitely Phishing = -100, Definitely Genuine = +100 – though numbers were not shown to participants) when being presented with the question “What is the probability this email is a genuine or phishing email?”. The question posed was worded as such to ensure ratings reflected the judgement that the equal opposite would hold true – i.e., if a participant provided a rating to indicate they believed an email to be 60% likely to be genuine, this would also indicate they consider there to be a 40% chance the email could be phishing. After a rating was given, this question and scale would disappear, still showing the same email, and be replaced with the question “Would you respond or not respond to this email?” along with buttons to respond/not respond.

The dependant variables consisted of expected utility ratings (Study 10), probability judgements of the likelihood the emails presented were phishing or genuine (Studies 9 and 10), and the proportion of participants who had chosen to respond/not respond to each of the 30 emails (Studies 8, 9, and 10). For Study 10, data from expected utility ratings and probability judgements were then input into an expected utility framework. Comparisons were made to measure the extent to which the data could indicate which behaviour participants were likely to value the most corresponded with actual respond behaviour. That is, the sum of all expected utility ratings (expected utility of the positive/negative valuation when choosing to respond/not respond to an email of a specific nature on the assumption an email was phishing/genuine) was multiplied by their respective state probabilities (subjective likelihood of phishing) to produce the expected utility for the actions to respond or not respond: with the highest number out of the possible actions (respond or not respond) indicating that choosing that action could be the most favourable on balance. An example can be found in the discussion of Study 10 (subsection 4.7.5) along with supporting tables (13 and 14).

Procedure

From signing up to the one of the three experiments on Prolific, all participants from Study 8, 9, and 10 were provided with a link to the Qualtrics survey, presented with a consent form, and they consented would first be asked to provide demographic information.

For study 10 only, after providing demographic information, participants would be asked to provide expected utility ratings for the extent to which they would value the positive/negative consequences of responding/not responding to each type of email context manipulated (conference, invoice, loss of access, personal finance, survey) on the belief that the email was genuine/phishing.

After providing demographic information for participants in Studies 8 and 9, and after completing expected utility ratings in Study 10, participants were provided with a link to the main email task created in Psychopy and run online in their browsers via Pavlovia. From clicking the link to open the program in a new tab, the task interface expanded across the full screen to avoid any potential onscreen distractions. On first opening the email task, participants from all experiments were instructed for the purpose of the task to imagine themselves as an individual called "Christie" who worked as an employee for a fictitious company called "Tech Supplies Ltd." as part of their southwest division. Christie was involved in the daily business operations of the company and worked on technology-based projects within the company. For the purpose of the task, all participants were asked to imagine themselves as this individual and complete the task as though they were this person called Christie.

All participants for each of the studies would then be provided with instructions and a trial run (consisting of a single email example) before they were presented with the same 30 emails, one at a time in a randomised order, for which they were instructed to read through and indicate whether they would respond or not respond to the email presented. For Studies 9 and 10, prior to being asked on whether they would respond or not respond, participants were asked to indicate the probability the email presented was genuine or phishing on a VAS scale. For Study 8, participants were only asked to indicate whether they would choose to respond or not respond to the email presented. In Studies 8 and 9, participants were free to complete the task in their own time with no time constraints, whereas in Study 10, participants were randomly assigned to one of the five time constraint conditions (13s, 19.5s, 26s, 32.5s, and 39s) and had to complete their judgement ratings and make a decision within their assigned limited time. For Study 10, participants were provided with a timer in the top-right of the screen to indicate how much time remained (in seconds) to provide the probability judgement and a decision for the email being presented. If a response was not provided within the time allowed in Study 10, the Psychopy program would move participants onto the next email trial automatically. After confirming understanding of the instructions and completing a practice trial, all participants in each study would then work through the 30 experimental trials. For all three studies, emails were presented in a random order. After completing the task, all participants were instructed to return to the Qualtrics survey and read a debriefing form with information about the experimental manipulations.

4.5 - Study 8: Results

All 255 participants included in the analysis provided responses to all email trials. Table 8 summarises the data collected on the number of participants who had indicated they would respond/not respond to each email. A Bonferroni correction was adopted to reduce the susceptibility to statistical errors from the 11 Cochran's Q tests which were carried out across the same dataset of behavioural responses (five to examine overall difference across email contexts, six for overall differences across persuasion technique levels). With two-tailed tests being adopted across all comparisons, as the direction of differences may not always be clearly defined between email contexts, the new *p* value from the Bonferroni correction to determine statistical significance was 0.0091. Note tests below with *sig* – this indicates that the test was found be significant with a *p* value below this new threshold.

From Cochran's Q tests, analyses found there were significant differences in response proportions across all email context conditions for each persuasion technique condition – Authority (x^2 (4) = 181.978, *sig.*), Scarcity (x^2 (4) = 370.341, *sig.*), Time Urgency (x^2 (4) = 387.728, *sig.*), Authority + Time Urgency (x^2 (4) = 188.409, *sig.*), Scarcity + Time Urgency

(x^2 (4) = 222.495, *sig.*), and no technique (x^2 (4) = 227.064, *sig.*). Significant differences were found for response proportions across all persuasion technique conditions within the Conference (x^2 (5) = 221.250, *sig.*), Invoice (x^2 (5) = 139.162, *sig.*), Personal Finance (x^2 (5) = 170.324, *sig.*), and Survey (x^2 (5) = 562.186, *sig.*) context conditions. For the Loss of Access context, no significant differences between persuasion techniques were found in response proportions (x^2 (5) = 5.242, p = .387).

Table 8.

Percentage of participants in Study 8 (n = 255) who chose to respond to the email within each persuasion technique and email context condition.

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	22.4%	85.5%	45.5%	56.9%	44.3%
Time Urgency	34.1%	93.3%	51.8%	84.7%	24.7%
Authority	74.5%	94.9%	51.4%	87.5%	62.7%
Scarcity	39.6%	85.5%	49.0%	69.0%	8.2%
Authority + Time Urgency	57.6%	70.2%	49.0%	49.0%	93.3%
Scarcity + Time Urgency	35.3%	68.2%	51.8%	70.2%	16.9%

4.6 - Study 9: Results

4.6.1 - Overview

All 271 participants included in the analysis provided responses to all email trials. Table 9 summarises the data collected on the number of participants who had indicated they would respond/not respond to each email, and Table 10 summarises the average probability estimates on the extent to which each email type was believed to be genuine or phishing. As with Study 8, a Bonferroni correction was adopted to reduce the susceptibility to statistical errors from the 11 Cochran’s Q tests which were carried out across the same dataset of behavioural responses, and with two-tailed tests being adopted across all comparisons as the direction of differences may not always be clearly defined between email contexts, the new *p* value to determine statistical significance was 0.0091.

However, the Bonferroni correction was different for the pattern of analyses for the probability measures. In addition to using 11 Friedman's tests to evaluate overall differences within each email context and persuasion manipulations, 135 Wilcoxon signed rank tests for pairwise comparisons were adopted for the probability analyses to explore whether there were any specific patterns between specific conditions. From these comparisons, with the added context of the binary regression analyses on the probability judgements detailed in subsection 4.6.5, these analyses could provide insight into why some conditions may result in more participants choosing to respond compared to others. Consequently, from using 146 tests to evaluate differences between conditions, the original *p* value of 0.1 for two-tailed tests was corrected using the Bonferroni correction to a new critical *p* value of 0.0006849315. Note that tests below with *sig* indicates that the test was found be significant with a *p* value below these new thresholds.

For testing behavioural differences between low risk salience (Study 8) and high risk salience (Study 9), a *p* value of 0.05 was corrected using a Bonferroni correction was adopted for the 30 one-tailed Wilcoxon signed rank tests evaluating whether an increase in risk salience in Study 9 versus Study 8 (low salience) reduced the likelihood of responding to emails to a new critical *p* value of .00167.

4.6.2 – Behavioural Findings: Response Differences

From Cochran's Q tests on the respond/not respond behavioural data, analyses found there were significant differences in response proportions across all emails context conditions for each persuasion technique condition – Authority (x^2 (4) = 126.530, *sig.*), Scarcity (x^2 (4) =

239.678, *sig.*), Time Urgency (x^2 (4) = 329.783, *sig.*), Authority + Time Urgency (x^2 (4) = 183.987, *sig.*), Scarcity + Time Urgency (x^2 (4) = 284.453, *sig.*), and no technique (x^2 (4) = 218.623, *sig.*). Significant differences were found for response proportions across all persuasion technique conditions within the Conference (x^2 (5) = 169.063, *sig.*), Invoice (x^2 (5) = 42.773, *sig.*), Loss of Access (x^2 (5) = 19.059, *sig.*), Personal Finance (x^2 (5) = 87.786, *sig.*), and Survey (x^2 (5) = 296.295, *sig.*) context conditions.

Table 9.

Percentage of participants in Study 9 (n = 271) who chose to respond to the email within each persuasion technique and email context condition.

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	24.4%	83%	36.9%	51.3%	46.9%
Time Urgency	38%	87.5%	41%	77.5%	25.1%
Authority	69.7%	84.9%	43.2%	70.5%	69%
Scarcity	35.8%	70.5%	46.5%	76.4%	21.4%
Authority + Time Urgency	46.1%	85.6%	48.7%	72.3%	40.5%
Scarcity + Time Urgency	41.7%	81.5%	37.5%	57.9%	13.3%

4.6.3 - Behavioural Findings: Differences between Low Risk Salience (Study 8) and High Risk Salience (Study 9) Conditions

To evaluate whether the inclusion of repeated risk probability measurements in Study 9 potentially increased the salience of risk, resulting in a reduction in the decision to respond, chi-squared tests of independence were adopted. These 30 tests compared for differences in behavioural responses for each of the 30 email conditions in Study 8 (low risk salience) with those from Study 9 (high risk salience). As these pairwise tests are evaluating the same hypothesis for different conditions, a Bonferroni correction was adopted to reduce the chance of false positives occurring (Type 1 statistical error). The original *p* value of 0.05 was corrected to a new *p* value to determine statistical significance: 0.00167.

Chi-squared tests of independence revealed significantly fewer participants in the high risk salience condition responded to the invoice email containing authority (x^2 (1, *N* = 526) = 14.350, *p* < .001), invoice with scarcity (x^2 (1, *N* = 526) = 17.115, *p* < .001), loss of access with scarcity and time urgency (x^2 (1, *N* = 526) = 10.616, *p* < .001), personal finance with authority (x^2 (1, *N* = 526) = 22.579, *p* < .001), and the survey email with authority and time urgency (x^2 (1, *N* = 526) = 163.239, *p* < .001). Significantly fewer responded in the low risk salience condition for the conference email containing scarcity and time urgency (x^2 (1, *N* = 526) = 27.911, *p* < .001), invoice with authority and time urgency (x^2 (1, *N* = 526) = 18.269, *p* < .001), invoice with scarcity and time urgency (x^2 (1, *N* = 526) = 12.453, *p* < .001), personal finance with authority and time urgency (x^2 (1, *N* = 526) = 30.001, *p* < .001), and the survey email with scarcity (x^2 (1, *N* = 526) = 17.846, *p* < .001). All other comparisons resulted in no significant differences being found (*p* > .00167).

4.6.4 – Probability Judgements: Differences between Persuasion Techniques and Email Contexts

As one-sample Kolmogorov-Smirnov tests revealed the probability judgement data was not normally distributed, Friedman tests were utilised as a non-parametric equivalent to a repeated measures ANOVA to analyse differences between email contexts and persuasion techniques. Wilcoxon signed rank tests were utilised to assess differences between individual conditions within each email context and persuasion technique manipulation. From Friedman tests, analyses found there were significant differences in phishing/genuine probability estimations across all email contexts for each persuasion technique condition - Authority (x^2 (4, *N* = 271) = 120.051, *sig.*), Scarcity (x^2 (4, *N* = 271) = 156.968, *sig.*), Time Urgency (x^2 (4, *N* = 271) = 232.058, *sig.*), Authority + Time Urgency (x^2 (4, *N* = 271) = 137.724, *sig.*), Scarcity + Time Urgency (x^2 (4, *N* = 271) = 222.109, *sig.*), and no technique (x^2 (4, *N* = 271) = 158.081, *sig.*). Significant differences were found for phishing/genuine probability estimations across all persuasion technique conditions within the Conference (x^2 (5, *N* = 271) = 191.902, *sig.*), Invoice (x^2 (5, *N* = 271) = 65.777, *sig.*), Personal Finance (x^2 (5, *N* = 271) = 104.521, *sig.*), and Survey (x^2 (5, *N* = 271) = 312.288, *sig.*) context conditions. For the Loss of Access context, no significant differences (as deemed by the Bonferroni corrections) between persuasion techniques were found in phishing/genuine probability estimations (x^2 (5, *N* = 271) = 12.050, *p* = .034). See Table 10 for an overview of probability estimations across all email conditions.

To conclude from this subsection's findings, in most cases there were significant differences between persuasion techniques and email contexts. Pairwise comparisons for probability differences between conditions can be found in Appendix G which highlight where specific differences may have occurred, however these comparisons can only provide initial conclusions as to how persuasion techniques and email contexts can influence judgements of phishing risk in specific conditions. As the likelihood of replicating such pairwise comparisons may be small – notwithstanding large Bonferroni corrections for the two-tailed tests – further replications would be required to evaluate how consistent pairwise comparison findings may be. However, the pairwise comparisons made can still provide some insight into which email contexts and persuasion techniques should be focused upon in future research using a simplified version of the present paradigm. To address the aim to understand the extent to which beliefs and values could predict behaviour considering these pairwise comparisons, binary logistic regressions were adopted to evaluate the extent estimations of phishing risk for different email contexts and persuasion techniques could predict behaviour. These are reported in the next subsection.

Table 10.

Average probability estimations (%) participants in Study 9 (n = 271) indicated the likelihood emails were genuine across persuasion technique and email context conditions.

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	46.69%	74.88%	46.57%	58.78%	67.25%
Time Urgency	58.92%	80.07%	46.71%	72.30%	51.11%
Authority	77.92%	79.08%	49.81%	64.21%	75.89%
Scarcity	60.23%	66.97%	51.19%	75.68%	47.66%
Authority + Time Urgency	66.26%	77.25%	51.95%	73.00%	59.77%
Scarcity + Time Urgency	62.70%	74.88%	46.57%	59.18%	38.63%

Note. Original data was collected on a VAS (Definitely Phishing = -100, Definitely Genuine = +100). For the table above, VAS ratings have been transformed to percentages indicating the average probability an email was believed to be phishing – e.g., 0 on the VAS is equal to a 50% probability the email is genuine. See Appendix H for original data means and standard deviations.

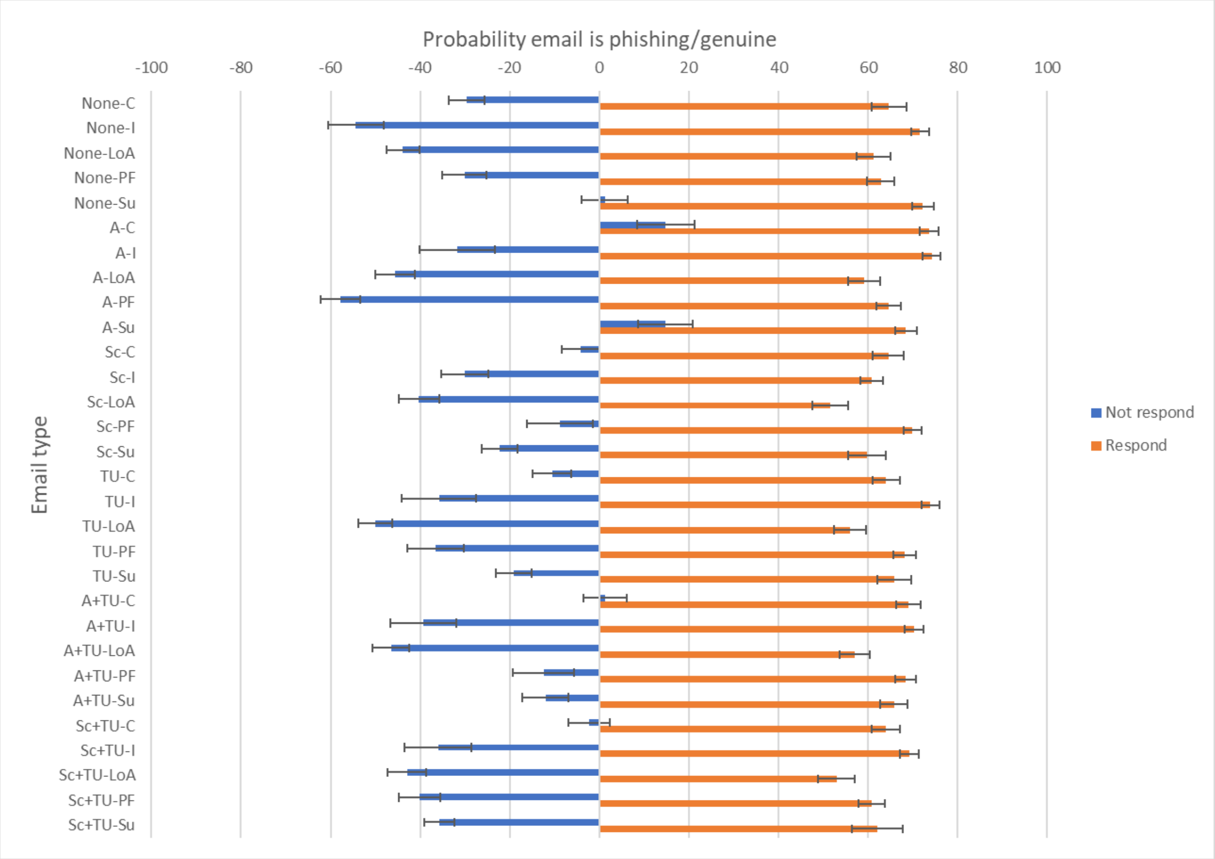
4.6.5 - Probability Judgements: Phishing Risk Perception Predicting Behavioural Responses

Binary logistic regressions were run for each of the 30 email conditions to examine whether the estimates of likelihood for the present emails was phishing/genuine were associated with the choice to respond/not respond to emails. As these tests are evaluating the same hypothesis for different conditions, a Bonferroni correction was adopted to reduce the chance of false positives occurring (Type 1 statistical error). The original *p* value of 0.05 was corrected to a new *p* value to determine statistical significance: 0.00167.

All regression models were significant ($p < .001$), indicating between 33.9% and 82.4% of variance (Nagelkerke R^2) could be explained depending upon the condition – with between 76% and 95.9% of behaviour being correctly classified. Odds ratios across conditions suggested participants who chose to respond were between 1.027 and 1.063 times more likely to rate emails as being genuine compared to those who chose not to respond. This indicated on average participants were more likely to choose to respond if they were more likely to believe the email was genuine, and vice versa (see Figure 23). Binary logistic regressions on a condition by condition basis can be found in Appendix I.

Figure 23.

Average probability judgements in Study 9 on the likelihood each email type is phishing or genuine (-100 = definitely phishing, 100 = definitely genuine) depending upon whether participants chose to respond or not to respond. Number of participants who chose to respond/not respond are reported in Table 9.



Note. Persuasion techniques: None = no technique, A = authority, Sc = scarcity, TU = time urgency, A+TU = authority and time urgency, Sc+TU = scarcity and time urgency. Email context: C = conference, I = invoice, LoA = loss of access, PF = personal finance, Su = survey.

4.7 - Study 10: Results

4.7.1 - Overview

All included data was collected from the 270 participants who completed the study in full. However, of the 270, a number of data points in the probability (10 or fewer within each within-subjects manipulation) and behavioural (28 or fewer – less than 18 in most cases - within each within-subjects manipulation) responses were missing due to the time constraint manipulation forcing participants to move on if they had not provided a respond within the time limit allowed. Going by time constraint manipulation, fourteen or fewer datapoints were missing across within-subject conditions in the highest time constraint condition (13s) and decreased as time constraint relaxed to three or fewer for the lowest time constraint condition (39s). As only a limited number of datapoints were missing, no further datasets were removed. Table 11 summarises the data collected on the number of participants who had indicated they would respond/not respond to each email regardless of time constraint condition, and Table 12 summarises the average probability estimates on the extent to which each email type was believed to be genuine or phishing regardless of time constraint condition. Tables summarising data collected from Study 10 also note the total number of datapoints for each condition within each data. Summaries of these probability and behavioural response tables can be found in Appendix J and K. As different amount of data points was missing in different conditions, tables for Study 10 also label the number of data points for each condition.

Table 11.

Percentage of participants in Study 10, who responded within time constraints, who chose to respond to the email within each persuasion technique and email context condition – regardless of time constraint condition.

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	29.6% (76/257)	75% (192/256)	39.9% (101/253)	55.1% (135/245)	43.6% (113/259)
Time Urgency	40% (102/255)	88.7% (235/265)	43.2% (115/266)	78.7% (203/258)	32.2% (84/261)
Authority	70.5% (182/258)	88.3% (226/256)	39.7% (100/252)	74.4% (180/242)	66.9% (174/260)
Scarcity	50.2% (127/253)	76.8% (195/254)	37.8% (93/246)	58.8% (147/250)	18.6% (48/258)
Authority + Time Urgency	42.5% (110/259)	71.4% (182/255)	48% (123/256)	51.6% (129/250)	84.1% (207/246)
Scarcity + Time Urgency	38.8% (100/258)	65.6% (164/250)	40.9% (105/257)	72.2% (182/252)	27.7% (71/256)

Note. Numbers in brackets indicates proportion of datapoints for that condition. i.e., (number of participants who chose to respond to the email/total number of participant datapoints for that condition).

Table 12.

Average probability estimations (%) participants in Study 10, who responded within time constraints, indicated the likelihood emails were genuine across persuasion technique and email context conditions – regardless of time constraint condition.

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	43% (266)	69.1% (267)	46.6% (268)	58.2% (262)	60.5% (265)
Time Urgency	52.8% (265)	80.5% (267)	48.4% (268)	72% (268)	48.7% (268)
Authority	71.4% (268)	77.5% (266)	45.6% (268)	66.7% (263)	73% (267)
Scarcity	59.6% (263)	69% (261)	43.9% (263)	57.4% (260)	37.6% (266)
Authority + Time Urgency	52.5% (265)	67.9% (263)	62.7% (262)	61.4% (264)	75.7% (263)
Scarcity + Time Urgency	50.6% (267)	61.1% (265)	45.1% (267)	70.1% (265)	45.4% (266)

Note. Numbers in brackets indicates proportion of datapoints for that condition.

Comparisons and replication of findings on the differences in phishing susceptibility due to persuasion technique and email context, with small exceptions in specific conditions due to changes in risk salience, have already been demonstrated within Studies 8 and 9. The main analyses of this experiment (Study 10) therefore focused on the more novel aspects of the phishing email paradigm which have gone beyond what was explored within Study 8 and 9. These novel aspects are as follows: the differences in phishing/genuine probability estimations and behavioural responses (respond/not respond) in respect to the time constraint between-subjects manipulation, observed differences in the expected utility ratings for all possible decision outcomes in the decision to respond/not respond to an email, and the retrospective use of the Expected Utility Theory framework as a tool to predict engagement with email response behaviour.

4.7.2 - Objective Time Pressure Differences: Behavioural Responses

Chi-squared tests of independence were conducted to evaluate whether there were significance differences for behavioural responses due to the third manipulation adopted within Study 10 – time constraints on the ability to form judgements and act on decisions (13s, 19.5s, 26s, 32.5s, and 39s). The chi-squared tests of independence revealed only that significantly more people were likely to respond than not respond when time constraint was higher for the loss of access email which contained scarcity cues (x^2(258, 4) = 9.51, p = .049). However, it was also found that significantly fewer people were likely to respond when time constraint was higher for the personal finance email which contained no persuasion cues (x^2(258, 4) = 14.26, p = .007). Other than these two email types, no significant differences in behavioural responses were found between time constraint conditions for the other 28 email types (p > .05). Consequently, it can be concluded that the manipulation of time constraints had little to no effect upon the choice to respond or not respond to emails.

4.7.3 - Objective Time Pressure Differences: Probability Judgements

One-sample Kolmogorov-Smirnov tests revealed probability judgements were not normally distributed, therefore comparisons between emails between time constraint conditions were made using Kruskal-Wallis tests. It was found there were significant differences indicating as time constraint was decreased the probably of emails being deemed to be genuine increased for the conference email containing authority and time urgency cues ($H(4) = 9.857$, $p = .043$). No significant differences were found in probability judgements between time constraint conditions for the other 29 email types ($p > .05$). As with the behavioural responses, it can be concluded that the manipulation of time constraints had little to no effect upon the probability judgements of whether emails were genuine or phishing.

4.7.4 - Expected Utility: Outcome Ratings Overview

One-sample Kolmogorov-Smirnov tests revealed that all positive and negative combined expected utility scores in the instances of replying, or not replying, to each email context type were not normally distributed, thus comparisons between email context utility ratings were made using two-tailed Friedman's tests. Four Friedman's tests were conducted to evaluate whether significant differences (with a critical *p* value of 0.1) occurred for email context (one for each utility rating type - reply to a genuine email, replying to a phishing email, not reply to a genuine email, and not reply to a phishing email). Pairwise comparisons using Wilcoxon signed rank tests were then adopted to evaluate the differences between specific email contexts for each utility rating type (with a new critical *p* value of 0.01 after Bonferroni corrections).

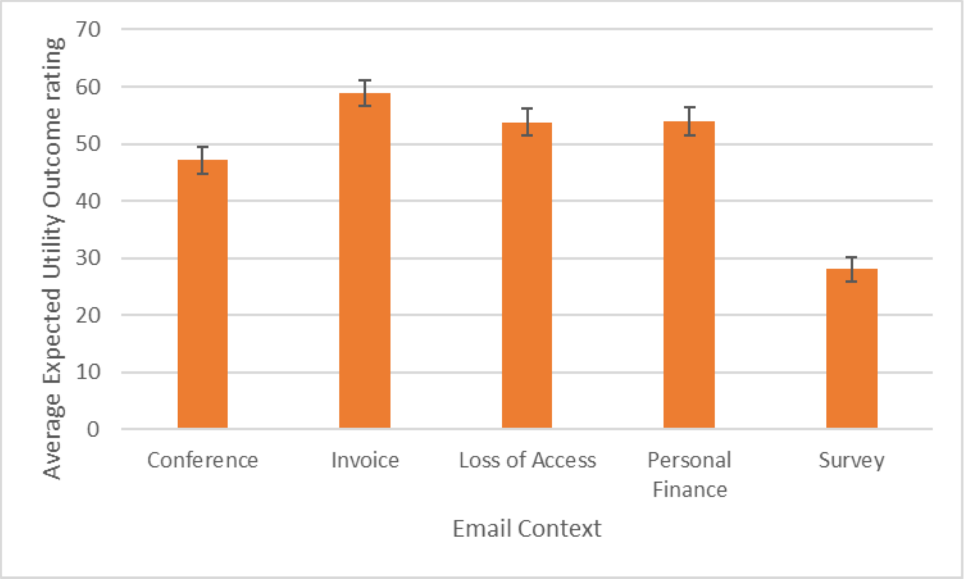
From Friedman's tests, there appear to be significant differences between email contexts in the utility ratings of replying to a genuine email (x^2 (4, $N = 270$) = 116.229, $p < .1$), replying to a phishing email (x^2 (4, $N = 270$) = 17.193, $p < .1$), and not replying to a genuine email (x^2

(4, N = 270) = 68.072, p < .1). No significant differences were found between email context utility ratings for not replying to a phishing email (x^2 (4, N = 270) = 4.234, p = .375). Figures 24a, 24b, 24c, and 24d summarise these utility ratings visually with the Wilcoxon signed rank tests to analysis differences on a more specific level are below.

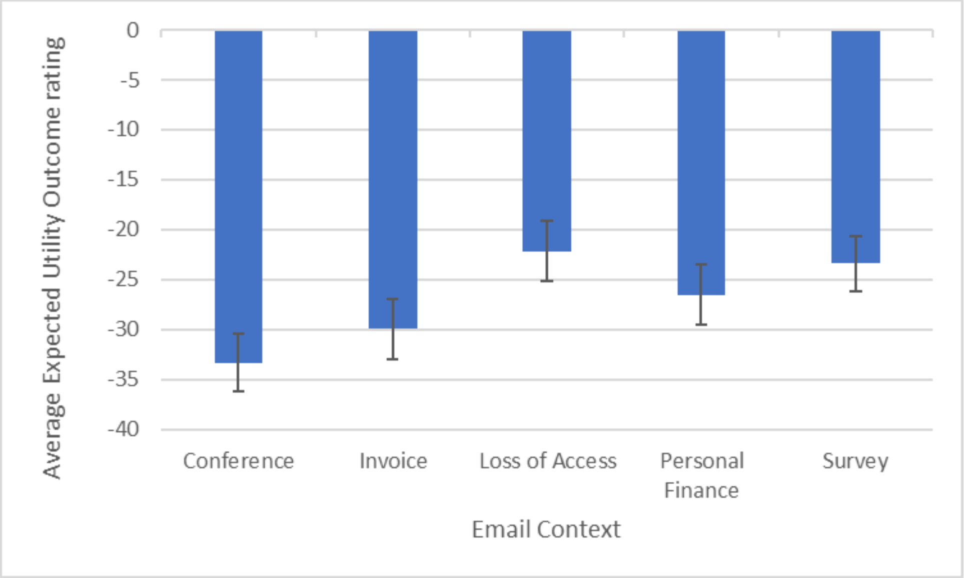
Figure 24.

The average expected utility outcome (EU$_O$) ratings in Study 10, consisting of combined negative value (-100 to 0) and positive value (0 to 100) ratings, from participants for each possible state (email is genuine or phishing) for each action (respond/not respond) across email contexts: a) the utility of replying to a genuine email, b) replying to a phishing email, c) not replying to a genuine email, and d) not replying to a phishing email. Error bars represent standard error +/-.

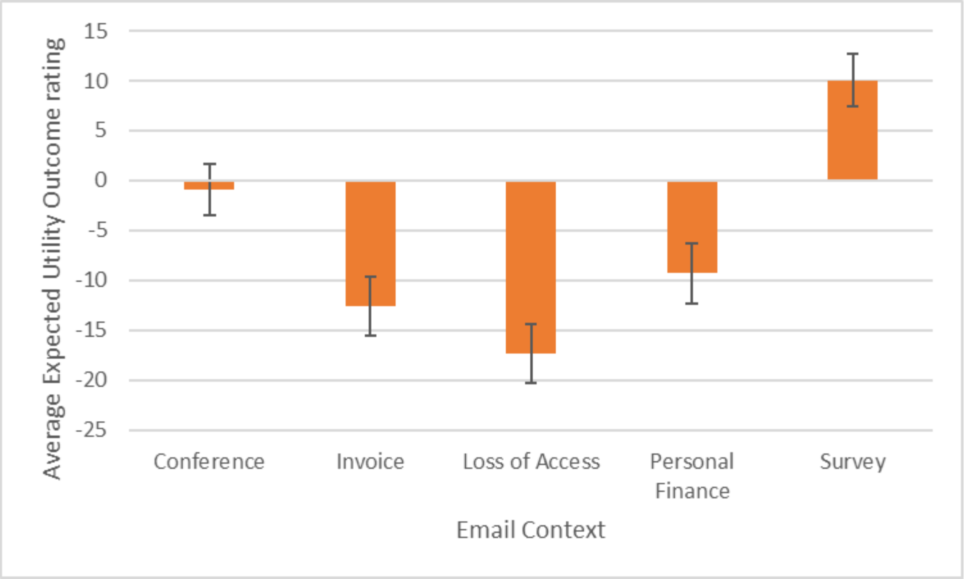
a)



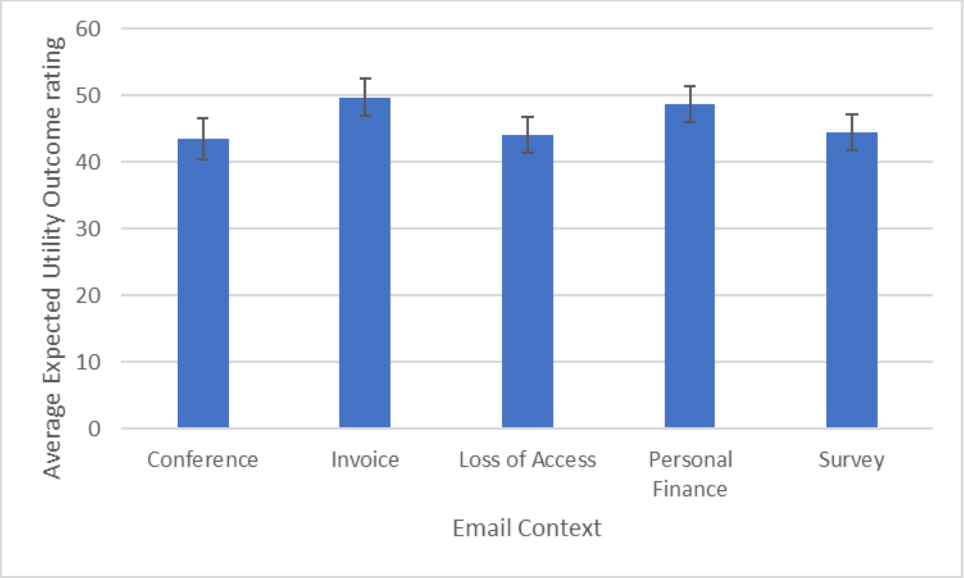
b)


Average Expected Utility Outcome rating
0
-5
-10
-15
-20
-25
-30
-35
-40
Conference
Invoice
Loss of Access
Personal Finance
Survey
Email Context

c)


Average Expected Utility Outcome rating
15
10
5
0
-5
-10
-15
-20
-25
Conference
Invoice
Loss of Access
Personal Finance
Survey
Email Context

d)



Expected Utility Outcomes for replying to genuine emails (Figure 24a) – Ratings for conference emails were significantly lower than invoice emails (*z* = -3.835, *p* < .01) and higher than survey emails (*z* = -6.585, *p* < .01). Survey email ratings were significantly lower than invoice (*z* = -9.663, *p* < .01), loss of access (*z* = -8.181, *p* < .01), and personal finance ratings (*z* = -7.938, *p* < .01).

Expected Utility Outcomes for replying to phishing emails (Figure 24b) – Ratings for conference emails were significantly lower than loss of access (*z* = -3.758, *p* < .01), personal finance (*z* = -2.596, *p* < .01), and survey emails (*z* = -3.281, *p* < .01). The invoice email ratings were lower than loss of access (*z* = -2.504, *p* = .012) in the direction of significance, and lower than survey ratings (*z* = -2.945, *p* < .01).

Expected Utility Outcomes for not replying to genuine emails (Figure 24c) – Ratings for conference emails were significantly higher than invoice (*z* = -3.131, *p* < .01), loss of access (*z* = -4.430, *p* < .01), and marginally higher than personal finance emails (*z* = -2.250, *p* = .024) – but not statistically significant according to the Bonferroni correction. Conference ratings were significantly lower than survey ratings (*z* = -4.143, *p* < .01). Invoice ratings were significantly lower than survey ratings ($z = -6.840$, $p < .01$). Loss of access ratings were lower than personal finance ($z = -2.618$, $p < .01$) and survey ratings ($z = -7.489$, $p < .01$). Survey ratings were lower than personal finance ratings ($z = -5.915$, $p < .01$).

Expected Utility Outcomes for not replying to phishing emails (Figure 24d) – Survey ratings were marginally lower than invoice email ratings ($z = -5.915$, $p = .012$) - but not statistically significant according to the Bonferroni correction.

All other comparisons were found to not show statistically significant differences (*p*s > .01).

4.7.5 - Expected Utility and Probability Judgements: Differences in Behavioural Responses

When using binary logistic regressions to evaluate associations between the expected utility outcome ratings (EUo – calculated from the ratings provided using the measures in Appendix E) for replying or not replying on the believe each email type there appeared to be no significant associations between individuals who chose to respond compared to those who chose not to respond. However, as was also found in Study 9, participants who chose to respond to emails were more likely to judge the probability of emails being presented as genuine compared to those who chose not to respond for all email types ($p < .001$).

4.7.6 - Expected Utility Framework Calculation

From collecting positive and negative expected utility ratings for all possible outcomes (EU_O) to the decision to respond or not respond to presented emails, along with estimations of probably of the likelihood of whether emails presented were genuine or phishing (P_S), the expected utility framework calculation could indicate based upon these factors what action (respond/not respond) should be expected for each given state of the world (EU_T). These expectations were then compared with actual behavioural to indicate the extent to which actual behaviour could be explained by estimations of expected utility ratings weighted by associated phishing and genuine probability judgements. Below is an example of this process using data from a randomly selected participant's dataset using the expected utility framework formula:

$$\boldsymbol{EU\ (Action) = \Sigma\ (U(Outcome) \times P(State)}$$

This participant, like all participants, had to make 30 decisions in the email task – to choose to respond or not respond to each of 30 emails presented to them. Each email consisted of one of five contexts (conference, invoice, loss of access, personal finance, and survey) containing one of six persuasion techniques (authority, time urgency, scarcity, authority + time urgency, scarcity + time urgency, no persuasion technique). This example will focus on the calculations for one of these 30 decisions – the decision to respond or not respond to a conference email which contained authority and time urgency cues. Before completing the email task, the participant provided eight ratings for the expected utility of each possible outcome to the set of actions available within the decision prior to taking part in the main email task. That is, participants were asked to indicate how much they would value the positive (or negative) consequences of replying (or not replying) to a genuine (or phishing) email (using the scales detailed in Appendix E). These scores were then added together for their respective states of the world to form the total expected utility rating for that outcome (EU_O). In this instance, the participant's values on these eight ratings and how they were calculated can be found below in Table 13.

Table 13.

Example using data from a randomly selected participant from Study 10 of expected utility outcome (EU_O) rating calculations in relation to conference emails.

Raw outcome rating judgement (0 = Do not value, 100 = Completely value)	EU_{raw}	EU_O (+ve EU_{raw} + -ve EU_{raw})
Positive consequences of replying to a genuine email	83	65
Negative consequences of replying to a genuine email (N)	-18	
Positive consequences of replying to a phishing email	0	-87
Negative consequences of replying to a phishing email (N)	-87	
Positive consequences of not replying to a genuine email	35	-31
Negative consequences of not replying to a genuine email (N)	-66	
Positive consequences of not replying to a phishing email	68	59
Negative consequences of not replying to a phishing email (N)	-9	

Note. (N) = Scale was scored negatively.

When being presented with the example of a conference email containing authority and time urgency cues, the participant providing an estimation on the likelihood that the presented email was genuine or phishing (scaled -100 = phishing, 100 = genuine). Ratings for this would determine the perceived probability the presented email was genuine or phishing (P_S). This participant provided a rating of -6.75 for this email, thus indicating they believed there was a 46.62% probability the email was genuine and therefore a 53.38% probability it was phishing. The EU_O for each state of the world within each action would then be weighted to calculate a total expected utility of that specific state of the world becoming true (EU_O x P_S = EU_T) as seen in Table 14. The EU_T within each action would then be added to give the total Expected Utility (EU_{Action}) for choosing that specific action – with this higher number indicating which action holds the highest expected utility. In this example, the calculation would suggest that the decision not to respond would have greater expected utility than choosing to respond – thus, theoretically, should indicate the participant would be more likely in this instance to choose not to respond than respond. This decision prediction was then compared with their actual behaviour and in this instance, it was found their predicted behaviour matched their actual behaviour. This process was carried out for all 270 participants where possible.

Table 14.

Example Expected Utility Action (EU_{Action}) calculation for a participant's expected decision to respond or not respond to a conference email containing authority and time urgency cues in Study 10.

Action	State	EU_O	P_S	EU_T	EU_{Action}
Respond	Genuine	65	46.62%	3030.54	-1613.21
	Phishing	-87	53.38%	-4643.75	
Not Respond	Genuine	-31	46.62%	-1445.34	1703.86
	Phishing	59	53.38%	3149.2	

With 270 participants in the final analysis, and with 30 decisions being made per participant, this meant there was a possible total of 8100 decisions being made. As probability estimations or behavioural responses were missing in select cases, likely due to the time constraint manipulation, EU_{Action} calculations and comparisons of outputs to actual behaviour were able to be carried out for 7643 decisions to find out the extent to which the EU framework could explain actual behaviour. From comparisons of EU_{Action} calculations with actual behaviour, it was found that 68.5% of actual behaviour could be explained by the EU framework.

4.8 - Studies 8, 9, & 10: Discussion

4.8.1 - Overview

From these final studies within the thesis, six key research questions (RQs) were addressed:

1) How successful are known persuasion techniques across different types of emails contexts?
2) Would participants be more likely to judge emails which contained a persuasion technique as genuine compared to passively written emails?
3) Are participants who are more likely to judge an email as being genuine more likely to respond?
4) Does an increase in risk salience reduce the likelihood of responding to emails?
5) Do hard time constraints increase the likelihood of phishing susceptibility?
6) Can the Expected Utility Framework be utilised retrospectively to highlight risks in phishing susceptibility?

In Study 8, addressing RQ1, the experimental paradigm was developed to be able to focus on comparisons between behavioural responses (i.e., choice to respond/not respond) across 30 emails varying in context (conference, invoice, loss of access, personal finance, and survey) and persuasion technique (authority, scarcity, time urgency, authority with time urgency, scarcity with time urgency, and no persuasion technique). From comparing the behavioural responses, as predicted, there were significant differences in response likelihood due to both persuasion technique and email context (Table 8) – suggesting that both manipulations can significantly influence phishing susceptibility if decisions are made solely upon the text of emails.

This finding was furthered to explore other components of RQ 1 in Study 9, not only by mirroring the broad pattern of behavioural findings (Table 9), but by including the requirement for participants to judge the likelihood that emails presented to them were genuine/phishing prior to decision making. In the majority of cases, as predicted in the hypothesis for RQ2, the inclusion of persuasion cues did increase response likelihood for emails which were deemed to be genuine compared to no persuasion techniques adopted – though differences are also noted depending upon the application of persuasion in different email contexts (Appendix G and I; Table 10). These initial insights from the pairwise comparisons considering the binary regressions in subsection 4.6.5 could indicate that phishing susceptibility due to persuasion technique and context could likely vary due to differences in probability judgements of phishing risk.

Whilst these differences for probability could provide some initial insights into reasons why differences in behaviour occurred across different conditions, the conclusions from the pairwise comparisons may be limited due to replication concerns - regardless of the large Bonferroni corrections adopted. Further replications would be required to check for consistencies of specific comparisons, though initial insights could indicate specific conditions of interest to investigate phishing susceptibility adopting a simplified version of the present paradigm. What can be firmly concluded, however, is that estimations of phishing risk could significantly predict whether individuals chose to respond or not respond regardless of condition – i.e., individuals who chose to respond were more likely to have believed the email presented was genuine compared to those who chose not to respond

(Figure 23 – addressing RQ3). Regarding RQ4, few differences in risk salience were found in behavioural responses between Study 8 and 9 – thus an increase in risk salience due to the inclusion of repeated measures has had a very mixed and limited influenced for only a few specific conditions as will be discussed below in more detail.

Study 10 built upon this experimental paradigm even further in two important ways. A third manipulation, time constraint (i.e., levels of restricting the amount of time to form judgements and act on decisions), was added to allow for the comparison of differences in phishing susceptibility between objective time pressure (time constraint) and subjective time pressure (time urgency persuasion technique) factors from findings of these three experiments. Participants were also required to provide expected utility ratings to all possible outcomes in the decision to respond to emails from different contexts, in addition to probability and behavioural responses. For the time constraint condition, addressing RQ5, almost no differences were found between probability and behavioural responses on the basis of hard time constraints.

Regarding expected utility ratings to address RQ6, however, multiple findings indicated how useful these measures are in explaining phishing susceptibility. First, comparisons in expected utility outcome ratings (provided from the measure detailed in Appendix E) across email contexts revealed that there were differences in participants' subjective value in the decision to choose to respond or not respond to different types of emails on the assumption they were genuine or phishing (Figures 24a to d). This indicates that there were sufficient differences in expected utility of outcomes for the email contexts included in the design to evaluate email context in phishing susceptibility. Second, because data was collected for expected utility ratings, probability judgements (perceived likelihood emails were genuine or phishing), and behavioural responses (respond/not respond), this data could be calculated using the Expected Utility framework to evaluate the extent to which actual behaviour could be explained by perceived outcomes and risk perceptions. From comparisons between EU predicted and actual behaviour (see subsection 4.7.6 with Table 13 and 14), it was found that of all 7643 decisions which consisted of full datapoints , 68.5% of actual behaviour could be explained by the Expected Utility Theory framework. This final point not only indicates that the novel application of EUT could be used to highlight risks in phishing susceptibility for a large majority of cases, but it could also be potentially applied to design user-centric phishing interventions.

Interestingly, whilst it appeared that participants who chose to respond were more likely to judge emails as genuine compared to those who did not respond in Study 10 as they did in Study 9, there were no significant associations with expected utility outcome (EUo) ratings and the decision to choose to respond/not respond. Subsections below focus on greater detail about each of these major points described, followed up by highlighting design limitations, future directions, and conclusions.

4.8.2 - Behavioural and Probability Differences

One of the assumptions previous research investigating persuasion techniques in phishing emails is that the inclusion of persuasion techniques into emails can increase the likelihood of responding to them (Bishop, Asquith, and Morgan, 2022; De Bona & Paci, 2020; Cui et al., 2020; Marett & Wright, 2009; Parsons et al., 2015; Vishwanath et al., 2011; Williams, Hinds, & Joinson, 2018). Whilst to some extent this has been found from examining behavioural responses in Study 8 and 9 within this thesis, it did not appear to always be the case. Differences in the success of persuasion techniques in phishing emails, within the current studies, appear to be also dependent upon the context of the email. This finding, whilst only demonstrating overarching differences between condition groups (persuasion technique and email context type), clearly demonstrates the limitations of previous research discussed by indicating that email context can have a huge impact upon how successful different persuasion techniques can be in increasing risk of phishing susceptibility. Furthermore, the finding provides a justification not just for why email context needs to be considered for future research but could explain why inconsistences in the success of specific techniques have been so varied.

Differences in phishing success (which from a cyber-security perspective could be described as a failure) across email contexts is particularly applicable to the inconsistencies noted in success for scarcity from previous literature (Bishop, Asquith, & Morgan, 2022; Lin et al., 2019; Parsons et al., 2019). In the case of scarcity, another reason for inconsistent findings in the present and previous studies (Bishop, Asquith, & Morgan, 2022; Lin et al., 2019; Parsons et al., 2019) could also be in part due to how scarcity is defined. In the present studies, scarcity has been divided into time urgency (i.e., cues within text indicating the need to respond by a perceived deadline) and scarcity of quantity (i.e., the limited number of offers or options available). With time urgency potentially differing in success across different contexts as a separate persuasion technique compared to when scarcity of quantity is also treated as a conceptually different technique (with initial insights indicated from pairwise probability ratings in Appendix G and regressions in subsection 4.6.5), this clearly demonstrates the necessity to distinguish aspects of persuasion techniques on a more granular level. Whilst behavioural findings from Study 8 and 9 have furthered the knowledge and understanding of how the success of persuasion techniques within emails can differ across contexts, differences between behaviours and participants can only be inferred from the manipulation of context and persuasion. What can be firmly concluded, however, is that significant differences overall do appear to occur due to both manipulations of persuasion and email context.

The inclusion of probability judgements in Study 9 and 10 further Study 8 and previous literature discussed above (e.g., Akbar, 2014; Bishop, Asquith, & Morgan, 2022; Butavicus et al., 2015; Williams, Hinds, & Joinson, 2018) which focused solely on behavioural responses by highlighting a key aspect of motivation in influencing behaviour. Two main findings were revealed from the analyses of phishing probability judgements. First, like behavioural responses, there appeared to be significant differences on the basis of both persuasion technique and email context. The second main finding, from comparing the extent to which phishing likelihood estimations could predict the choice to respond or not respond, it was observed that those who chose to respond were more likely to have perceived the email as genuine than phishing compared to those who did not respond (Figure 23). This supports the prediction that participants would be more likely to respond to emails they believe to have a higher probability of being genuine, demonstrating motivational differences between behavioural responses could have been due to differences in the perception of risk being influenced by persuasion technique and email context.

With this finding from the binary logistic regressions (subsection 4.6.5), and the added context of pairwise comparisons for probability judgements between the 30 email conditions (Appendix G), these findings provide some initial insight into how manipulations for persuasion technique and email context may be more successful in increasing phishing susceptibility compared to others. For example, from the pairwise comparisons detailed in Appendix G, loss of access emails on average were less likely to be believed to have been genuine compared to other emails contexts – regardless of the persuasion technique adopted in most cases. Invoice emails, on the other hand, were fairly consistently believed to have been more likely to be genuine than phishing. Whilst in some cases authority and time urgency, previously believed to be the most successful techniques consistently (e.g., Bona & Paci, 2020; Williams, Hinds, & Joinson, 2018), can increase the likelihood of believing the email presented appears to be genuine – pairwise comparisons indicate persuasion techniques can vary in this regard between different emails contexts. To summarise the findings on the extent to which probability judgements can address research questions 3 and 4, it can be concluded probability judgements on phishing risk perception can be useful in predicting the likelihood of participants choosing to respond/not respond to emails; and overarching differences in probability between the two manipulations further indicate both persuasion cues and email context can influence potential phishing susceptibility. However, despite the large Bonferroni corrections adopted for the pairwise comparisons – the extent to which firm conclusions can be drawn from these granular comparisons may still be limited due to replication concerns. Consequently, findings from pairwise comparisons should only indicate initial insight into conditions which may differ in phishing susceptibility risk. To make firmer conclusions for these types of granular comparisons, further replications with simplified paradigms would be needed. The pairwise comparisons from this thesis, however, could be utilised to inform such replications as a baseline example of specific instances in which risk may differ. Conditions in which no significant differences were found in Study 9 for risk perception have been highlighted, this future work could use these findings as a way to remove conditions and simply comparisons to only specific areas of interest.

When observing the mean probability of phishing likelihood between those who chose to respond/not respond (see Figure 23), in most cases the average perception of the email being genuine for those who chose to respond appeared to be greater than the average perception of the email being phishing for those who chose not to respond. In other words, it could be possible that there is a lower threshold for people to consider an email as being phishing to not respond than it does for people to consider an email as being genuine to respond. This observed difference is fitting with prospect theory and loss aversion – whereby, as discussed in Chapter 1, the perception of risk outweighs the equivalent gain (Brown et al., 2021;

Kahneman & Tversky, 1979). Kahneman and Tversky's (1979) prospect theory originally described this process often in terms of being based upon monetary gains and objective probabilities of outcomes which is not the case for most decisions outside of behavioural economics as objective probabilities are not always available for judgement – as was this case across the final three studies from this thesis. However, what these probabilities from Study 9 could show is that subjective judgements of risk probability derived from available information (not just from the text of the emails presented but from available memories) also form the same pattern of judgement and behaviour expected according to prospect theory.

Unlike previous research (e.g., De Bona & Paci, 2020; Trang & Nastjuk, 2021; Williams, Hinds, & Joinson, 2018), this experimental phishing paradigm allowed for the high level of control necessary to manipulate what information was presented to participants. What makes an email phishing or not is whether it contains some form of malicious capacity – i.e., the capacity to visit a non-secure website, download a virus, or steal personal information such as bank details. However, as participants were only presented with the manipulated text of emails, with no other cues being made available which could be used to form judgements and make decisions, clear conclusions can be made about availability bias in the susceptibility to phishing.

Outside of the subjective perception of the world, the text content of emails alone is not a completely objective property of what makes an email genuine or phishing – for example authority and time urgency cues can and do appear in both genuine and phishing emails. McAlaney and Hills (2020) examined how, through using eye tracking, people might look at emails to scan for factors which could be used to determine how genuine or not they might be – suggesting that those with phishing indicators defined by the authors (misspellings, grammatical issues, threatening language, urgency cues, financial information) were deemed to be less trustworthy. However, many of these features appear in non-malicious emails as well. Eye tracker heatmaps indicated that email addresses were one of the cues focused upon frequently (McAlaney & Hills, 2020). Once again, in reality, these phishing indicators defined by McAlaney and Hills (and is the case in other work – e.g., De Bona & Paci, 2020; Cui et al., 2020) do not objectively indicate whether an email is genuine or phishing.

Whilst false email addresses impersonating a genuine person/organisation (if correctly identified) could indicate that an email is phishing, phishing emails can still be sent from authentic email address – with this becoming more and more sophisticated. For example, an insider of an organisation could send phishing emails with malicious intent but might not be deemed a threat from observing their email address. Furthermore, with non-malicious intentions, phishing emails could be forwarded by unsuspecting users; or an authentic email account is hijacked by a cybercriminal and becomes a mode of delivery for phishing emails to unsuspecting victims. It is therefore important to consider that that both potential victims and researchers need to be able to clearly define what makes an email genuine or phishing. By not accurately defining the difference between cues which *define* an email as genuine versus phishing, and cues which *could* be used to judge whether emails are genuine or phishing, there is a risk that efforts to reduce phishing susceptibility could not be well targeted (a problem in the accuracy of judgement formation highlighted in Chapter 1). From this judgement accuracy formation issue, it is clear how easily cybercriminals could manipulate users using phishing techniques in targeted email contexts should they be biased to cues which do not reflect reality.

4.8.3 - Risk Salience

Within Study 9, it was expected that the inclusion of multiple requests for participants to judge the likelihood of presented emails being genuine or phishing could increase the salience of risk perception to judgements. Consequently, this could influence judgement formation around risk and subsequently behavioural responses to the decision to respond/not respond. Comparisons were made between the behavioural responses in Study 8 with Study 9 to examine for possible differences in risk salience prior to decision making: with it being predicted that with higher salience in risk in Study 9 (i.e., asking for prior judgements around phishing likelihood) could provide difference behavioural responses compared to those in Study 8 (low risk salience) to reduce risky decisions being made. However, only in a handful of specific comparisons was it found that higher salience resulted in fewer participants choosing to respond to the email. Furthermore, a few comparisons interestingly found significantly more people responded in the higher risk salience instance with a further case in the direction of significance. This suggests the capacity that of the measurement for phishing risk multiple times could influence behavioural responses is limited. With a lack of consistency, it suggests simply prompting the consideration of risk is not a reliable nudge (i.e., an influence over behaviour without coercion – Thaler & Sunstein, 2008) to prompt participants to consider not responding to emails. Subsequently, this not only suggests other nudge interventions to risk could be more worthy of adoption in practice (e.g., CybSafe's Human Risk Management platform which provides alerts to specific behaviour engagement – Nurse, Giddens, & Alashe, 2020), but that having so many repeated measures for individual participants to respond to in a single design only had a limited influence upon follow-up behavioural responses.

4.8.4 - Objective versus Subjective Time Pressure

To briefly recall, the key distinction between objective and subjective time pressure sources are as follows: Objective time pressure sources are a form of intrinsic cognitive load which consist of hard time constraints (e.g., five-minutes to complete a task, dealing with fixed-time interruptions or distractions during a task), whereas *Subjective* time pressure sources are a form of extraneous cognitive load include levels of stress derived from an individual's perception of time, sense of urgency, and the perception of hard deadlines.

Based upon previous literature, initially discussed in Chapter 2 (e.g., Acar et al., 2016; Capraro, 2017; Capraro, Schulz & Rand, 2019; Chowdhury et al., 2019; Cui et al., 2020; De Bona & Paci, 2020; Jones et al., 2019; Marett & Wright, 2009; Trang & Nastjuk, 2021; Vishwanath et al., 2011; Wang et al., 2012; Wright, Marett & Thatcher, 2014), it was predicted that both higher time constraints on forming judgements/making decisions and the inclusion of time urgency cues within email texts would increase participants' likelihood of engaging in riskier behaviour (i.e., choosing to respond to emails). In the majority of cases in Study 9, highlighted by both comparisons between probability estimations of phishing risk across conditions and the extent to which risk perception could predict actual behaviour, participants appeared to be more likely to respond than not respond when the indicated the email appeared more likely to be genuine. Although, as previously discussed, this in part was potentially moderated by the email context, and even though these pairwise comparisons can highlight initial areas of interesting further replication is required to strength conclusions. However, unlike the manipulated source of subjective time pressure, no significant differences were found for the majority of behavioural responses (28/30) or probability judgements (29/30) between the objective source of time pressure – hard time constraint. This difference in significance between objective and subjective time pressure in influencing phishing risk is quite different to what previous research has suggested. Trang and Nastjuk (2021) found as the time constraint within cyber-security decision making scenarios increased so did time stress ratings (i.e., stress derived from time perception), and subsequently as time stress increased compliance with information security policy decreased. From this example, Trang and Nastjuk (2021) outlined a framework for how hard time constraints influenced the stress derived from time perception, and subsequently cyber-security behaviour. However, findings from Study 10 bring some doubt into this explanation of the mechanisms behind how stress from the perception of time, manipulated by hard time constraints, influence behaviour.

A possible explanation for why differences were found for the subjective time pressure source but not for the objective time pressure is because they consist of different types of cognitive load (Sweller, 1988). Objective time pressure is a form of intrinsic cognitive load whereby there is an aspect of a task which is innately difficult. With objective time pressure, there is physically only so much information which can be processed within a certain amount of time even under the best of circumstances (e.g., Capraro, 2017; Capraro et al., 2019). Subjective time pressure, on the other hand, is a form of extraneous cognitive load whereby contextual factors can influence the perception of information. Within Studies 8-10, there was some initial evidence to suggest presence of time urgency cues within the emails appeared to alter the perception of the deadline for requests – increasing a sense of urgency. As a consequence, participants appeared to be more likely to choose to respond than not respond. This clearly demonstrates the distinction between objective and subjective time pressure in this decision-making context, and could be an indication, therefore, that intrinsic cognitive load (time constraint) was not high enough to provoke an increased need to respond to emails; whereas the manipulation of extraneous load indicated subjective time pressure sources (time urgency cues within emails) are critical to phishing susceptibility.

Future iterations of this paradigm could explore constraining time even further, but there may be some problems with this potential line of thought. First, as was observed in some instances in the higher constrained conditions in Study 10 (especially in the highest time constraint condition) increasing time constraint might increase mental demand to the point that it becomes impossible for participants to form judgements and make decisions within the time allotted – resulting in floor effects. Second, to restrict time available even further to make the decision to respond/not respond, might not be reflective of how much time actually spend on average reading and actioning emails – as noted by the average time taken from Study 9 being 26-seconds for this length and complexity of email (with a consistent length and complexity having been maintained across all three final studies). This average time spent could be even longer for actual emails which may not only vary in length and complexity but include more information cues such as images and addresses which may encourage people to take more time assessing emails which in reality people tend to do (McAlaney & Hills, 2020; Sturman et al., 2023).

4.8.5 - Expected Utility Theory (EUT): Measures and Applications

As introduced and critically discussed in Chapter 1, the original function of the EU framework by Von Neumann and Morganstern (1953) was to indicate on the basis of expected utility of possible action outcomes weighted by the probability outcomes are to come true how people *should* make *rational* decisions. However, as previously mentioned in Chapter 1, this basis is flawed because not only do people tend to violate the assumptions of the model (Kourouxous & Bauer, 2019; Oliver, 2003; Tversky, 1969), multiple irrational elements of decision making such as the perception of contextual pressures (Dykstra & Paul, 2018) and non-malicious motivations due to time pressure (Chowdhury et al., 2019) need to be considered to accurately understand *actual* decision making. Having a high level of control over the experimental environment, and collecting subjective estimations of expected utility and probability, means biasing factors which influence decision making such as availability bias can be captured by the EU framework. Furthermore, instead of utilising the framework to determine how people *should* be making decisions, the framework was used retrospectively: and for Study 10 – it has been demonstrated that EU can predict a large majority – over two thirds – of actual behaviour.

Whilst this means 31.5% of behaviour is not accurately predicted, it still indicates how the framework could be used retrospectively through simulations to highlight where the significant risks lie in phishing susceptibility – going above and beyond previous research and current phishing simulations which focus largely on actual behaviour responses (e.g., Akbar, 2014; Bishop, Asquith, & Morgan, 2022; Butavicus et al., 2015; De Bona & Paci, 2020; MetaCompliance, 2023; TitanHQ, 2023; Williams, Hinds, & Joinson, 2018). By breaking down the expected utility of replying/not replying to different types of emails, being weighted by estimations of phishing probability when exposed to controlled stimuli, this framework could be used as a diagnostic tool to indicate where the risk may lie in the decision-making process. In the instance of Study 10, despite there being significant differences in the expected utility outcome ratings for responding/not responding to different types of emails, there did not appear to be any associations in expected utility ratings for those who chose to respond and those who chose not to respond. However, in Study 9 participants who chose to respond to emails were on average more likely to believe that the emails were genuine and those who did not respond were more likely to believe emails were phishing. What this could indicate is that probability estimations of risk are the driving factors behind the significance in expected outcomes influencing actual behaviour – though as these are observational comparisons based upon the manipulations within these studies, clear causal relationships cannot be established.

On average, however, what could be indicated is that biases in decision-making for these instances could largely be determined by availability bias rather than preconceptions of outcome expectations. Subsequently, interventions could be designed in a way to target these specific biases as a way of reducing susceptibility to phishing by encouraging metacognitive reflection – i.e., reflection upon thought processes (Flavell, 1985). In Chapter 1, the quality of a decision was defined as the suitability of the framework of the decision-making process in the given circumstances, which considers the potential for desirable and undesirable outcomes coming true, combined with the quality of the information available being used. From the decision maker’s perspective, however, how do they determine whether they have made a good decision? If the focus within interventions such as phishing simulations which focus on just behavioural outcomes (e.g., MetaCompliance, 2023; TitanHQ, 2023), then only one aspect determining the quality of decision-making is being addressed (and potentially reinforcing the misbelief that outcomes are the most important aspect of decisions – Yates, Veinoot, & Patalano, 2003).

Evidence, such as Cofense (2022) and Gordon et al. (2019), suggests repeated use of simulations can help reduce susceptibility to some extent indicating the percentage of responders to phishing emails reducing with amount of exposure, though part of this success could be due to factors beyond simply observing click rates as feedback. It was noted the majority users in Cofense (2022) who clicked on fraudulent links in phishing emails presented only spent between 0-19 seconds reflecting upon the phishing simulation education page. This indicates at least two things – first, the need to reflect upon information outside of the immediate content of emails, and second, more time spent reflecting upon on educational hints could help reduce phishing susceptibility. An interesting area for future research, therefore, could be to examine how users could use the EU framework as a human risk assessment tool to highlight risks to phishing susceptibility and evaluate the extent to which it actually helped to reduce risky decision making.

4.9 - Limitations, Future Directions, and Chapter 4 Conclusions

Unlike the previous research discussed in the introduction of Chapter 4, Studies 8-10 using a novel experimental paradigm demonstrated that the context of emails can be a significant factor in influencing phishing email susceptibility and that the success of persuasion of phishing techniques can be dependent upon the context in which they are used. Furthermore, through the retrospective collecting expected utility and risk probability estimations with controlled simulated scenarios it has been demonstrated the EU framework could be utilised retrospectively to highlight areas of phishing susceptibility such as availability bias. This high level of control and manipulation in a complex paradigm over what information is presented to participants allowed the ability to control for extraneous variables which could also influence phishing susceptibility which were not key to understanding the key research aims of these studies. Nevertheless, there are limitations and these need to be considered.

One limitation is the extent to which findings can be applied to decisions outside of the laboratory and in real life situations e.g. involving actual work with emails. Participants were presented with only the manipulated text within emails, whilst other cues which could have potentially been used to determine whether emails were genuine or phishing were hidden such as email addresses, links, attachments, images/logos and so on. In real life, however, people can, and do, use these other cues to judge whether emails are genuine or not (e.g., McAlaney & Hills, 2020; Bishop, Asquith, and Morgan, 2022; Parsons et al., 2015; Sturman et al., 2023) – thus findings in these studies simply detail the worst-case scenarios whereby people are only relying upon, or relying too heavily upon, the text of emails. As discussed, the main body of text content of emails has no indication in reality of whether an email is genuine or phishing – e.g., both can contain persuasion techniques across different types of emails – yet significant differences were found in both behaviour and probability judgements on phishing likelihood across emails with differing outcome utilities based purely upon the information available. Future directions, using emails of varying length and complexity (a limitation of the present design), could involve manipulations to the availability of other cues which could be utilised to verify the authenticity of emails: for example checking consistency of other cues within the email (e.g., email addresses, links, images etc.) and verifying with cues outside of the email (e.g., in-person availability to known senders, searching the internet to verify website authenticity). These comparisons could build upon the present paradigm by providing insight into how trust and authenticity could be perceived for different types of emails, as previous research has indicated the inclusion of other cues such as images could increase believability (Stojmenovic et al., 2022).

To build upon the restrictions (deliberately kept simple – binary – within the current experiments) of decision options (only respond/not respond), a broader selection of options could be explored to gain further insight into whether, when permitted to, people would engage in other available real life actions such as deleting and reporting emails; or not responding to email requests but following up with emails to confirm authenticity. As the significance of expected utility ratings, probability estimations of risk, and behavioural measures have been established across different email types and persuasion techniques, this could expand the capacity of the EU framework to better reflect the capacity of actions in real life. Further work is needed to explore variance in behaviour which was not explained. In part, this could be due to the binary nature of the output to this actuarial formulation; thus, a future development could be to examine whether boundaries could be established to indicate likelihood of choice as an output in comparison with actual behaviour rather than simply a comparison of whether one action rating is higher than others. For example, this could be based upon the size of the difference between EU ratings – with large differences indicating a stronger likelihood of choosing that option compared to smaller differences indicating little variety in motivation for choosing a particular action within a decision.

Another way of expanding upon the framework could be to incorporate temporal utility – i.e., differences in expected utility due to when outcomes are likely to occur. With temporal discounting being known to influence decision making behaviour, i.e., the tendency to perceived desired results in the future as being less valuable than the present (Abdellaoui, Gutierrez, & Kemel, 2018; Odum, 2011; Stewart, Chater, and Brown, 2006), including this within the paradigm could go some way to explaining further variance in behaviour. In Study 10, expected utility ratings were in relation to the positive or negative value in replying or not replying to different types of emails on the assumption they were genuine or phishing. By constraining ratings to simply positive or negative, this is both a limitation and a strength. On the one hand, by not distinguishing between individual variables which could be used to weight negative and positive utility outcome ratings it is unclear what topics have been used to inform subjective values. However, on the other hand, by not making distinctions and defining specific variables which inform utility outcome ratings, it means raters are not limited by what can be used to inform their ratings. A future direction, therefore, could be to measure the utility of outcomes occurring at different times to examine whether temporal discounting could also influence phishing susceptibility to different types of emails. Whilst behavioural estimations of time perception averaged over time might not be predictive of cyber-security behaviour, as indicated from Study 6 in Chapter 2, initial estimations of time perception and utility ratings weighted by outcome timing payoff could be worth further investigation in the context of phishing decision making.

Another possible topic of exploration could be to examine emotional triggers such as fear which provoke stress reactions and attentional misdirection (Norris & Brookes, 2021; Williams, Beardmore, & Joinson, 2017) in real-time decision making using neurophysiological measures such as eye tracking to measure attention to specific cues (McAlaney & Hills, 2020) with pupil dilation to evaluate the depth of stimulus processing (Langer et al., 2017). This would have been difficult to control and manipulate in an online design, such as that used in Studies 8-10 which was adopted to collect a sizable sample of data from members of the general population within a practical period of time. Measures for utility outcome and probability were intentionally kept vague in order to not limit what variables could be used to form judgement. Furthermore, as this paradigm is a novel evaluation of phishing susceptibility from the user's perspective, it was necessary to establish a proof of concept that such a framework could be suitable to explaining actual behaviour. However, future adoptions of the paradigm could explore using more specific measures of utility to investigate the extent to which specific variables might be relevant, and valued, in decisions to respond to emails. This direction of research could indicate what might be the most relevant and valued utilities to form judgements out of the 68.5% which has been explained presently. Heart rate and skin conductance measures could accompany these suggestions in an in-person adaptation to observe differences in stress responses (Can, Arnrich, & Ersoy, 2019) with exposure to different types of cues (persuasion or otherwise) in real time to add further layers to potentially explaining actual behaviour responses.

Collectively with the suggestions above for future work, these areas could highlight the extent to which the EU framework within this novel phishing simulation paradigm could be used to evaluate phishing risks over time as part of a metacognitive intervention to maladaptive cyber-security decision making. Therefore, to conclude Chapter 4, these experiments have clearly shown phishing susceptibility can be greatly manipulated through the use of persuasion techniques such as time urgency, authority, and scarcity across specific email contexts – and these vulnerabilities can be predicted with a good degree of accuracy using the EU framework in a phishing simulation. Through the adoption of a complex paradigm which adopted multiple manipulations with several levels, consistencies (and inconsistencies) found can help refine the focus of future phishing susceptibility evaluation research to specific high-risk email contexts and persuasion techniques which may require further support. Whilst it is important to develop training to spotting persuasion cues with their associated high-risk email context, it is with paramount importance other cues which clearly determine the capacity for phishing are identified and evaluated by users through metacognitive interventions to avoid the overreliance upon unreliable available information which could put individuals, organisations, and businesses at risk to phishing threats.

General Discussion

Overview

The main aim of this thesis was to examine the impact of cognitive load, how it applies to, and impacts upon, cyber-security decision making quality, and subsequently how research to address this could be utilised in the development of tools and user-centric interventions to reduce risky cyber-security decision making. Throughout, from literature reviews and the progression of studies, it became apparent a critical source of cognitive load was that of time pressure – both *objective* (i.e., hard time constraints) and *subjective* (i.e., stress derived from time perception); and exploration of the impact of these workload factors became a central focus to addressing risky cyber-security decision making. In the context of cyber-security, it became apparent (from a novel systematic review – Chapter 2) that some previous literature has evaluated the significance of time pressure, though there has largely been focus upon *objective* time pressure and the risk it might pose to engaging in maladaptive cyber-security behaviours (e.g., within a previous systematic review by Chowdhury et al., 2019). Less was known (prior to the research within this thesis) about the risks that sources of *subjective* time pressure could pose to decision making in cyber-security, and subsequently how they could be mitigated from with user-centric interventions became a focus to address the gap in this literature.

Across Chapters 1-4, the research transitioned from theoretical evaluation of decision making theory (e.g., EUT – Bernoulli, 1738/1954; Prospect Theory – Kahneman & Tversky, 1979; Bounded Rationality - Simon, 1957; Cognitive load - Sweller, 1988) to applied cognitive science and then within the context of cyber-security. The critical evaluation of previous research highlighted how the quality of decision making can change due to changes in cognitive load or highlight where limited conclusions can be drawn from research. For example, by evaluating research suggesting experience of higher cognitive load in controlled experiments (i.e., derived from task difficulty) can increase the engagement in maladaptive behaviour when given the opportunity to be expressed in a similar way to priming cognitive load (Mead et al., 2009; Chapter 1) to inform motivations to insider threats in cyber-security. Whilst Chapter 1 highlighted that there was limited evidence to support the notion dishonesty could increase when cognitive load is high when individuals are not under public scrutiny, it was suggested an increase in subjective time pressure could potentially reduce the likelihood of engaging in maladaptive behaviour. but also result in underestimations of performance under low cognitive load.

These findings are of theoretical importance as they indicate awareness of time could influence confidence in one's own ability through increasing self-awareness, with implications suggesting this psychological mechanism could be useful in trying to reduce insider threat in cyber-security behaviour (when motivated by self-interest) in more applied settings. However, the nuances of subjective time pressure in cyber-security may differ compared to controlled laboratory experiments, thus this warranted more applied research exploring time pressure in cyber-security decision making. Through a novel systematic review to evaluate the extent to which subjective time pressure had been researched in the context of cyber-security, all included research suggested this form of cognitive load can increase risky decision making in cyber-security. However, only a limited amount of research – 10 papers in total – appeared to be relevant to this research domain (Chapter 2); highlighting a clear dearth in understanding within this area regarding a broader variety of cyber-security decision making, the need to evaluate how time perception and pressure measures could be used to predict cyber-security behaviour engagement, and how nuances of cyber-security contexts may influence perceived outcomes and risks.

Chapter 3 drew upon the first 2 of these 3 main focus points drawn from the findings of the systematic review in Chapter 2. It addressed these by exploring how novel applications of subjective time pressure and accuracy measures could reliably predict a broad range of safe (and unsafe) cyber-security behaviour engagement compared to other individual difference predictors (e.g., decision-making styles – Egelman & Peer, 2015; personality - Shappie et al. 2020). Whilst there were mixed findings related to the ability to predict cyber behaviour engagement with subjective time pressure and time perception measures, reasons behind these were evaluated through a follow-up study (Study 7), and improvements to self-report measures were investigated through comparing the adoption of Visual Analogue Scales (VAS) with more traditionally and frequently used Likert scales. Comparisons highlighted that VAS should be preferred across the board due to the possibility of reducing noise in data collection due to anchoring and adjustment and because responding using VAS allows a greater level of granularity in the data.

Chapter 4 was then developed to explore the remaining gaps highlighted in Chapter 2 – specifically the wider context of phishing emails needed to be considered when evaluating the success of urgency as a persuasion technique. The experiments were designed to demonstrate how phishing susceptibility could be increased from the inclusion of persuasion cues (e.g., instilling a sense of urgency from cues within emails as a sources of subjective time pressure), but vary in success due to differences in the wider email context. It was also found that phishing susceptibility can be dependent upon the context of perceived risks and outcomes when people only have access to, and utilise, poor quality information into judgement formation. A novel application of expected utility theory (EUT - Bernoulli, 1738/1954) was adopted within this thesis through developing a new experimental paradigm that has the capability of highlighting where the risk in phishing susceptibility may lie – with a large percentage of variance in the behaviour data (68.5%) could be explained from utilising the adapted EUT framework. From these findings in Chapter 4, it has been possible to indicate the extent to which cognitive load in the form of subjective time pressure can impact the quality of cyber-security decision making, along with providing the groundwork for the development of a phishing susceptibility tool which could hold the potential to support metacognitive interventions to improve decision making quality. However, in the context of these final chapter studies, it was found objective time pressure did not pose a significant threat to phishing susceptibility. Through being able to highlight the weighting of key variables which could weight motivations behind behaviour, this phishing susceptibility tool could allow for the reflection of the processes going into a decision – not just allowing for reflection upon the outcomes of decisions.

The below subsections expand upon what each chapter set out to achieve, how the current 10 studies and systematic review add novel contributions to current bodies of research, as well as further discussions around limitations and subsequent recommendations with future directions.

Chapter 1: Contributions to the Thesis and Research

Chapter 1 began with a review of decision making theories in order to outline what constitutes the quality of a decision – making it possible to determine how previous literature on cognitive load (e.g., Chowdhury et al., 2019; Sweller, 1988) could influence the likelihood of engaging in risky maladaptive behaviours. Earlier psychometric-based theories such as Expected Value Theory (EVT – Hald, 1990) and Expected Utility Theory (EUT – Bernoulli, 1738/1954) incorporated aspects of probability and outcomes designed to indicate what would be the *rational* choice to a given decision. However, numerous examples following the development of these psychometrics indicated they we not completely reflective of *actual* decision-making behaviour (e.g., Allais, 1953; Ellsberg, 1961; Kourouxous & Bauer, 2019;

Loomes, 1989; Oliver, 2003; Ranyard, 1977; Tversky, 1969) with principles for what was deemed to be *rational* often being violated (i.e., axioms of cancellation, transitivity, dominance, and invariance). Acknowledging the difference between how people *should* make decisions to optimise goals, how people *ought* to make decisions based upon ethical dilemmas, and how people actually *do* act was critical into understanding how the quality of decision making can be influenced by the irrational in the context of cyber-security.

Brunswik's lens model (1956) was a cornerstone throughout the thesis in acknowledging this difference by distinguishing between reality, subjective perception, and the level of accuracy between the two (Figure 2). It was established that reality and subjective perception can exist simultaneously, and often subjective perception does not accurately reflect the judgement of reality. This was important for two reasons. First, this could have been the mechanism behind understanding why cognitive load such as subjective time pressure may influence risk – i.e., because the quality of, and attention to, information used to form judgements of reality being manipulated. Second it was determined and posed that researchers within this field, when designing studies, must clearly define the difference between reality and subjective perception as this can impact what can be concluded from research conducted (e.g., distinguishing between different types of cognitive load, objective and subjective time pressure, and defining what makes an email phishing). From the review – it was possible to create a definition of what aspects defined the quality of a decision: *the suitability of the framework of the decision making process in the given circumstances, which considers the potential for desirable and undesirable outcomes coming true, combined with the quality of the information available being used*. The definition of what makes a good decision was vital to establish to inform what aspects of decision making were being evaluated in the research throughout the thesis. The definition was drawn upon to understand and contextualise how the quality of decision making can be influenced by different forms of cognitive load, and subsequently identify why maladaptive behaviour may occur in both controlled and applied research environments.

For example, when reviewing the background literature to the studies in Chapter 1 having a clear definition of what the quality of decision making consisted of helped to define how maladaptive behaviour could occur due to malicious and non-malicious motivations in both laboratory and cyber-security settings. Adopting a series of theoretically based studies with experimental designs in Chapter 1 allowed for high levels of control over targeted manipulations which built upon previous use of a paradigm used to investigate to what extent cognitive load influences acts of dishonesty. Acts of dishonesty had been found to be significantly more likely under higher cognitive load conditions (e.g., Mead et al., 2009) – a pattern of behaviour which could be akin to that of insider threats in cyber-security (both with malicious and non-malicious intentions noting that most insider threats are acting non-maliciously – e.g. striving to achieve a goal for the perceived better).

Whilst there was little evidence from studies 1-5 to suggest that high cognitive load increased dishonesty when individuals are not under public scrutiny, through running multiple adaptations of the developed paradigm, with the new addition of manipulation checks such as the NASA-TLX workload measure (Hart & Staveland, 1988), it was possible to highlight why the predicted results were not found. The main reasons for these findings could potentially be due to an ineffective manipulation of cognitive load (despite a clear distinction between the manipulations – so possibly a calibration issue) or lack of believability in performance not being judged publicly – with participants performing under controlled experimental conditions. These findings, consequently, do not contribute to the understanding of potential motivations to insider threat in cyber-security. However, the consistent finding of underreporting, somewhat in line with previous research (e.g., Gino & Mogilner, 2014), could hint at how increased time salience could reduce the likelihood of engaging in dishonest behaviour. As this was a finding from controlled laboratory experiments, however, this highlighted the next step needed was to explore what time pressure research had been carried out to date in the context of cyber-security settings.

By springboarding with a theoretical approach to address the thesis aims, it was intended that findings could help inform the direction of more applied research to follow with implications for behaviour patterns relevant to cyber-security. For example, small acts of dishonesty (with malicious or non-malicious intentions) in the context of cyber-security could result in a cyber breach occurring – potentially putting the decision maker and others (colleagues, an organisation, connected organisations, and so on) at risk to significant loss of personal data, or monetary loss. Whilst these first studies (1-5), rooted in theory, were instrumental in the beginning to understanding the impact of the cognitive load mechanism, a different approach was required as little to be concluded. Chapter 2, therefore, became the next logical step to collate and evaluate existing research in more applied contexts to inform what research approach should be taken to address the aims of the thesis.

Chapter 2: Contributions to the Thesis and Research

The development of a systematic review in Chapter 2 seemed to be the most appropriate transition from theory to applied research as it allowed for the identification of research gaps in relation to a highlighted topic of interest, cognitive load in the form of time pressure, which could help guide what topics need to be explored to best develop novel designs to address the thesis aims. As time was identified from Chapter 1 as a potential factor which could be utilised to reduce risk, it was necessary to understand how time pressure could be defined as this would go on to inform how different forms could influence the quality of applied cyber-security decision making, and whether research to date on the topic had found whether time pressure was a benefit or a risk. From having a pre-defined protocol and systematic approach to searching for literature, this reduced the possibility for bias to influence the search for relevant research to inform future directions. It also ensured a clear way of evaluating relevant literature for quality and consistent balances with the searching process and data extraction to form a qualitative narrative.

This work in Chapter 2 furthered previous reviews in the area such as Chowdhury et al. (2019) which had a less refined search strategy, focused on more objective sources of time pressure, and was somewhat outdated by the final search in the present systematic review in Chapter 2 (having searched for literature up to 2017, compared to February 2023 in the present work). There is still the possibility that relevant literature could have been missed due to the fixed search strategy, or other sources from which literature was not searched – but the search strategy was comprehensive and refined to try and capture the breadth and depth of relevant literature from a rage of databases, having tested the search terms thoroughly. Furthermore, handsearching outside of the systematic search strategy was included within the protocol for any relevant literature which could have been missed to reduce this possibility. Given the thoroughness of the approach, there can be a high level of confidence that what was found provides an excellent and unique representation of what research had been carried out which addressed the understanding of subjective time pressure in cyber-security decision making.

Identifying only 10 relevant papers which evaluated subjective time pressure in cyber-security (Cui et al., 2020; De Bona & Paci, 2020; Marett & Wright, 2009; Nthala & Flechais, 2017; Parsons et al., 2015; Trang & Nastjuk, 2021; Vishwanath et al., 2011; Wang et al., 2012; Williams, Hinds & Joinson, 2018; Wright, Marett & Thatcher, 2014) was indicative of a few key points. First and foremost, that subjective time pressure in the context of cyber-security decision making had been consistently found to be a risk factor – the opposite of what was suggested from the theoretical studies in Chapter 1. This was key because it clearly indicated this type of time pressure within the context of cyber-security could pose a risk to the quality of decisions being made, also indicating that the significance of the context in which time perception evaluated is relevant. Second, it allowed for the highlighting of key limitations to what research to date had investigated on the topic of subjective time pressure (i.e., need to examine more sources of subjective time pressure across a broader range of cyber-security behaviours, and how context may be a moderating factors in the quality of decision making in the context of phishing susceptibility). The conclusions taken from this systematic review not only contribute to current research by highlighting the directions in which wider research in the area needs to explore, but guided what empirical work was required to evaluate the topic of subjective time pressure in the context of the thesis aims.

Chapter 3: Contributions to the Thesis and Research

The systematic review to some extent addressed the aim to understand the impact of cognitive load, specifically subjective time pressure, in the context of decision-making. Although, the review clearly indicated more research needed to be conducted, based upon the previous research found, to explore a broader range of behaviours and sources of subjective time pressure. Study 6 in Chapter 3, therefore, took a new approach, considering the role of individual differences, and adopted a series of observational methods which allowed for the comparison of subjective time pressure and time perception measures with previously known predictors of cyber-security behaviours (e.g., decision-making styles – Egelman & Peer, 2015; personality - Shappie et al. 2020); as it was possible time urgency and time perception accuracy could vary between individuals. The novel applications of Chronic Time Pressure questionnaire (Denovan & Dagnall, 2019; Denovan et al., 2023) and the behavioural measure for time perception accuracy (Alison et al., 2013; Dougherty et al., 2005; Kim, Alison, & Christiansen, 2020) indicated there was variance in subjective time pressure and perception. However, only select aspects of the self-report measure were significant contributing factors to predicting specific types of cyber-security behaviours. Overall models and other contributors were broadly in line with previous research (e.g., Bishop et al., 2019; Safa et al., 2015; Shappie et al., 2020) with up to 43.5% of the variance in behaviour being explained – thus findings from Study 6 to some extent support current research findings in the area. This could go to some extent in explaining why there may be differences in decision making quality regardless of exposure to cognitive load and form the basis of the development of personas which could indicate which types of interventions could be more suitable depending upon individual differences. However, as explored within the Chapter 3 discussion and Study 7 follow up, the nature of time perception (i.e., how it changes over time) and how it is measured (i.e., wording of self-report items in respect to time scales and goals) could explain why mixed findings were found in the ability to predict cyber-security behaviour engagement.

With the findings for the time perception accuracy measure from Study 6 suggesting it may not be a useful predictor for maladaptive cyber-security behaviour, compared to what previous research in other applied areas have suggested (Alison et al., 2013; Dougherty & Hunter, 2003; Dougherty et al., 2005; Kim, Alison, & Christiansen, 2020), Study 7 consisted of a follow up to this measure used in Study 6 to evaluate why a measure for time perception accuracy may not be a useful predictor for maladaptive behaviours. Findings from Study 7 were able to indicate the calculation for time perception accuracy may not be reliable due to potential changes in time perception over time – specifically that early estimations may tend to underestimate time perception, but on average become more accuracy over time. These findings and discussions from Study 6 and 7, therefore, highlight that this measure of time perception why it may not be useful in predicting cyber-security behaviours.

From comparing VAS with Likert scales for self-report measures in Study 6, a recommendation which can be easily implemented when using self-report measures in practice could be to adopt VAS within this subfield of research, and quite possibly others. As VAS appeared to be more likely to produce normally distributed data than Likert scales with fewer rating points, it had the potential to reduce the likelihood of anchoring and adjustment bias and result in more accurate representations of relationships between variables being evaluated: a useful finding both to inform how self-report measures of cognitive load could be improved, but how self-report measures in general could be better adopted. Although, with over 60% of behaviour variance remaining unexplained for the majority of cyber-security behaviours measured, many other variables beyond individual differences needed to be explored. The empirical work in Chapter 4, therefore, need to address the third point which remained unaddressed from Chapter 2 (i.e., how context may be a moderating factors in the quality of decision making in the context of phishing susceptibility) and explore other methods of explaining variance in behaviour.

Chapter 4: Contributions to the Thesis and Research

With the need to compare motivation changes due to change in cognitive load, and how these changes related to actual behaviour, Chapter 4 tried to address the thesis aim by evaluating the significance of subjective time pressure as a persuasion technique (i.e., time urgency) in phishing susceptibility. Drawing inspiration from the review of decision making theories from Chapter 1, the limitations of research to date on urgency in phishing susceptibility in Chapter 2, and then the need to understand individual differences in motivations relating to cyber-security behaviour from Chapter 3, Studies 8-10 targeted the impact of subjective time pressure in phishing susceptibility to address the final component of the thesis aim which had not been properly addressed until this point: the development of a tool to aid the reduction of risk due to cognitive load changes in cyber-security.

Through creating a novel experimental paradigm, these final studies go beyond previous literature (e.g., De Bona & Paci, 2020; Marett & Wright, 2009; Nthala & Flechais, 2017) by not just exploring behavioural differences in phishing susceptibility due to persuasion techniques, but by considering the moderating effect of email context and hard time constraints to decision making, differences in motivation due to expected utilities of outcomes, and changes in risk perception due to availability bias. Overarching differences were found in the choice to respond/not respond to emails indicating phishing susceptibility could change due to the inclusion of both different persuasion cues within emails and differing wider email contexts. Binary logistic regressions and pairwise comparisons from probability judgements provided initial insight into granular comparisons for where consistent risks may occur.

Considering the aims of the thesis, the comparisons made highlights that cognitive load in the form of subjective time pressure in phishing susceptibility can pose a threat, though the extent of this threat may differ depending upon the wider email context in which it is situated in. However, as previously discussed, these granular pairwise comparisons should be treated with caution. Whilst they can provide some insight into specific situations, more research would be needed to support (or refute) these granular comparisons. As these pairwise comparisons highlight where some findings may be more consistent than others, future research could use these to inform which email contexts and persuasion comparisons should be compared when evaluating these factors in phishing susceptibility in a simplified version of the paradigm developed in this thesis. The evaluation of the novel introduction of the probability estimations in Study 9 indicated the perception of phishing likelihood could predict the choice to respond/not respond – suggesting this measure could be useful in predicting when time urgency or other persuasion techniques may pose more of a risk to phishing susceptibility.

The main contribution from the empirical work in Chapter 4, however, was the exploration of a novel retrospective application of EUT which appeared to be capable of explaining over two thirds (68.5%) of actual behaviour. With a high level of accuracy being detected, the phishing susceptibility EUT tool has demonstrated it holds the potential to go beyond current techniques such as phishing simulations (MetaCompliance, 2023; TitanHQ, 2023) as a means to encourage metacognitive processes as an intervention. This tool could not only highlight the risks to phishing susceptibility due to changes in different forms of cognitive load such as time urgency, but other vulnerabilities which could develop due to other contextual factors such as temporal discounting (Abdellaoui, Gutierrez, & Kemel, 2018) if developed further.

In addition to suggestions made above, next steps which were beyond the aims of the thesis could involve the development of immersive simulations and workplace studies in which knowledge and methods gained from this thesis could be applied to. This could involve the inclusion of numerous neurophysiological measures such as, but not limited to, 1) EEG technology to identify neural pathways in cognitive processing (Nicolae et al., 2017; Schreiter et al., 2019) which are noteworthy in cyber-security decision-making quality, 2) eye tracking with pupil dilation measurements indicating attention and depth of stimulus processing in more naturalistic cyber-security decisions (Langer et al., 2017; McAlaney & Hills, 2020), and 3) heart rate and skin conductance monitors to note changes in stress responses in cyber-security decision-making over time (Can, Arnrich, & Ersoy, 2019). Through adopting these measures in immersive simulations, it could be possible to gain insight into how targeted interventions, built upon the novel findings of this thesis, may be successful in reducing risky cyber-security decision making over varying periods of time in applied individual and group decision making settings. Interventions could then be tailored to individuals from examining people who come from different backgrounds (e.g., home-workers vs office workers, hybrid variations of work-home balance, general home use of technology vs work use) working in different contexts which involve varying levels, and types of, cognitive load (e.g., SOCs, IT and human resource departments).

Beyond this further, interventions will come to a limit in the ability to improve the quality of decision making due to what is within the control of the decision maker, and what remain to be biases which consistently appear despite tailored metacognitive interventions. In which case, it could then be possible the most suitable type of intervention for further decision-making improvement could be through making changes to cyber-security policies or changes to physical/user interface environments. For example, it could be the case in which a user interface (UI) does not sufficiently warn users of unsafe actions in instances which user commonly act out certain types of behaviour; or an information security policy which, despite other efforts, users still try to find work arounds for (e.g., to save time/effort). As such, once what is within the control of decision makers is intervened – UI, physical environment, and policy changes might be other areas which should be considered.

Conclusion

The key takeaway message from the current thesis is that cognitive load, namely subjective time pressure, can pose a significant threat to decision making in cyber-security – though its impact may vary depending upon the source and context. Whilst the purpose of highlighting where, when, and how these risks may occur is important, the crucial detail going forward is to note how decision making quality can be improved in practice. If the quality of a decision is determined by the combination of the suitability of the framework of the decision making process in the given circumstances, which considers the potential for desirable and undesirable outcomes coming true, combined with the quality of the information available being used, how do decision makers themselves accurately determine whether they are making the best possible decision? What information (e.g., feedback) can, and do, decision makers use to judge past, present, and future success? If the weighting of the expected utility of decision options is biased towards outcomes of decisions (Yates, Veinott, & Patalano, 2003), and motivations can be influenced by the availability of poor quality information and cognitive load (Chapters 1-4), then it should not be a surprise about the variance in decision making quality without interventions which highlight the full process of decision making. Future directions, therefore, should focus on the evaluation of user-centric tools effectiveness, such as the one created in Chapter 4, in reducing susceptibility to cognitive load through the encouragement of constructive metacognition. Through reflecting and re-assessing actions in relation to the wider aspects of decision making, decision makers could increase the overlap between reality and their subjective perception of the world – acknowledging what is, and is not, within their control over time.

References

Abdellaoui, M., Gutierrez, C., & Kemel, E. (2018). Temporal Discounting of Gains and Losses of Time: An Experimental Investigation. *Journal of Risk and Uncertainty, 57,* 1-28.

Acar, Y., Backes, M., Fahl, S., Kim, D., Mazurek, M., & Stransky, C. (2016). You Get Where You're Looking For – The Impact of Information Sources on Code Security. *International Journal of System Assurance Engineering and Management, 7*(2), 229-238.

Ahn, H-K., Liu, M. W., & Soman, D. (2006). Memory for Time: A Cognitive Model of Retrospective Duration and Sequence Judgments. *SSRN.* Retrieved from https://ssrn.com/abstract=897933

Ajzen, I. (2011). The Theory of Planned Behaviour: Reactions and Reflections. *Psychological Health, 26*(9), 1103-1127.

Ajzen, I., Brown, T. C., & Carvajal, F. (2004). Explaining the Discrepancy between Intentions and Actions: The Case of Hypothetical Bias in Contingent Valuation. *Personality and Social Psychology Bulletin, 30*(9), 1108-1121.

Akbar, N. (2014). Analysing Persuasion Principles in Phishing Emails. *Unpublished Master's Thesis,* University of Twente.

Akdemir, N., & Yenal, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open,* 1-14.

Al-Haijaa, Q. A., & Ishtaiwia, A. (2021). Machine Learning Based Model to Identify Firewall Decisions to Improve Cyber-Defence. *International Journal on Advanced Science, Engineering and Information Technology, 11*(4), 1688-1695.

Alison, L., Doran, B., Long, M. L., Power, N., & Humphrey, A. (2013). The Effects of Subjective Time Pressure and Individual Differences on Hypotheses Generation and Action Prioritization in Police Investigations. *Journal of Experimental Psychology: Applied, 19*(1), 83-93.

Allais, M. (1953). Le Comportement de l'Homme Rationnel Devant le Risque: Critique des Postulats et Axiomes de l'École Américaine [The Behaviour of the Rational Man in the Face of Risk: Criticism of the Rostulates and Rxioms of the American Rchool]. *Econometrica*, *21*(4), 503–546.

Allingham, E., Hammerschmidt, D., & Wollner, C. (2021). Time Perception in Human Movement: Effects of Speed and Agency on Duration Estimation. *Quarterly Journal of Experimental Psychology, 74*(3), 559-572.

Ambady, N., & Rosenthal, R. (1993). Half a Minute: Predicting Teacher Evaluations from Thin Slices of Nonverbal Behaviour and Physical Attractiveness. *Journal of Personality and Social Psychology, 64*(3), 431–441.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior, 69*, 437-443.

Ariely, D. (2012). The (Honest) Truth about Dishonesty. Harper Collins Publishers: New York.

Arushanyan, E. B., Baida, O. A., Mastyagin, S. S., Popova, A. P., & Shikina, I. B. (2002). Influence of Caffeine on the Subjective Perception of Time by Healthy Subjects in Dependence on Various Factors. *Human Physiology, 29*(4), 433-436.

Atkins, B., & Huang, W. (2013). A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences, 1*(3), 23-32.

Atkinson, R. C., & Shiffrin, R. M. (1968). Human Memory: A Proposed System and its Control Processes. In Spence, K.W.; Spence, J.T. (eds.). *The Psychology of Learning and Motivation*. Vol. 2. New York: Academic Press. pp. 89–195.

Ayaburi, E., & Andoh-Baidoo, F.K. (2019). Understanding Phishing Susceptibility: An Integrated Model of Cue-Utilization and Habits. *ICIS Proceedings, 43*, 3290.

Baddeley, A., & Hitch, G. (1974). Working Memory. *Psychology of Learning and Motivation, 8,* 47-89.

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018). Insider Threat: The Human Element of Cyberrisk. *McKinsey Quarterly,* 1-8.

Baldauf, D., Burgard, E., & Wittmann, M. (2009). Time Perception as a Workload Measure in Simulated Car Driving. *Applied Ergonomics, 40*(5), 929–935.

Banker, S., Ainsworth, S., Baumeister, R., Ariely, D., & Vohs, K. (2017). The Sticky Anchor Hypothesis: Ego Depletion Increases Susceptibility to Situational Cues. *Behavioral Decision Making, 30*(5), 1027-1040.

Baryshevtsev, M., & McGlynn, J. (2020). Persuasive Appeals Predict Credibility Judgments of Phishing Messages. *Cyberpsychology, Behaviour, and Social Networking, 23*(5), 297-302.

Baumeister, R. F., Heatherson, T. F., & Tice, D. M. (1994). *Losing Control: How and Why People Fail at Self-Regulaton.* (1st ed.). San Diego, CA, US: Academic Press.

Baumeister, R., Muraven, M., & Tice, D. (2000). Ego Depletion: A Resource Model of Volition, Self-Regulation, and Controlled Processing. *Social Cognition, 18*(Social Ignition: The Interplay of Motivation and Social Cognition), 130–150.

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive Behaviour in Response to Email Phishing Threats: The Roles of Rewards and Response Costs. *Computers and Security, 106*(C), 102278.

Beautement, A., Sasse, M., A., & Wonham, M. (2009). The Compliance Budget: Managing Security Behaviour in Organisations. *NSPW 2008: Proceedings of the New Security Paradigms Workshop,* 47-58.

Behm, D. G., & Carter, T. B. (2020). Effect of Exercise-Related Factors on the Perception of Time. *Frontiers in Psychology: Section of Exercise Psychology, 11*, Article No. 770.

Bernoulli, D. (1954). Exposition of a New Theory on the Measurement of Risk. *Econometrica, 22*(1), 23–36.

Bickel, W., Odum, A., & Madden, G. (1999). Impulsivity and Cigarette Smoking: Delay Discounting in Current, Never, and Ex-smokers. *Psychopharmacology, 4*, 447–454.

Bishop, L. M., Asquith, P. M., & Morgan, P. L. (2022). The Prevalence and Success Rates of Persuasion Techniques Employed in Phishing Emails. *Airbus Internal Report. Airbus and Endeavr Wales,* 1-42.

Bishop, L.M., Morgan, P.L., Asquith, P.M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). Examining Human Individual Differences in Cyber Security and Possible Implications for Human-Machine Interface Design. In: Moallem A. (eds) *HCI for Cybersecurity, Privacy and Trust*. *HCII 2020. Lecture Notes in Computer Science, vol 12210*. Springer, Cham.

Blais, A. R., & Weber, E. U. (2006). A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations. *Judgement and Decision Making, 1*(1), 33-47.

Block, F., & Gellersen, H. (2010). The Impact of Cognitive Load on the Perception of Time. *NordiCHI '10: Proceedings on the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries*, 607-610.

Blotner, C., & Bergold, S. (2023). It is Double Please to Deceive the Deceiver: Machiavellianism is Associated with Producing but not Necessarily with Falling for Bullshit. *British Journal of Social Psychology, 62*(1), 467-485.

Borkenau, P., Brecke, S., Möttig, C., & Paelecke, M. (2009). Extraversion is Accurately Perceived after a 50-ms Exposure to a Face. *Journal of Research in Personality, 43*(4), 703-706.

Bowman, C. H., Evans, C. E. Y., & Turnbull, O. H. (2005). Artificial Time Constraints on the Iowa Gambling Task: The Effects on Behavioural Performance and Subjective Experience. *Brain & Cognition, 57*(1), 21-25.

Brand, M. (2019). Mine Games: Cognitive Bias, US Intelligence, and the 1968 Soviet Invasion of Czechoslovakia. *Intelligence and National Security, 34*(5), 743-757.

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies, 2022*, 2693080.

Brown, J., & Gallagher, F. (1992). Coming to Terms with Failure: Private Self-Enhancement and Public Self-Effacement. *Journal of Experimental Social Psychology, 28*(1), 3–22.

Brown, A., Imai, T., Vieider, F., & Camerer, C. (2021). Meta-Analysis of Empirical Estimates of Loss-Aversion. *CESifo Working Paper No. 8848.*

Brown, G. D. A., Neath, I., & Chater, N. (2007). A Temporal Ratio Model of Memory. *Psychological Review, 114*(3), 539-576.

Brunken, L., Buckmann, A., Hielscher, J., & Sasse, M. A. (2023). “To Do This Properly, You Need More Resources”: The Hidden Costs of Introducing Simulated Phishing Campaigns. *Proceedings of the 32nd USENIX Security Symposium,* 4105-4122.

Brunswik, E. (1956). *Perception and the Representative Design of Psychological Experiments.* (2nd ed.). Berkeley: University of California Press.

Buehler, R., Griffin, D., & Ross, M. (1994). Exploring the "Planning Fallacy": Why People Underestimate their Task Completion Times. *Journal of Personality and Social Psychology, 67*(3), 366–381.

Buehner, M., & Townsend, E. (2015). Rude Assessment and I’m Faking It: Does Witnessing Incivility Compel People to Cheat? *Assessment and Development Matters, 7*(4), 20-24.

Buffardi, L. (1971). Factors Affecting the Filled-Duration Illusion in the Auditory, Tactual, and Visual Modalities. *Perception & Psychophysics, 10*, 292-294.

Burt, C. D. B., & Kemp, S. (1994). Construction of Activity Duration and Time Management Potential. *Applied Cognitive Psychology, 8*(2), 155–168.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails. In: *Australasian Conference on Information Systems (ACIS) Proceedings.* arXiv:1606.00887

Butavicius, M., Taib, R., & Han, S.J. (2022). Why People Keep Falling for Phishing Scams: The Effects of Time Pressure and Deception Cues on the Detection of Phishing Emails. *Computers & Security, 123,* 102937.

Can, Y., S, Arnrich, B., & Ersoy, C. (2019). Stress Detection in Daily Life Scenarios using Smart Phones and Wearable Sensors: A Survey. *Journal of Biomedical Informatics, 92,* Article No. 103139.

Capraro, V. (2017). Does the Truth Come Naturally? Time Pressure Increases Honesty in One-Shot Deception Games. *Economic Letters*, *158,* 54-57.

Capraro, V., Schulz, J., & Rand, D. G. (2019). Time Pressure and Honesty in a Deception Game. *Journal of Behavioral and Experimental Economics, 79*, 93-99.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy & Security, 1*(3), 18-41.

Chen, Y., Peng, Y., Xu, H., & O'Brien, W. H. (2018). Age Differences in Stress and Coping: Problem-Focused Strategies Mediate the Relationship Between Age and Positive Affect. *The International Journal of Aging and Human Development, 86*(4), 347–363.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, *29*(3), 157-188.

Choi, D. W., Chun, S. Y., Lee, S. A., Han, K. T., & Park, E. C. (2018). Association between Sleep Duration and Perceived Stress: Salaried Worker in Circumstances of High Workload. *International Journal of Environmental Research and Public Health*, *15*(4), 796.

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The Impact of Time Pressure on Cybersecurity Behaviour: A Systematic Review. *Behaviour & Information Technology, 38*(12), 1290-1308.

Chowdhury, N., Adam, M., & Teubner, T. (2020). Time Pressure in Human Cybersecurity Behavior: Theoretical Framework and Countermeasures. *Computers & Security, 97*(3), Article No. 101963.

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2023). Rushed to Crack - On the Perceived Effectiveness of Cybersecurity Measures for Secure Behaviour under Time Pressure. *Behaviour & Information Technology, 42*(10), 1568-1589.

Cialdini, R. B. (2009). *Influence: Science and practice*. Boston: Pearson Education.

Ciernak, G., Scheiter, K., & Gerjets, P. (2009). Explaining the Split-Attention Effect: Is the Reduction of Extraneous Cognitive Load Accompanied by an Increase in Germane Cognitive Load? *Computers in Human Behavior, 25*(2), 315-324.

Cofense. (2022). *2022 Annual State of Email Security Report: It's Always a Phish*. Retrieved from https://cofense.com/wp-content/uploads/2023/01/2022-AnnualReport-Final-Web.pdf

Corvi, A. P., Jeurgensen, J., Weaver, J. S., Demaree, H. A. (2012). Subjective Time Perception and Behavioral Activation System Strength predict Delay of Gratification Ability. *Motivation and Emotion, 36*, 483-490.

Crescenzi, A., Capra, R., & Arguello, J. (2014). Time Pressure, User Satisfaction and Task Difficulty. *Proceedings of the American Society for Information Science and Technology, 50*(1), 1-4.

Cowan, N. (1988). An Embedded-Processes Model of Working Memory. In Miyake, A., and Shah, P. *Models of Working Memory: Mechanisms of Active Maintenance and Executive Control*. Cambridge University Press.

Cowan N (1995). *Attention and Memory: An Integrated Framework*. Oxford [Oxfordshire]: Oxford University Press.

Cowan, N. (2001). The Magical Number 4 in Short-Term Memory: A Reconsideration of Mental Storage Capacity. *Behavioral and Brain Sciences, 24*(1), 87-114.

Cui X., Ge Y., Qu W., & Zhang K. (2020) Effects of Recipient Information and Urgency Cues on Phishing Detection. In: Stephanidis C., Antona M. (eds) *HCI International 2020 - Posters*. *HCII 2020. Communications in Computer and Information Science, vol 1226*. Springer, Cham.

CybSafe. (2020, February 7). *Human Error to Blame for 9 in 10 UK Cyber Data Breaches in 2019* [Press release]. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

Darshan, K. R., & Anandakumar, K. R. (2015, December). A Comprehensive Review on Usage of Internet of Things (IoT) in Healthcare System. In *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)* (pp. 132-136). IEEE.

Danet, D. (2020). Punish and Perish: The Human Factor in Cybersecurity. *Proceedings of the Italian Conference on Cybersecurity (ITASEC21) All Digital Event, April 7-9 2021*, 1-8.

De Becker, P., Roeykens, J., Reynders, M., McGregor, N., & De Meirleir, K. (2000). Exercise Capacity in Chronic Fatigue Syndrome. *Archives of Internal Medicine., 160*(21), 3270-3277.

De Bona, M., & Paci, F. (2020). A Real World Study on Employees' Susceptibility to Phishing Attacks. In *The 15th International Conference on Availability, Reliability and Security* (ARES 2020), August 25-28, 2020, Virtual Event, Ireland. ACM, New York, NY, USA, 10 pages.

DeDonno, M. A., & Demaree, H. A. (2008). Perceived Time Pressure and the Iowa Gambling Task. *Judgment and Decision Making, 3*(8), 636-640.

Denovan, A., & Dagnell, N. (2019). Development and Evaluation of the Chronic Time Pressure Inventory. *Frontiers in Psychology, 10*, Article No. 2717.

Denovan, A., Dagnall, N., Drinkwater, K., & Escola-Gascon, A. (2023). Evaluating the Psychometric Properties of the Chronic Time Pressure Inventory using Rasch Analysis. *PeerJ, 11,* e15218.

Dertwinkel-Kalt, M., & Koster, M. (2019). Salience and Skewness Preferences. *CESifo Working Paper Series,* No. 7416.

Di Lernia, D., Serino, S., Pezzulo, G., Pedroli, E., Cipresso., P., & Riva, G. (2018). Feel the Time: Time Perception as a Function of Interoceptive Processing. *Frontiers in Human Neuroscience, 12,* 74.

Dougherty, M. & Hunter, J. (2003). Probability Judgment and Subadditivity: The Role of Working Memory Capacity and Constraining Retrieval. *Memory & Cognition, 31*(6), 968-982.

Dougherty, M., Mathias, C. W., & Marsh, D. M. (2005). Laboratory Behavioral Measures of Impulsivity. *Behavior Research Methods, 37*(1), 82-90.

Drèze, J., & Stern, N. (1987). The theory of cost-benefit analysis. In *Handbook of public economics* (Vol. 2, pp. 909-989). Elsevier.

Dykstra, J., & Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying Fatigue, Frustration, and Cognitive Workload in Cybersecurity Operations. In *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18).*

Eddy, M., Hasselquist, L., Giles, G., Hayes, J., Howe, J., Rourke, J., et al. (2015). The Effects of Load Carriage and Physical Fatigue on Cognitive Performance. *PLoS ONE, 10*(7), e0130817.

Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (sebis). *In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM*, 2873-2882

Ellsberg, D. (1961). Risk, Ambiguity, and the Savage Axioms. *Quarterly Journal of Economics*. *75*(4), 643–669.

Eze, C. S., & Shamir, L. (2024). Analysis and Prevention of AI-Based Phishing Email Attacks. *Electronics, 13*(10), 1839.

Fagan, M., Albayram, Y., Khan, M., M., H., & Buck, R. (2017). An Investigation into Users' Considerations towards using Password Managers. *Human-Centric Computing and Information Sciences, 7*, Article No. 12.

Falk, A., & Hermle, J. (2018). Relationship of Gender Differences in Preferences to Economic Development and Gender Equality. *Science, 362*(6412), eaas9899.

Faro., D., Leclerc, F., & Hastie, R. (2005). Perceived Causality as a Cue to Temporal Distance. *Psychological Science, 16*(9), 673-677.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical Power Analyses using G*Power 3.1: Tests for Correlation and Regression Analyses. *Behavior Research Methods, 41*, 1149-1160.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, and Biomedical Sciences. *Behavior Research Methods, 39*, 175-191.

Fereday, R., Buehner, M. J., & Rushton, S. K. (2019). The Role of Time Perception in Temporal Binding: Impaired Temporal Resolution in Causal Sequences. *Cognition, 193*, Article No. 104005.

Fine, T., & Vajsbaher, T. (2013). How Good are Groups at Estimating Time? *Proceedings of the International Symposium on Performance Science 2013*, 741-746.

Flavell, J. H. (1985). *Cognitive Development*. Englewood Cliffs, NJ: Prentice Hall.

Giacobe, N., McNeese, M., Mancuso, V., & Minotra, D. (2013). Capturing Human Cognition in Cyber-Security Simulations with NETS. *2013 IEEE International Conference on Intelligence and Security Informatics*, 284-288.

Gable, P. A., Wilhelm, A. L., & Poole, B. D. (2022). How does Emotion Influence Time Perception? A Review of Evidence Linking Emotional Motivation and Time Processing. *Frontiers in Psychology, 13*, 848154.

Giger, J., & Pochwatko. G. (2008). Sometimes It Is Not So Bad to Decide in a Hurry: Influence of Different Levels of Temporal Opportunity on the Elaboration of Purchasing Intention. *Polish Psychological Bulletin, 39*(4), 209–216.

Gino, F., Ayal, S., & Ariely, D. (2009). Contagion and Differentiation in Unethical Behaviour: The Effect of One Bad Apple on the Barrel. *Psychological Science, 20*(3), 393–398.

Gino, F., Ayal, S., & Ariely, D. (2013). Self-Serving Altruism? The Lure of Unethical Actions that Benefit Others. *Journal of Economic Behavior & Organization, 93*, 10.1016/j.jebo.2013.04.005.

Gino, F., & Mogilner, C. (2014). Time, Money, and Morality. *Psychological Science, 25*(2), 414-421.

Gino, F., Schweitzer, M., Mead, N., & Ariely, D. (2011). Unable to Resist Temptation: How Self-Control Depletion Promotes Unethical Behaviour. *Organizational Behaviour and Human Decision Processes*, *115*, 191–203.

Goldreich, D. (2007). A Bayesian Perceptual Model Replicates the Culaneous Rabbit and Other Tactile Spatiotemporal Illusions. *PLoS One, 2*(3), e333.

Gonzalez, C. (2004). Learning to Make Decisions in Dynamic Environments: Effects of Time Constraints and Cognitive Abilities. *Human Factors, 46*(3), 449-460.

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, *2*(3), e190393

Grasmick, H., Tittle, G., Bursik Jr., R., & Arneklev, B. (1993). Testing the Core Implications of Gettfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency*, *30*(1), 5-29.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2017). Correlating Human Traits and Cybersecurity Behaviour Intentions. *Computers and Security, 73*, 345-358.

Greenberg, J., & Pyszczynski, T. (1985). Compensatory Self-inflation: A Response to the Threat to Self-regard of Public Failure. *Journal of Personality and Social Psychology, 49*(1), 237–280.

Greeno, D., Asquith, P. M., & Morgan, P. L. (2022). Cyber Security Language Repository (CSLR): Creating a Word Norms Database for Specialised Cyber Security Language. *Airbus Internal Report. Airbus and Endeavr Wales*, 1-59.

Grieco, D., & Hogarth, R. (2009). Overconfidence in Absolute and Relative Performance:

The Regression Hypothesis and Bayesian Updating. *Journal of Economic Psychology, 30*(5), 756–771.

Griffiths, C. (2023). *The Latest 2023 Phishing Statistics (Updated January 2023). AAG*. Retrieved from https://aag-it.com/the-latest-phishing-statistics/

Groot, W., & van den Brink, H. M. (2010). The Effects of Education on Crime. *Applied Economics, 42*(3), 279-289.

Hagger, M. S., Wood, C., Stiff, C., & Chatzisarantis, N. L. D. (2010). Ego Depletion and the Strength Model of Self-Control: A Meta-Analysis. *Psychological Bulletin, 136*(4), 495–525.

Hald, A. (1990). The Foundation of Probability Theory by Pascal and Fermat in 1654. In A. Hald (Ed.), *History of Probability and Statistics and Their Applications before 1750*, (pp. 42-64).

Harrison, J., Toreini, E., & Mehrnezhad. (2023). A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards. *2023 IEEE Symposium on Security and Privacy Workshops (EuroS&PW),* Delft, Netherlands, 270-280.

Hart, S., & Staveland, L. (1988). Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. *Advances in Psychology*, *52*, 139–183.

Heatherton, T., & Ambady, N. (1993). Self-Esteem, Self-Prediction, and Living up to Commitments. *In Self-Esteem* (pp. 131–145). Springer, Boston, MA.

Henrich, J., Boyd, R., Bowles, S., Camerer, C., Fehr, E., Gintis, H., & McElreath, R. (2001). In Search of Homo Economicus: Behavioral Experiments in 15 Small-Scale Societies. *American Economic Review*, *91*(2), 73–78.

Herawati, K., & Gayatri, D. (2019). The Correlation between Sleep Quality and Levels of Stress among Students in Universitas Indonesia. *Enfermeria Clinica*, *29*(2), 357-361.

Herman, A. M., Critchley, H. D., & Duka, T. (2018). Risk-Taking and Impulsivity: The Role of Mood States and Interoception. *Frontiers in Psychology*, *9*, Article No. 1625.

Heyes, S. B., Adam, R. J, Urner, M., Van der Leer, L., Bahrami, B., Bays, P. M., & Husain, M. (2012). Impulsivity and Rapid Decision-Making for Reward. *Frontiers in Psychology, 3*, Article No. 153.

Hodgetts, H. M., & Jones, D. M. (2006). Interruption of the Tower of London Task: Support for a Goal-Activation Approach. *Journal of Experimental Psychology: General, 135*(1), 103–115.

Hoerl, C., Lorimer, S., McCormack, T., Lagnado, D. A., Blakey, E., Tecwyn, E. C., & Buehner, M. J. (2020). Temporal Binding, Causation, and Agency: Developing a New Theoretical Framework. *Cognitive Science, 44*(5), e12843.

Hu, Q., West, R., & Smarandescu, L. (2015). The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective. *Journal of Management Information Systems*, *31*(4), 6-48.

Hunter, L., & Thatcher, S. (2007). Feeling the Heat: Effects of Stress, Commitment, and Job Experience on Job Performance. *Academy of Management Journal*, *50*(4), 953-968.

Ilic, J., Radovic, K., Savic-Stankovic, T., Popovac, A., Miletic, V., & Lemic, A. M. (2021). The Effect of COVID-19 Pandemic on Final Year Dental Students' Self-confidence Level in Performing Clinical Procedures. *PloS One*, *16*(10): e0257359.

Jex, S. M. (1998). *Stress and Job Performance: Theory, Research, and Implications for Managerial Practice.* Thousand Oaks, CA: Sage.

Jiang, Q., Zhang, Y., Zhu, Z., Zhang, J., Ding, K., & Liu, J. (2023). Is Dishonesty Normally Distributed? Evidence from Six Behavioral Experiments and Simulation Study. *Personality and Individual Differences, 205*, 112105.

Jones, D. M., & Macken, B. (2018). In the Beginning Was the Deed: Verbal Short-Term Memory as Object-Oriented Action. *Current Directions in Psychological Science*, *27*(5), 351–356.

Jones H., S., Towse, J., N., Race, N., & Harrison, T. (2019). Email Fraud: The Search for Psychological Predictors of Susceptibility. *PLoS ONE, 14*(1): e0209684.

Jeske, D., Briggs, P., & Coventry, L. (2016). Exploring the Relationship Between Impulsivity and Decision-Making on Mobile Devices. *Personal and Ubiquitous Computing*, *20*(4): 545–557.

Kahn, A., Sharma, N. K., & Dixit, S. (2006). Effect of Cognitive Load and Paradigm on Time Perception. *Journal of the Indian Academy of Applied Psychology, 32*(1), 37-42.

Kahneman, D. (2011). *Thinking, Fast and Slow*. New York, NY, US: Farrar, Straus, and Giroux.

Kahneman, D., & Tversky, A. (1977). Intuitive Prediction: Biases and Corrective Procedures. *TIMS Studies in Management Science, 12*, 313-327.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263–291.

Karau, S. J., & Kelly, J. R. (1992). The Effect of Time Scarcity and Time Abundance on Group Performance Quality and Interaction Process. *Journal of Experimental Social Psychology, 28*(6), 542-571.

Keizer, K., Lindenberg, S. & Steg, L. (2008). The Spreading of Disorder. *Science, 322*(5908), 1681-1685.

Kelly, J. R., & McGrath, J. E. (1985). Effects of Time Limits and Task Types on Task Performance and Interaction of Four-Person Groups. *Journal of Personality and Social Psychology, 49*(2), 395–407.

Kennedy, J. A., & Kray, L. J. (2022). Gender Similarities and Differences in Dishonesty. *Current Opinion in Psychology, 48*, 101461.

Kim, S., Alison, L., & Christiansen, P. (2020). The Impact of Individual Differences on Investigative Hypothesis Generation under Time Pressure. *International Journal of Police Science & Management, 22*(2), 171-182.

Kim, J., & Park, N. (2020). Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments. *Applied Sciences, 10*(14), 4718.

Kirlappos, I., & Sasse, M., A. (2012). Security Education Against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security & Privacy, 10*(2), 24–32.

Kirlappos, I., Parkin, S., & Sasse, M., A. (2014). Learning from "Shadow Security": Why Understanding Non-Compliance Provides the Basis for Effective Security. In *(Proceedings) Workshop on Usable Security*. Retrieved from https://discovery.ucl.ac.uk/id/eprint/1424472

Kleiner, S. (2014). Subjective Time Pressure: General or Domain Specific? *Social Science Research, 47*, 108-120.

Kristal, A. S., Whillans, A. V., Bazerman, M. H., Gino, F., Shu, L. L., Mazar, N., & Ariely, D. (2020). Signing at the Beginning Versus at the End does not Decrease Dishonesty. *Psychological and Cognitive Sciences, 117*(13), 7103-7107.

Kourouxous, T., & Bauer, T. (2019). Violations of Dominance in Decision-Making. *Business Research, 12*, 209-239.

Kuroda, T., Grondin, S., Miyazaki, M., Ogata, K., & Tobimatsu, S. (2016). The Kappa Effect with only Two Visual Markers. *Multisensory Research, 29*(8), 703–725.

Lake, J. I., LaBar, K. S., & Meck, W. H. (2016). Emotional Modulation of Interval Timing and Time Perception. *Neuroscience & Biobehavioral Reviews, 64*, 403-420.

Langer, N., Ho, E. J., Alexander, L. M., Xu, H. Y., Jozanovic, R. K., Henin, S., Petroni, A., Cohen, S., Marcelle, E. T., Parra, L. C., Milham, M. P., & Kelly, S. P. (2017). A Resource for Assessing Information Processing in the Developing Brain using EEG and Eye Tracking. *Scientific Data, 4*: 170040.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behaviour. *International Journal of Information Management, 45,* 13-24.

Li, W., Lee, J., Purl, J., Greitzer, F. L., Yousefi, B., & Laskey, K. B. (2020). Experimental Investigation of Demographic Factors related to Phishing Susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2240-2249.

Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A Survey. *Information Systems Frontiers, 17*(2), 243-259.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction: A Publication of the Association for Computing Machinery,* 26(5), 32.

Loftus, E., & Palmer, J. (1974). Reconstruction of Automobile Destruction: An Example of the Interaction between Language and Memory. *Journal of Verbal Learning and Verbal Behavior, 13*(5), 585-589.

Loomes, G. (1989). Predicted Violations of the Invariance Principle in Choice Under Uncertainty. *Annals of Operations Research, 19,* 103-113.

Machiavelli, N., 1469-1527. (1981). *The Prince*. Harmondsworth, Eng.; New York, N.Y.: Penguin Books.

Mandel, D. R., Karvetski, C. W., & Dhami, M. K. (2018). Boosting Intelligence Analysts' Judgment Accuracy: What Works, What Fails? Judgment and Decision Making, 13(6), 607-621.

Marcus, A. (2021). Highly Criticized Paper on Dishonest Retracted. Retrieved from https://retractionwatch.com/2021/09/14/highly-criticized-paper-on-dishonesty-retracted/

Marett, K., & Wright, R. (2009). The Effectiveness of Deceptive Tactics in Phishing. *AMCIS 2009 Proceedings.* Paper 340.

McAlaney, J. & Hills, P. (2020). Understanding Phishing Email Processing and Perceived Trustworthiness through Eye Tracking. *Frontiers in Psychology, 11,* Article No. 1756.

McGill, T., & Thompson, N. (2017). Old Risks, New Challenges: Exploring Differences in Security between Home Computer and Mobile Device Use. *Behaviour & Information Technology, 36*(11), 1111-1124.

Mead, N., Baumeister, R., Gino, F., Schweitzer, M., & Ariely, D. (2009). Too Tired to Tell the Truth: Self-Control Resource Depletion and Dishonesty. *Journal of Experimental Social*

Psychology, *45*, 594–597.

MetaCompliance (2023). *Cyber Security Behavioural Maturity Model.* https://www.metacompliance.com

Metcalfe, J., & Shimamura, A. P. (1994). *Metacognition: Knowing about Knowing*. Cambridge, MA: MIT Press.

Miller, G. A. (1956). The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information. *Psychological Review*, *63*(2), 81–97.

Mizar, N., Amir, O., & Ariely, D. (2008). The Dishonesty of Honest People: A Theory of Self-Concept Maintenance. *Journal of Marketing Research*, *45*, 633–644.

Moore, D. A., & Tenney, E. R. (2012). Time Pressure, Performance, and Productivity. *Research on Managing Groups and Teams*, *15*, 305–326.

Moore, L., Wilson, M., McGrath, J., Waine, E., Masters, R., & Vine, S. (2015). Surgeons' Display Reduced Mental Effort and Workload While Performing Robitically Assisted Surgical Tasks, when Compared to Conventional Laparoscopy. *Surgical Endoscopy, 29,* 2553-2560.

Morgan, P. L., & Asquith, P. M. (2021). Airbus Cyber Security Behaviours Tool: Experimental Findings and Recommendations. *Airbus Internal Report. Airbus and Endeavr Wales*, 1-76.

Morgan P.L., Asquith P.M., Bishop L.M., Raywood-Burke G., Wedgbury A., Jones K. (2020). A New Hope: Human-Centric Cybersecurity Research Embedded Within Organizations. In: Moallem A. (eds) *HCI for Cybersecurity, Privacy and Trust. HCII 2020. Lecture Notes in Computer Science, vol 12210*. Springer, Cham

National Cyber Security Centre. (2016). NCSC Glossary. Received from https://www.ncsc.gov.uk/files/NCSC_glossary.pdf

Neu, D., Kajosch, H., Peigneux, P., Verbanck, P., Linkowski, P., & Le Bon, O. (2010). Cognitive Impairment in Fatigue and Sleepiness Associated Conditions. *Psychiatry Research*, *189*(1), 128–134.

News 13. (2022). The Source, Season 21, Episode 19: The Lie Investigator (Translated from Hebrew). Retrieved from https://13tv.co.il/item/news/hamakor/season-21/episodes/veo9a-903318236/ on November 22nd 2022.

Nicolae, I. E., Acqualagna, L., & Blankertz, B. (2017). Assessing the Depth of Cognitive Processing as the Basis for Potential User-State Adaptation. *Frontiers in Neuroscience, 11,* 548.

Nordqvist, S., Hovmark, S., & Zita-Viktorsson, A. (2004). Perceived Time Pressure and Social Processes in Project Teams. *International Journal of Project Management*, *22*(6), 463-468.

Norris, G., & Brookes, A. (2021). Personality, Emotion and Individual Differences in response to Online Fraud. *Personality and Individual Differences, 169*, Article No. 109847.

Nthala, N., & Flechais, I. (2017). "If it's urgent or it is stopping me from doing something, then I might just go straight at it": A Study Into Home Data Security Decisions. In: Tryfonas T. (eds) *Human Aspects of Information Security, Privacy and Trust*. *HAS 2017. Lecture notes in computer science, vol 10292*. Springer, Cham.

Nurse, J., Giddens, J., & Alashe, O. (2020). *Meaningful Cybersecurity Metrics for Human Cyber Risk*. Retrieved from https://www.cybsafe.com/whitepapers/meaningful-metrics-whitepaper/

Nuyens, F. M., Billieux, J., & Maurage, P. (2021). Time Perception and Alcohol Use: A Systematic Review. *Neuroscience & Biobehavioral Reviews, 127*, 377-403.

Odum, A. (2011). Delay Discounting: I'm a K, you're a K. *Journal of the Experimental Analysis of Behaviour, 96*(3), 427–439.

Ogden, R. (2022). Are We Nearly There Yet? Why Long Car Journeys are so Excruciating for Your Kids. *The Conversation*. ISSN 2201-5639

Ogden, R., Dobbins, C., Slade, K., McIntyre, J., & Fairclough, S. (2022). The Psychophysiological Mechanisms of Real-world Time Experience. *Scientific Reports, 12*, Article No. 12890.

Ogden, R., Henderson, J., McGlone, F., & Richter, M. (2019). Time Distortion Under Threat: Sympathetic Arousal Predicts Time Distortion only in the Context of Negative, Highly Arousing Stimuli. *PLoS ONE, 14*(5), e0216704.

Ogden, R., & Faulkner, J. (2022). The Influence of Recreational Drug Use on Experiences of the Passage of Time. *SUCHT, 68*(2), 65-74.

Okamoto. (2015). SecondDEP: Resilient Computing that Prevents Shellcode Execution in Cyber-Attacks. *Procedia Computer Science, 60*, 691-699.

Oliver, A. (2003). A Quantitative and Qualitative Test of the Allais Paradox using Health Outcomes. *Journal of Economic Psychology, 24*(1), 35-48.

Onwubiko, C., & Ouazzane, K. (2020). SOTER: A Playbook, for Cybersecurity Incident Management. *IEEE Transactions on Engineering Management, 69*(6), 3771-3791.

Ordonez, L., & Benson, L. III. (1997). Decisions under Time Pressure: How Time Constraint Affects Risky Decision Making. *Organisational Behavior and Human Decision Processes, 71*(2), 121-140.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Moher, D. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *British Medical Journal, 372*, Article No. 71.

Parkinson, C. N. (1957). *Parkinson's Law, and Other Studies in Administration*. Boston: Houghton Mifflin.

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting Susceptibility to Social Influence in Phishing Emails. *International Journal of Human-Computer Studies*, *128*, 17-26.

Parsons, K., Butavicius, M., Pattinson, M., McCormac, A., Calic, D, & Jerram, C. (2015). Do Users Focus on the Correct Cues to Differentiate between Phishing and Genuine Emails? In: *Australasian Conference on Information Systems.* arXiv:1605.04717.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., Jerram, C. (2013). Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In: Janczewski, L.J., Wolfe, H.B., Shenoi, S. (eds) *Security and Privacy Protection in Information Processing Systems*. *SEC 2013. IFIP Advances in Information and Communication Technology, vol 405*. Springer, Berlin, Heidelberg.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information

Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129.

Patton, J. H., Stanford, M. S., & Barratt, E. S. (1995). Factor Structure of the Barratt Impulsiveness Scale. *Journal of Clinical Psychology*, *51*(6), 768-774.

Peirce, J. W., Gray, J. R., Simpson, S., MacAskill, M. R., Höchenberger, R., Sogo, H., Kastman, E., Lindeløv, J. (2019). PsychoPy2: Experiments in Behavior Made Easy. *Behavior Research Methods,* 10.3758/s13428-018-01193-y

Pluye, P., Robert, E., Cargo, M., Bartlett, G., O'Cathain, A., Griffiths, F., Boardman, F., Gagnon, M. P., & Rousseau, M.C. (2011). Proposal: A Mixed Methods Appraisal Tool for Systematic Mixed Studies Reviews. Retrieved from http://mixedmethodsappraisaltoolpublic.pbworks.com

Primer, A. T. (2009). Structured Analytic Techniques for Improving Intelligence Analysis. CIA Center for the Study of Intelligence.

Prolific. (2022). Prolific Academic Ltd., Oxford, UK. www.prolific.com

Proofpoint (2020). 2020 State of the Phish. Available at: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish- 2020.pdf

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems, 32*(4), 179-214.

Quinn, R. (2023). *Harvard Dishonesty Researcher Now on Administrative Leave.* Inside Higher Ed. https://www.insidehighered.com/news/quick-takes/2023/06/21/harvard-dishonesty-researcher-now-administrative-leave

Ranyard, R. H. (1977). Risky Decisions which Violate Transitivity and Double Cancellation. *Acta Psychologica, 41*(6), 449-459.

Raywood-Burke G., Bishop L.M., Asquith P.M., Morgan P.L. (2021) Human Individual Difference Predictors in Cyber-Security: Exploring an Alternative Scale Method and Data Resolution to Modelling Cyber Secure Behavior. In: Moallem A. (eds) *HCI for Cybersecurity, Privacy and Trust*. HCII 2021. Lecture Notes in Computer Science, vol 12788. Springer, Cham.

Raywood-Burke, G., Jones, D., Morgan, P. (2023). Maladaptive Behaviour in Phishing Susceptibility: How Email Context Influences the Impact of Persuasion Techniques. *In: Abbas Moallem (eds) Human Factors in Cybersecurity. AHFE (2023) International Conference. AHFE Open Access, vol 91.* AHFE International, USA.

Regan, J. W., Gosselink, H., Hubsch, J., & Ulsh, E. (1975). Do People have Inflated Views of their own Ability? *Journal of Personality and Social Psychology, 31*(2), 295.

Rogers, R.W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In: Cacioppo BL, Petty LL, editors. In: Social Psychophysiology: A Source Book. London: Guildford Press, 153–76.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection Motivation Theory. In D. S. Gochman (Ed.), *Handbook of Health Behavior Research 1: Personal and Social Determinants* (pp. 113–132). Plenum Press.

Roy, M., Christenfeld, N., & McKenzie, C. (2005). Underestimating the Duration of Future Events: Memory Incorrectly Used or Memory Bias? *Psychological Bulletin, 131*(5), 738-756.

Rudolph, C. W., Katz, I. M., Lavigne, K. N., & Zacher, H. (2017). Job Crafting: A Meta-Analysis of Relationships with Individual Differences, Job Characteristics, and Work Outcomes. *Journal of Vocational Behavior, 102*, 112-138.

Rundo, J. V., & Downey 3rd, R. (2019). Polysomnography, *Handbook of Clinical Neurology, 160*, 381-392.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organisations. *Computers and Security*, 53, 65-78.

Savage, L. J. (1954). *The Foundations of Statistics*. New York, Wiley.

Schmeichel, B. J. (2007). Attention Control, Memory Updating, and Emotion Regulation Temporarily Reduce the Capacity for Executive Control. *Journal of Experimental Psychology: General*, 136, 241–255.

Schreiter, M., L., Chmielewski, W., X., Muckschel, M., Ziemssen, T., & Beste, C. (2019). How the Depth of Processing Modules Emotional Interference – Evidence from EEG and Pupil Diameter Data. *Cognitive, Affective, and Behavioral Neuroscience, 19*, 1231-1246.

Scott, S. G., & Bruce, R. A. (1995). Decision-Making Style: The Development and Assessment of a New Measure. *Educational and Psychological Measurement, 55*(5), 818-831.

Sedikides, C., Campbell, K., Reeder, G., & Elliot, A. (1998). The Self-serving Bias in Relational Context. *Journal of Personality and Social Psychology*, *74*(2), 378–386.

Sen, B., Kurtaran, & Ozturk, L. (2023). The Effect of 24-Hour Sleep Deprivation on Subjective Time Perception. *International Journal of Psychophysiology, 192*, 91-97.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media, 9*(4), 475–480.

Shu, L., Mazar, N., Gino, F., Ariely, D., & Bazerman, M. (2012). Signing at the Beginning makes Ethics Salient and Decreases Dishonest Self-Reports in Comparison to Signing at the End. *Psychological and Cognitive Sciences, 109*(38), 15197-15200.

Simon, H. (1957). *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*. (2nd ed.). New York, NY, US: Macmillan.

Singh & Silakari. (2009). A Survey of Cyber Attack Detection Systems. *International Journal of Computer Science and Network Security, 9*(5), 1-10.

Sommestad, T. Karlzen, H., & Hallberg, J. (2015). The Sufficiency of Theory of Planned Behaviour for Explaining Information Security Policy Compliance. *Security Culture and Information Technology, 23*(2), 200-217.

Stachele, T., Domes, G., Wekenborg, M., Penz, M., & Kirschbaum, C. (2020). Effects of a 6-Week Internet-Based Stress Management Program on Perceived Stress, Subjective Coping Skills, and Sleep Quality. *Frontiers in Psychiatry, 11*, 463.

Stein, E. M. (2016). Do I have Enough Time? The Effects of Perceived Time Difficulty and Perceived Time Pressure on Cognitive Performance, *Unpublished Master's Thesis,* University of Texas at Austin, USA. Retrieved from http://hdl.handle.net/2152/45693

Stewart, N. (2009). The Cost of Anchoring on Credit-Card Minimum Repayments. *Psychological Science, 20*(1), 39–41.

Stewart, N., Chater, N., & Brown, G. (2006). Decision by Sampling. *Cognitive Psychology, 53*(1), 1-26.

Stilgherrian (2018). *Australian Government Lags UK in Deploying DMARC Email Spoofing Prevention.* https://www.zdnet.com/article/australian-government-lags-uk-in-deploying-dmarc-email-spoofing-prevention/

Stojmenovic, M., Spero, E., Stojmenovic, M., & Biddle, R. (2022). What is Beautiful is Secure. *ACM Transactions on Privacy and Security, 25*(4), 1-30.

Sturman, D., Valenzuela, C., Plate, O., Tanvir, T., Auton, J.C., Bayl-Smith, P., & Wiggins, M.W. (2023). The Role of Cue Utilization in the Detection of Phishing Emails. *Applied Ergonomics, 106,* 103887.

Sun, J. C-Y., & Yeh, K. P-C. (2017). The Effects of Attention Monitoring with EEG Biofeedback on University Students' Attention and Self-Efficacy: The Case of Anti-Phishing Instructional Materials. *Computers and Education, 106,* 73-82.

Sweller, J. (1988). Cognitive Load During Problem Solving: Effects on Learning. *Cognitive Science, 12*(2), 257-285.

Sweller, J., van Merrienboer, J. J. G., & Paas, F. G. W. C. (1998). Cognitive Architecture and Instructional Design. *Educational Psychology Review, 10*(3), 251–296.

Swol, L., & Sniezek, J. (2005). Factors Affecting the Acceptance of Expert Advice. *British Journal of Social Psychology, 44,* 443–461.

Symons, A., Dick, F., & Tierney, A. (2023). Salient Sounds Distort Time Perception and Production. *Psychonomic Bulletin & Review,* 10.3758/s13423-023-02305-2.

Thaler, R. H., & Sunstein, C. R. (2008) *Nudge: Improving Decisions about Health, Wealth, and Happiness.* Yale University Press.

Thompson, K., Sanchez, D., Wesley, A., & Reber, P. (2014). Ego Depletion Impairs Implicit

Learning. *PLoS ONE, 9*(10), e109370.

TitanHQ (2023). *SafeTitan Security Awareness and Phishing Training.* https://www.titanhq.com

Toniolo, A., Cerutti, F., Norman, T. J., Oren, N., Allen, J. A., Srivastava, M., & Sullivan, P. (2023). Himan-Machine Collaboration in Intelligence Analysis: An Expert Evaluation. *Intelligent Systems with Applications, 17,* Article No. 200151.

Trang, S., & Nastjuk, I. (2021). Examining the Role of Stress and Information Security Policy Design in Information Security Compliance Behaviour: An Experimental Study of In-task Behaviour. *Computers & Security, 104,* Article No. 102222.

Turpin, M., Meyers, E., Walker, A., Bialek, M., Stolz, J., & Fugelsang, J. (2020). The Environmental Malleability of Base-Rate Neglect. *Psychonomic Bulletin & Review, 27*, 385-391.

Tversky, A. (1969). Intransitivity of Preferences. *Psychological Review, 76*, 31-48.

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*, 1124–1130.

Valimail (2021). *Email Fraud Landscape Spring 2021.* https://www.valimail.com/blog/email-fraud-spring-2021/

Van Bavel, R. Rodriguez-Priego, N., Vila, J., & Briggs, P. (2019). Using Protection Motivation Theory in the Design of Nudges to Improve Online Security Behaviours. *International Journal of Human Computer Studies, 123,* 29-39.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk Perceptions of Cyber-Security and Precautionary Behaviour. *Computers in Human Behavior, 75*, 547-559.

Van Swol, L., Braun, M., & Acosta Lewis, E. (2015). Discussion of Shared Information can Increase the Influence of Divergent Members. *Communications Research, 45*(2), 1–25.

Vance, A., Anderson, B., Kirwan, C., & Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behaviour: Insights from Electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 679-722.

Vasile, C. (2015). Time Perception, Cognitive Correlates, Age and Emotions. *Procedia-Social and Behavioral Sciences, 187*, 695-699.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, 157- 178.

Verizon. (2022). *2022 Data Breach Investigations Report*. Received from https://www.verizon.com/business/resources/Tab0/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Verschuere, B, Meijer, E, H,, Jim, A., et al. (2018). Registered Replication Report on Mazar, Amir, and Ariely (2008). *Advances in Methods and Practices in Psychological Science, 1*(3), 299-317.

Vilhelmson, B., Thulin, E., & Elldér, E. (2017). Where does Time Spent on the Internet come from? Tracing the Influence of Information and Communications Technology Use on Daily Activities. *Information, Communication & Society, 20*(2), 250-263.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H., R. (2011). Why do People get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems, 51,* 576-586.

Vohs, K., & Faber, R. (2007). Spent resources: Self-regulator Resource Availability Affects

Impulse Buying. *Journal of Consumer Research, 33*, 537–547.

Von Neumann, J., & Morgenstern, O. (1953). *Theory of Games and Economic Behavior*. Princeton, NJ. Princeton University Press.

Walumbwa, F. O., Lawler, J. J., & Avolio, B. J. (2007). Leadership, Individual Differences, and Work-Related Attitudes: A Cross-Culture Investigation. *Applied Psychology, 56*(2), 212-230.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H., R. (2012). Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing email. *IEEE Transactions on Professional Communication, 55*(4), 345-362.

Waugh, N. C., & Norman, D. A. (1965). Primary Memory. *Psychological Review, 72*, 89-104.

Watson, D., Clark, L. A., & Tellagen, A. (1988). Development and Validation of Brief Measures of Positive and Negative Affect: the PANAS Scales. *Journal of Personality and Social Psychology, 54*(6), 1063.

Wearden, J. H., & Ogden, R. S. (2021). Filled-Duration Illusions. *Timing and Time Perception*, *10*(2), 97-121.

Webb, T. L., & Sheeran, P. (2006). Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence. *Psychological Bulletin, 132*(2), 249-268.

Wee, J. M. C., Bashir, M., & Memon, N. (2016). Self-Efficacy in Cybersecurity Tasks and Its Relationship with Cybersecurity Competition and Work-Related Outcomes. In *2016 USENIX Workshop on Advances in Security Education (ASE 16).*

Wehrt, W., Casper, A., & Sonnentag, S. (2022). More than a Muscle: How Self-Control Motivation, Depletion, and Self-Regulation Strategies Impact Task Performance. *Journal of Organizational Behavior, 43*(8), 1358-1376.

Weller, J. A., Levin, I. P., & Denburg, N. L. (2011). Trajectory of Risky Decision Making for Potential Gains and Losses from Ages 5 to 85. *Journal of Behavioral Decision Making, 24*(4), 331-344.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual Differences in Susceptibility to Online Influence: A Theoretical Review. *Computers in Human Behavior, 72*, 412-421.

Williams, E. J., Hinds, J., & Joinson, A., N. (2018). Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies, 120,* 1-13.

Williams, E. J., Morgan, P., L., & Joinson, A. N. (2017). Press Accept to Update Now: Individual Differences in Susceptibility to Malevolent Interruptions. *Decision Support Systems, 96*, 119-129.

Williams, E. J., & Polage, D. (2019). How Persuasive is Phishing Email? The Role of Authentic Design, Influence, and Current Events in Email Judgements. *Behaviour & Information Technology 2019, 38*(2), 184-197.

Williams, E. F., Pizarro, D., Ariely, D., Weinberg, J. D. (2016). The Valjean Effect: Visceral States and Cheating. *Emotion, 16*(6), 897-902.

Wissing, B. G., & Reinhard, M-A. (2019). The Dark Triad and Deception Perceptions. *Frontiers in Psychology: Section of Forensic and Legal Psychology, 10,* 1811.

World Economic Forum. (2022). *The Global Risks Report 2022.* Received from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Wright, R., M, K., & Thatcher, J. (2014). Extending Ecommerce Deception to Phishing. In Myers, M, D., & Straub, D. W. (eds) *Proceedings of the International Conference on Information Systems - Building a Better World through Information Systems*, ICIS 2014, Auckland, New Zealand, December 14-17, 2014. Association for Information Systems 2014, ISBN 978-0-615-15788-7

Wu, H., & Leung, S-O. (2017). Can Likert Scales be Treated as Interval Scales? – A Simulation Study. *Journal of Social Service Research, 43*(4), 527-532.

Wu, S., Peng, M., Mei, H., & Shang, X. (2019). Unwilling but not Unable to Control: Ego Depletion Increases Effortful Dishonesty with Material Rewards. *Scandinavian Journal of Psychology: Cognition and Neurosciences, 60*(3), 189-194.

Yates, J. F., Veinott, E., & Patalano, A. L. (2003). Hard Decisions, Bad Decisions: On Decision Quality and Decision Diding. In S.Schneider, & J. Shanteau (Eds.), *Emerging Perspectives in Judgment and Decision Research* (pp. 13-63). New York: Cambridge University Press.

Zajenkowski, M., Jonason, P. K., Leniarska, M., & Kozakiewicz, Z. (2020). Who Complies with the Restrictions to Reduce the Spread of COVID-19?: Personality and Perceptions of the COVID-19 Situation. *Personality and Individual Differences, 166*, 110119.

Zielinska, O. A., Welk, A. K., Mayhorn, C. B., & Murphy-Hill, E. (2016). A Temporal Analysis of Persuasion Principles in Phishing Emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 60*(1), pp. 765-769. Sage CA: Los Angeles, CA: SAGE Publications.

Zijlstra, F. R., Roe, R. A., Leonora, A. B., & Krediet, I. (1999). Temporal Factors in Mental Work: Effects of Interrupted Activities. *Journal of Occupational and Organizational Psychology, 72*(2), 163-185.

Appendices

Appendix A – *Composite of the NASA-TLX (Hart & Staveland, 1988)*

1. Mental demand: How mentally demanding was the task?

1 Not at all	2 Not very	3 Somewhat	4 Moderately	5 Quite	6 Very	7 Extremely

2. Performance: How successful were you in accomplishing what you were asked to do?

1 Not at all	2 Not very	3 Somewhat	4 Moderately	5 Quite	6 Very	7 Extremely

3. Effort: How hard did you have to work to accomplish your level of performance?

1 Not at all	2 Not very	3 Somewhat	4 Moderately	5 Quite	6 Very	7 Extremely

4. Frustration: How insecure, discouraged, irritated, stressed, and annoyed were you?

1 Not at all	2 Not very	3 Somewhat	4 Moderately	5 Quite	6 Very	7 Extremely

Appendix B – *Studies from the Chapter 2 systematic review which contained data relevant to subjective time pressure and human cyber secure behaviour*

Author/s (year)	**Brief description of study relevance**
Beautement, Sasse, & Wonham (2008)[b]	Semi-structured interviews with staff members from two major UK companies regarding the perceived cost and benefit of time pressures derived from cybersecurity compliance for multiple cyber secure behaviours.
Bona & Paci (2020)[a]	Field experiment investigating the significance of authority and urgency as persuasion techniques in phishing susceptibility in employees.
Chan, Woon, & Kankanhalli (2005)[b]	Ratings for one relevant item within a survey ("I tend to ignore information security procedures in order to complete my work quickly") to examine the relationship between this specific compliant behaviour related to time pressure and employee's perception of the information security climate ratings.
Chowdhury, Adam, & Teubner (2020)[b]	Semi-structured interviews with cybersecurity experts, non-security professionals, and private users examining how non-secure cyber secure behaviours in relation to time pressure can be conceptualised into an integrative framework.
Cui et al. (2020)[a]	Within-subjects experiment to examine the relationship between the presence of recipient information and time urgency cues in emails related to likelihood in reply to/deleting phishing emails.
Fagan et al. (2017)[b]	Ratings for one relevant item within a survey ("I do not have time to pay attention to security") examining differences in perceived subjective time pressure between users and non-users of password managers.
Hu et al. (2015)[b]	Investigated in two laboratory experiments the role of time urgency in the form of impulsivity and the contemplation of decisions in the context of information security policy violations using EEG.
Li et al. (2020)[b]	Used phishing emails containing urgency cues to investigate demographic factors related to phishing susceptibility.
Marett & Wright (2009)[a]	Field experiment investigated the role of phishing email content relating to time urgency and responses to emails.
Nthala & Flechais (2017)[a]	Using semi-structured interviews with home users to explore data security decisions involving time urgency in the home context.
Parsons et al. (2015)[a]	Laboratory experiment examining the presence of various cue, including urgency, in emails to determine which cues were significant in determining phishing susceptibility.
Trang & Nastjuk (2021)[a]	Mixed-subjects experiment examining how time constraints influence perceived time stress, and how perceived time stress related to information security policy compliance.
Vishwanath et al. (2011)[a]	Conducted a survey examining how users' attention to visual urgency triggers and phishing deception indicators influence their decision making.
Wang et al. (2012)[a]	Same dataset from Vishwanath et al (2011) with further developments.
Williams, Hinds, & Joinson (2018)[a]	Retrospectively assessed whether phishing emails containing urgency cues were more likely to have been responded to than without urgency cues.
Williams, Morgan, & Joinson (2017)[b]	Examined the role of influence techniques, including urgency cues, in the susceptibility to risky responses.
Williams & Polage (2019)[b]	Adopted qualitative responses to capture self-reported reasons for responding to emails, including the role of influence techniques such as the need to take an action quickly.
Wright, Marett, and Thatcher (2014)[a]	Same dataset from Marett & Wright (2009) with further developments.

Note. a = Included in review analysis (Appendix C), b = Did not demonstrate clear relationship and was subsequently excluded.

Appendix C – *Studies included in the Chapter 2 systematic review analysis demonstrating a clear relationship between subjective time pressure and cyber secure behaviour.*

Author (year), Country	Subjective time pressure source	Relevant aim/hypothesis/question	Participants	Study design	Main findings	MMAT Score/Dimension not met (if applicable)
Bona & Paci (2020), Italy	Time urgency induced from email content	RQ1: Do authority and urgency principles increase employees' susceptibility to phishing?	191 Employees from an Italian company based in Northern Italy Age: 23.5% 18-29 years, 42.4% 30-39 years, 19.9% 40-49 years, 14.1% 50+ years. Gender: 54% Female Role at work: 63.3% Clerks, 17.2% Workers, 10.5% Managers, 8.9% Interns. Education: 52.9% Degree, 40.3% High School, 6.8% Secondary School. Area of work: 18.3% R&D, 37.7% Marketing, 19.4% Production, 24.6% IT and Logistics. Phase 1: 191 employees Phase 2: 45 employees who fell victim to email attack in phase 1	Between-participants field experiment	More responses to phishing emails were due to urgency cues compared to influence of authority and control conditions.	4
Cui et al. (2020), China	Time urgency induced from email content	To examine the interaction effects of recipient information and urgency cues on phishing detection.	518 participants Age: 18-52 years (mean = 24.69, SD = 4.543) Gender: 54% Female Previous phishing experience: 68.9% Phone, 73.35 Mail, 75.29% Web. 9.46% lost money/private information.	Within-participants online experiment	Participants more likely to reply to phishing email if time urgency cues are present regardless of the presence of sender information.	2 Unclear whether participants recruited in way which minimised selection bias. Did not account for differences in groups.

			13.32% phishing education experience.			
Marett & Wright (2009), USA	Time urgency induced from email content	H1: Content-based deceptive tactics increase the likelihood of successfully deceiving others with a phishing effort. H2: Content-based deceptive tactics are equally effective for successfully deceiving others with a phishing effort.	224 US Undergraduate business students on an introductory management information systems course Mean age = 21.02 years Gender: 52% Male	Between-participants field experiment	Call to immediate response in email resulted in significantly more responses to phishing email.	3 Unrepresentative sample
Nthala & Flechais (2017), UK	Task time constraint impacting time urgency	To elicit data regarding data security decisions made by home users.	15 Home users from Oxford, UK, recruited through snowball sampling Age range = 18-34 Gender: 9 Male	Qualitative semi-structured interviews	Participants considered the significance of the task they are completing and looking for how they spend their time in data security decision making. Physical time constraints altered participants' sense of time urgency.	3 Potential researcher influence via interactions with participants
Parsons et al (2015), Australia	Time urgency induced from email content	To determine which cues in emails participants used which affected performance.	Stage One: Four registered Psychologists and a Doctor of Information Security Stage Two: 59 university students	Within-participants lab experiment	Participants were least likely to correctly manage emails that contained urgency cues.	3 Unrepresentative sample
Trang & Nastjuk (2021), Germany	Task time constraint impacting time urgency	RQ1: How does time pressure in the work environment influence information security policy (ISP) non-compliance behaviour? H1: Time constraint is related positively to perceived stress. H2: Perceived stress is related positively to ISP non-compliance.	229 participants with work experience Mean age: 33.6 years Nationality: German 88.2% Education: Degree 70.3% Work experience average: 9.9 years (SD=10.9); average 5.2 years with current employers (SD=7.4)	Between- and within-participants online experiment	Time constraints were positively related to perceived stress, and perceived stress positively related to ISP non-compliance.	4

Vishwanath et al (2011), USA	Time urgency induced from email content	H1c: The level of attention to urgency cues will be positively related to the likelihood to respond to phishing emails. H2c: The level of attention given to urgency cues will be negatively related to the level of elaboration. H3: Elaboration will be negatively related to the individual's likelihood to respond to phishing emails.	321 US communication and undergraduate students and business majors Mean age = 21 (SD = 3.19) Gender: 54% Female	Quantitative online survey	Participants were more likely to consider responding to the phishing email due to attention to urgency cues.	3 Unrepresentative sample
Williams, Hinds, & Joinson (2018), UK	Time urgency induced from email content	H1: The presence of urgency cues within simulated spear phishing emails will be related to an increased likelihood of responding to these emails.	Study One: Approximately 62,000 employees from a large UK public sector organisation	Retrospective observational study	The presence of urgency cues was related to an increase in likelihood in responding to phishing emails.	3 No details provided for key demographic information
Wright, Marett, & Thatcher (2014), USA	Time urgency induced from email content	H1c: A phishing message that contains veridicality manipulations will have a greater chance of success than a message without this manipulation.	224 US Undergraduate business students on an introductory management information systems course Mean age = 21.02 years Gender: 52% Male	Between-participants field experiment	Call to immediate response in email resulted in significantly more responses to phishing email.	3 Unrepresentative sample
Wang et al. (2012), USA	Time urgency induced from email content	H1: Attention to visceral triggers reduces overall cognitive effort in processing a targeted phishing email. H2: Attention to visceral triggers increases the likelihood of response to a targeted phishing email. H9: Knowledge of email-based scams weakens the effect of attention to visceral triggers on the likelihood to respond to a targeted phishing email.	321* US Communication undergraduate students and business majors Mean age = 21 years (SD = 3.19) Gender: 54% Female	Quantitative online survey	Participants were more likely to consider responding to the phishing email due to attention to urgency cues.	3 Unrepresentative sample

Note. * = After removing responses with severe missing data only 267 of these responses were used in the final analysis.

Appendix D – *Table of standard deviations for time estimation trials from the behavioural time perception measure in study 6 and study 7 (session one and two).*

Time Trial	Study 6	Study 7 Session One	Study 7 Session Two
1	10.855308801	15.8139325	13.2865492
2	11.872004684	17.3325306	13.9334259
3	11.714059304	16.6059327	16.4292900
4	11.922484826	16.1182330	12.8679688
5	11.889601547	14.1750831	15.2045853
6	N/A	16.4610763	13.7462224
7	N/A	17.2171298	13.9642542
8	N/A	15.7483322	14.3340336
9	N/A	16.7244117	13.5344258
10	N/A	17.4429764	13.5837179

Appendix E – *List of Expected Utility Outcome items for each email context created for Study 10 along with their associated context descriptions.*

Email type - Conference Invitation

These emails consist of an invitation to a conference. Conferences in this context are formal meetings which would consist of a large gathering of individuals from specialist backgrounds from industry or academia which encourage discussions on new innovations, as well as provide the opportunity to network with likeminded others.

- How much would you value the **positive consequences of replying** to a **genuine email** invitation to attend a conference? (0=Do not value, 100 = Completely value)
- How much would you value the **positive consequences of replying** to a **phishing email** detailing an invitation to attend a conference? (0=Do not value, 100 = Completely value)
- How much would you value the **negative consequences of replying** to a **genuine email** invitation to attend a conference? (0=Do not value, 100 = Completely value)
- How much would you value the **negative consequences of replying** to a **phishing email** detailing an invitation to attend a conference? (0=Do not value, 100 = Completely value)
- How much would you value the **positive consequences of not replying** to a **genuine email** invitation to attend a conference? (0=Do not value, 100 = Completely value)
- How much would you value the **positive consequences of not replying** to a **phishing email** detailing an invitation to attend a conference? (0=Do not value, 100 = Completely value)
- How much would you value the **negative consequences of not replying** to a **genuine email** invitation to attend a conference? (0=Do not value, 100 = Completely value)

- How much would you value the **__negative__ consequences of __not replying__** to a **__phishing email__** detailing an invitation to attend a conference? (0=Do not value, 100 = Completely value)

__Email type - Invoice__

These types of email would involve a request to confirm or review a purchase order on behalf of you or a company purchase.

- How much would you value the **__positive__ consequences of __replying__** to a **__genuine email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)
- How much would you value the **__positive__ consequences of __replying__** to a **__phishing email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)
- How much would you value the **__negative__ consequences of __replying__** to a **__genuine email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)
- How much would you value the **__negative__ consequences of __replying__** to a **__phishing email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)
- How much would you value the **__positive__ consequences of __not replying__** to a **__genuine email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)
- How much would you value the **__positive__ consequences of __not replying__** to a **__phishing email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)
- How much would you value the **__negative__ consequences of __not replying__** to a **__genuine email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)
- How much would you value the **__negative__ consequences of __not replying__** to a **__phishing email__** asking for approval of an invoice? (0= Do not value, 100 = Completely value)

Email type - Personal finance

These types of email consist of a notification that you may be at risk of losing leave days or incur loss of payment due to errors, and would detail what you need to do to avoid losing out on these personal finance issues.

- How much would you value the **positive consequences of replying** to a **genuine email** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

- How much would you value the **positive consequences of replying** to a **phishing email** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

- How much would you value the **negative consequences of replying** to a **genuine email** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

- How much would you value the **negative consequences of replying** to a **phishing email** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

- How much would you value the **positive consequences of not replying** to a **genuine email** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

- How much would you value the **positive consequences of not replying** to a **phishing email** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

- How much would you value the **negative consequences of not replying** to a **genuine email** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

- How much would you value the **<u>negative</u> consequences of <u>not replying</u>** to a **<u>phishing email</u>** notifying you on how to avoid personal finance loss? (0= Do not value, 100 = Completely value)

<u>Email type - Survey</u>

These types of email will consist of a request for you to complete a survey which may consist of providing personal information or feedback.

- How much would you value the **<u>positive</u> consequences of <u>replying</u>** to a **<u>genuine email</u>** asking for you to complete a survey? (0= Do not value, 100 = Completely value)
- How much would you value the **<u>positive</u> consequences of <u>replying</u>** to a **<u>phishing email</u>** asking for you to complete a survey? (0= Do not value, 100 = Completely value)
- How much would you value the **<u>negative</u> consequences of <u>replying</u>** to a **<u>genuine email</u>** asking for you to complete a survey? (0=Do not value, 100 = Completely value)
- How much would you value the **<u>negative</u> consequences of <u>replying</u>** to a **<u>phishing email</u>** asking for you to complete a survey? (0=Do not value, 100 = Completely value)
- How much would you value the **<u>positive</u> consequences of <u>not replying</u>** to a **<u>genuine email</u>** asking for you to complete a survey? (0= Do not value, 100 = Completely value)
- How much would you value the **<u>positive</u> consequences of <u>not replying</u>** to a **<u>phishing email</u>** asking for you to complete a survey? (0= Do not value, 100 = Completely value)
- How much would you value the **<u>negative</u> consequences of <u>not replying</u>** to a **<u>genuine email</u>** asking for you to complete a survey? (0= Do not value, 100 = Completely value)
- How much would you value the **<u>negative</u> consequences of <u>not replying</u>** to a **<u>phishing email</u>** asking for you to complete a survey? (0= Do not value, 100 = Completely value)

Email type - Loss of Access

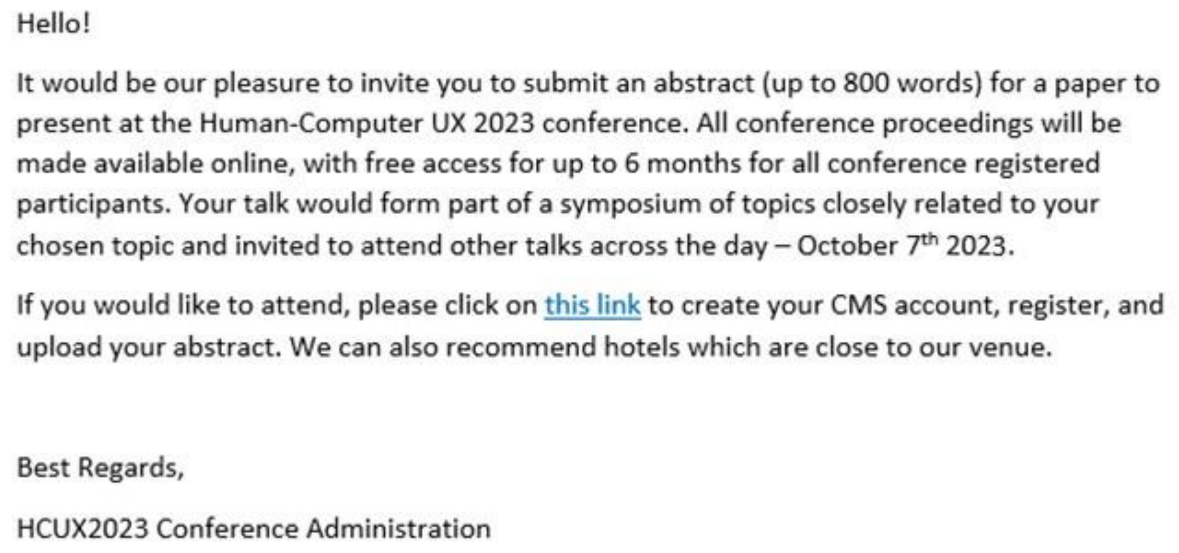
These types of email consist of a notification that you are at risk of losing access to work-related computer accounts, emails, and/or shared folders; and require you to take an action to avoid this loss of access.

- How much would you value the **positive consequences of replying** to a **genuine email** notifying you on how to avoid losing access to work-related accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)
- How much would you value the **positive consequences of replying** to a **phishing email** notifying you on how to avoid losing access to work-related accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)
- How much would you value the **negative consequences of replying** to a **genuine email** notifying you on how to avoid losing access to work-related online accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)
- How much would you value the **negative consequences of replying** to a **phishing email** notifying you on how to avoid losing access to work-related online accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)
- How much would you value the **positive consequences of not replying** to a **genuine email** notifying you on how to avoid losing access to work-related online accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)
- How much would you value the **positive consequences of not replying** to a **phishing email** notifying you on how to avoid losing access to work-related online accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)
- How much would you value the **negative consequences of not replying** to a **genuine email** notifying you on how to avoid losing access to work-related online accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)

- How much would you value the **<u>negative</u> consequences of <u>not replying</u>** to a **<u>phishing email</u>** notifying you on how to avoid losing access to work-related online accounts (e.g., emails, shared folders)? (0=Do not value, 100 = Completely value)

Appendix F – *Examples of stimuli used in Studies 8, 9 and 10 with labels for email context and persuasion cues included.*

Conference email passively written (no persuasion technique adopted):



Hello!

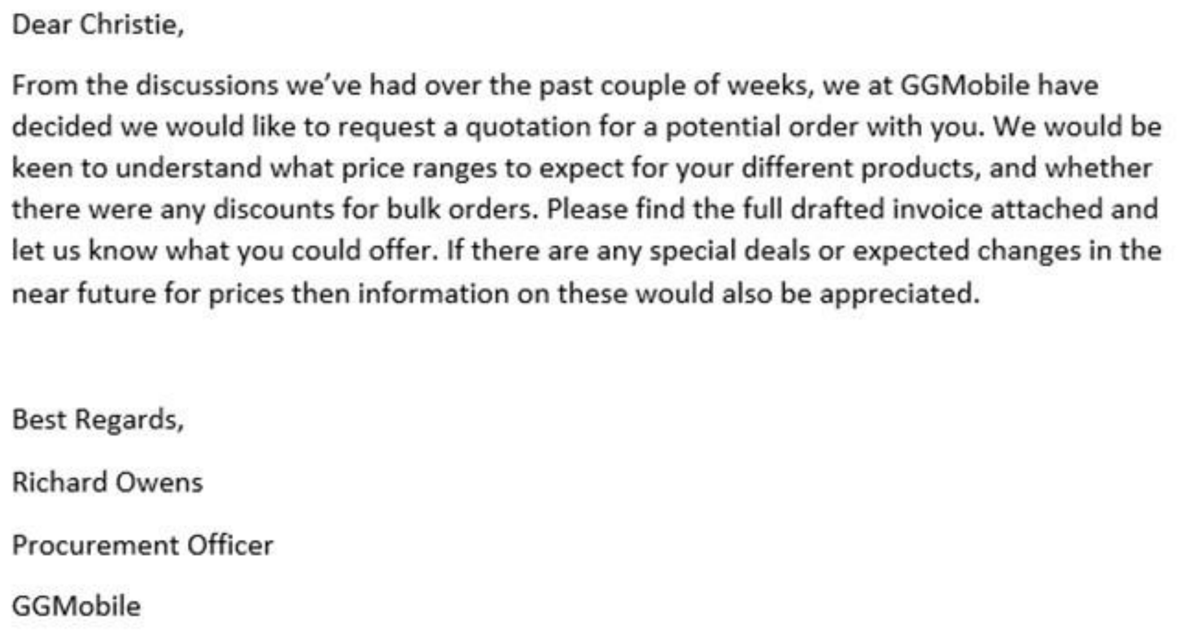
It would be our pleasure to invite you to submit an abstract (up to 800 words) for a paper to present at the Human-Computer UX 2023 conference. All conference proceedings will be made available online, with free access for up to 6 months for all conference registered participants. Your talk would form part of a symposium of topics closely related to your chosen topic and invited to attend other talks across the day – October 7th 2023.

If you would like to attend, please click on this link to create your CMS account, register, and upload your abstract. We can also recommend hotels which are close to our venue.

Best Regards,

HCUX2023 Conference Administration

Invoice email passively written (no persuasion technique adopted):



Dear Christie,

From the discussions we've had over the past couple of weeks, we at GGMobile have decided we would like to request a quotation for a potential order with you. We would be keen to understand what price ranges to expect for your different products, and whether there were any discounts for bulk orders. Please find the full drafted invoice attached and let us know what you could offer. If there are any special deals or expected changes in the near future for prices then information on these would also be appreciated.

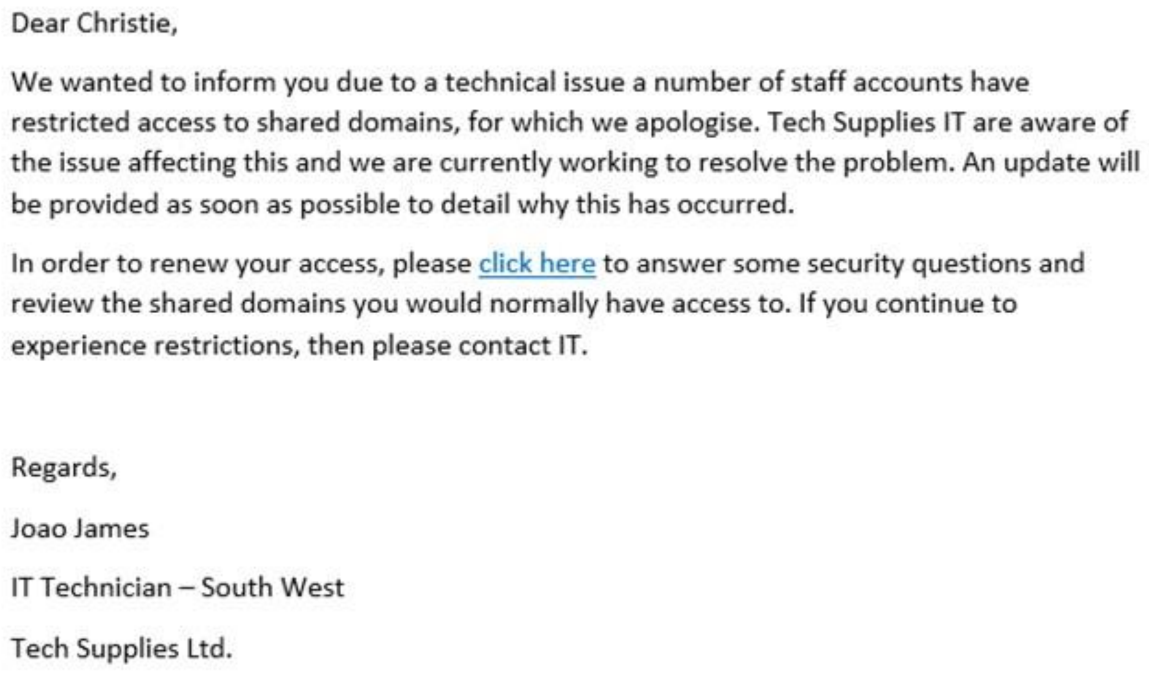
Best Regards,

Richard Owens

Procurement Officer

GGMobile

Loss of Access email passively written (no persuasion technique adopted):



Dear Christie,

We wanted to inform you due to a technical issue a number of staff accounts have restricted access to shared domains, for which we apologise. Tech Supplies IT are aware of the issue affecting this and we are currently working to resolve the problem. An update will be provided as soon as possible to detail why this has occurred.

In order to renew your access, please click here to answer some security questions and review the shared domains you would normally have access to. If you continue to experience restrictions, then please contact IT.

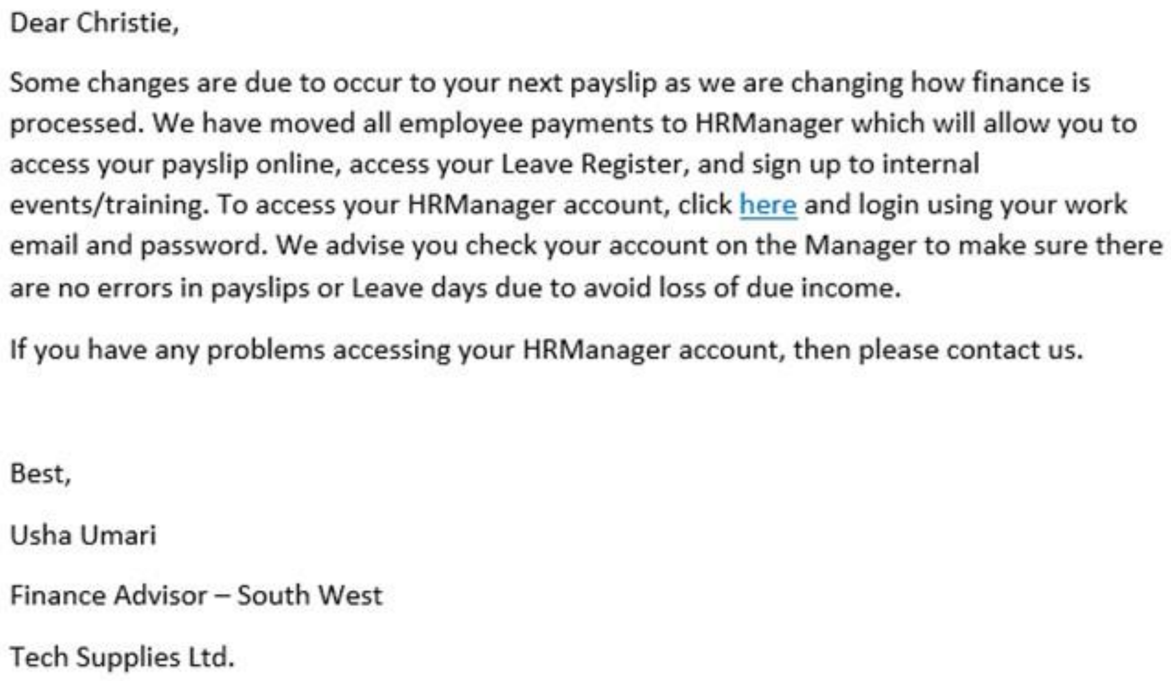
Regards,

Joao James

IT Technician – South West

Tech Supplies Ltd.

Personal Finance email passively written (no persuasion technique adopted):



Dear Christie,

Some changes are due to occur to your next payslip as we are changing how finance is processed. We have moved all employee payments to HRManager which will allow you to access your payslip online, access your Leave Register, and sign up to internal events/training. To access your HRManager account, click here and login using your work email and password. We advise you check your account on the Manager to make sure there are no errors in payslips or Leave days due to avoid loss of due income.

If you have any problems accessing your HRManager account, then please contact us.

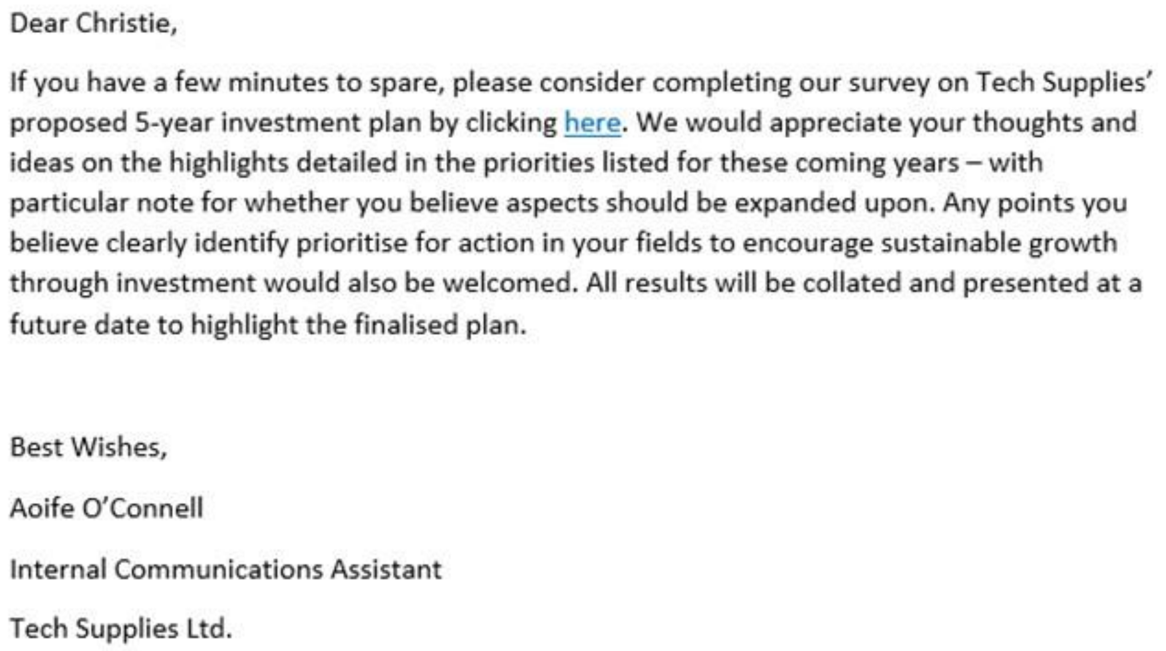
Best,

Usha Umari

Finance Advisor – South West

Tech Supplies Ltd.

Survey email passively written (no persuasion technique adopted):



Dear Christie,

If you have a few minutes to spare, please consider completing our survey on Tech Supplies' proposed 5-year investment plan by clicking here. We would appreciate your thoughts and ideas on the highlights detailed in the priorities listed for these coming years – with particular note for whether you believe aspects should be expanded upon. Any points you believe clearly identify prioritise for action in your fields to encourage sustainable growth through investment would also be welcomed. All results will be collated and presented at a future date to highlight the finalised plan.

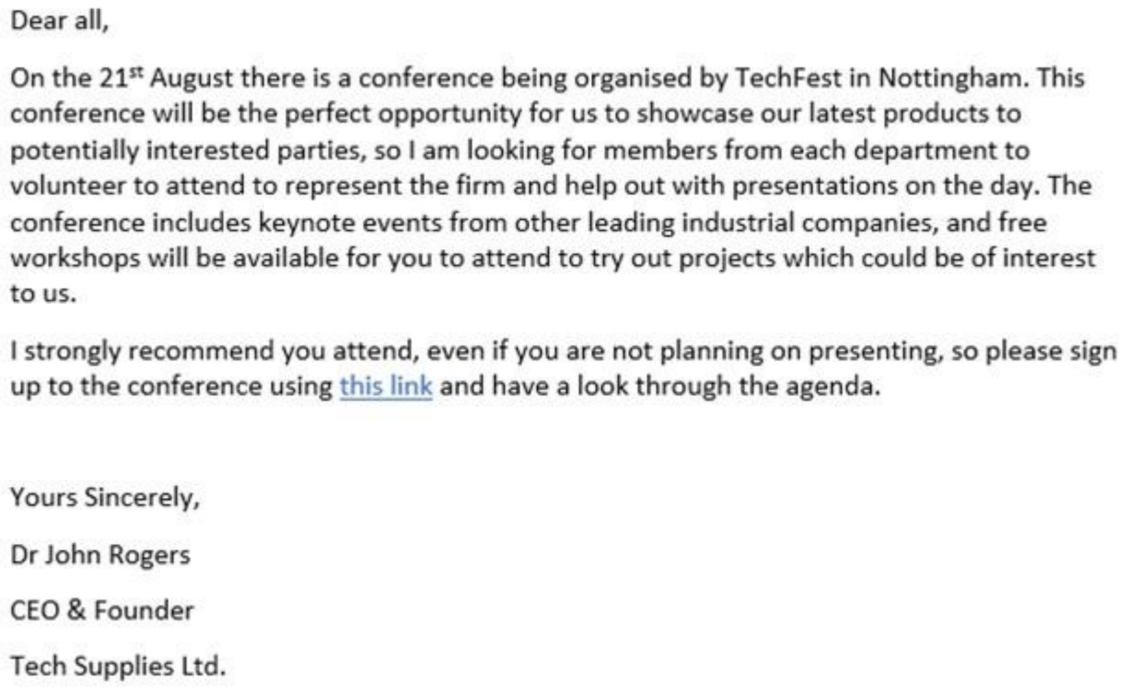
Best Wishes,

Aoife O'Connell

Internal Communications Assistant

Tech Supplies Ltd.

Conference email containing authority cues:



Dear all,

On the 21st August there is a conference being organised by TechFest in Nottingham. This conference will be the perfect opportunity for us to showcase our latest products to potentially interested parties, so I am looking for members from each department to volunteer to attend to represent the firm and help out with presentations on the day. The conference includes keynote events from other leading industrial companies, and free workshops will be available for you to attend to try out projects which could be of interest to us.

I strongly recommend you attend, even if you are not planning on presenting, so please sign up to the conference using this link and have a look through the agenda.

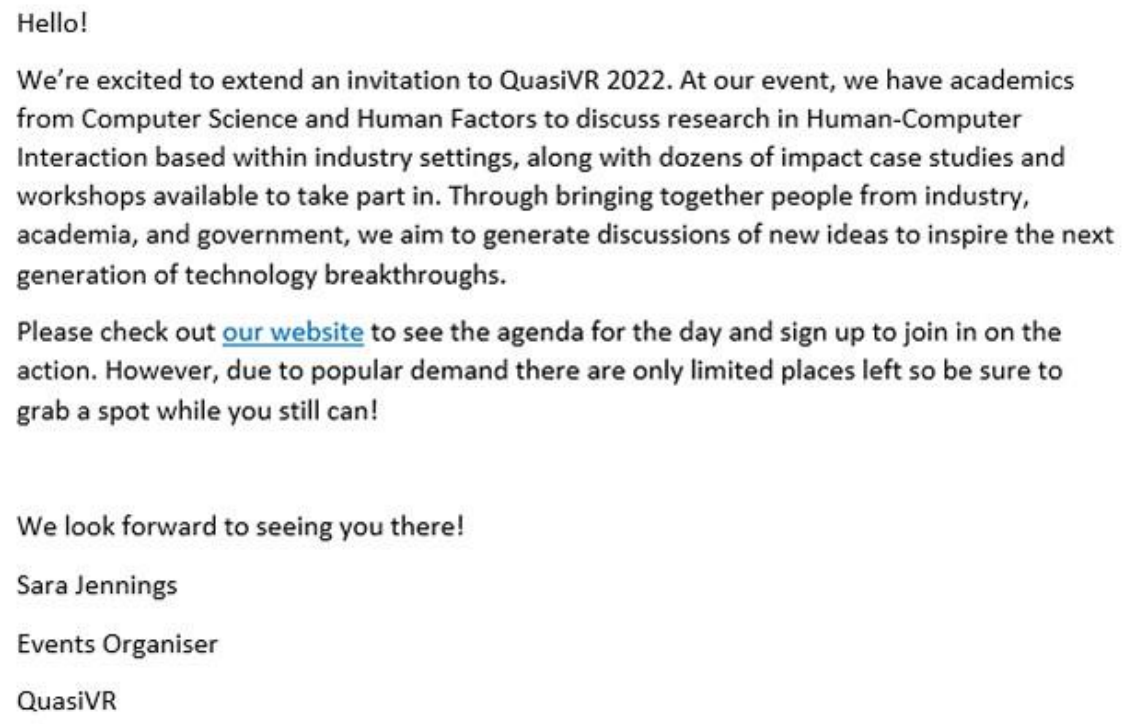
Yours Sincerely,

Dr John Rogers

CEO & Founder

Tech Supplies Ltd.

Conference email containing scarcity of quantity cues:



Hello!

We’re excited to extend an invitation to QuasiVR 2022. At our event, we have academics from Computer Science and Human Factors to discuss research in Human-Computer Interaction based within industry settings, along with dozens of impact case studies and workshops available to take part in. Through bringing together people from industry, academia, and government, we aim to generate discussions of new ideas to inspire the next generation of technology breakthroughs.

Please check out our website to see the agenda for the day and sign up to join in on the action. However, due to popular demand there are only limited places left so be sure to grab a spot while you still can!

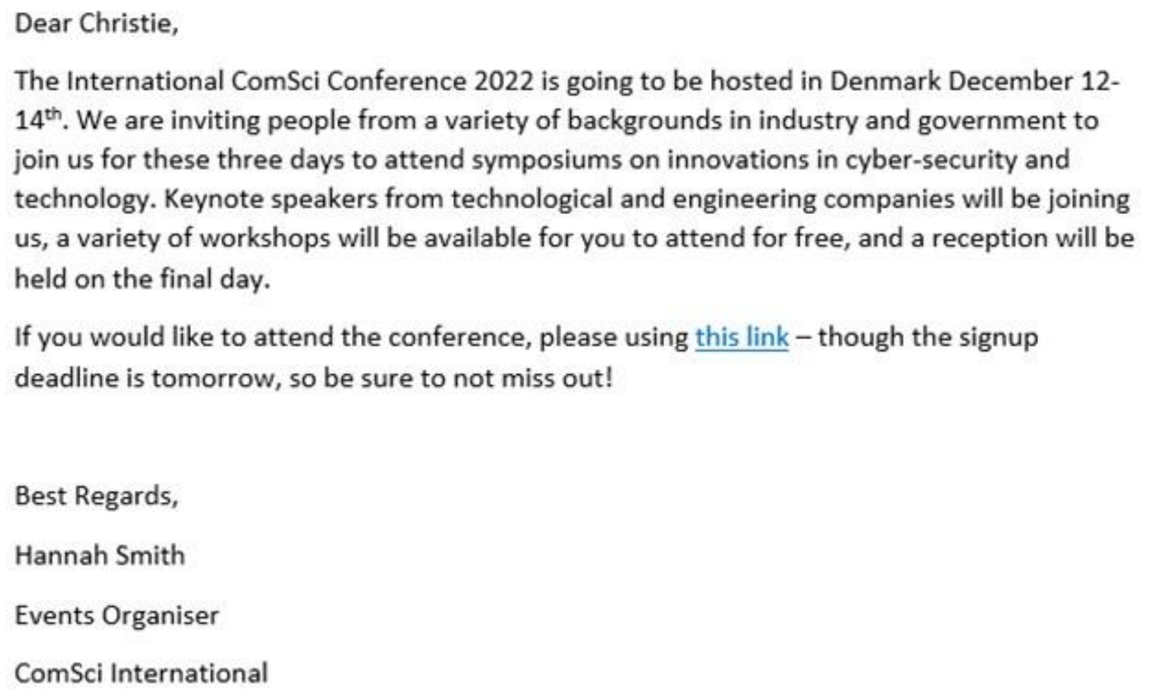
We look forward to seeing you there!

Sara Jennings

Events Organiser

QuasiVR

Conference email containing time urgency cues:



Dear Christie,

The International ComSci Conference 2022 is going to be hosted in Denmark December 12-14th. We are inviting people from a variety of backgrounds in industry and government to join us for these three days to attend symposiums on innovations in cyber-security and technology. Keynote speakers from technological and engineering companies will be joining us, a variety of workshops will be available for you to attend for free, and a reception will be held on the final day.

If you would like to attend the conference, please using this link – though the signup deadline is tomorrow, so be sure to not miss out!

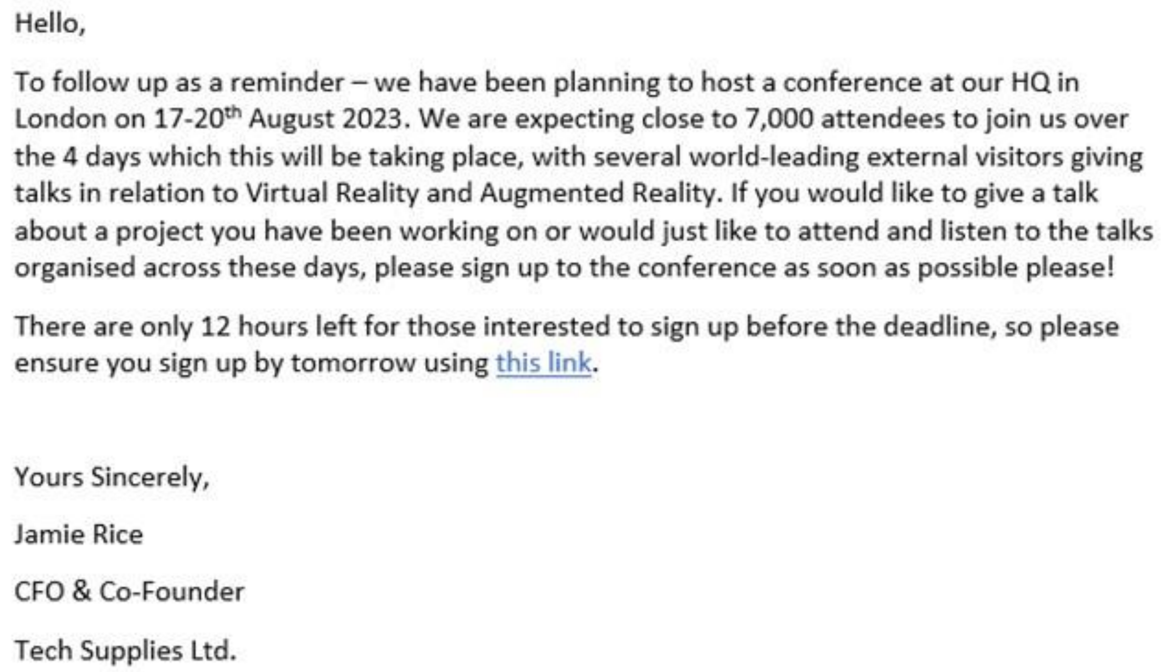
Best Regards,

Hannah Smith

Events Organiser

ComSci International

Conference email containing authority and time urgency cues:



Hello,

To follow up as a reminder – we have been planning to host a conference at our HQ in London on 17-20th August 2023. We are expecting close to 7,000 attendees to join us over the 4 days which this will be taking place, with several world-leading external visitors giving talks in relation to Virtual Reality and Augmented Reality. If you would like to give a talk about a project you have been working on or would just like to attend and listen to the talks organised across these days, please sign up to the conference as soon as possible please!

There are only 12 hours left for those interested to sign up before the deadline, so please ensure you sign up by tomorrow using this link.

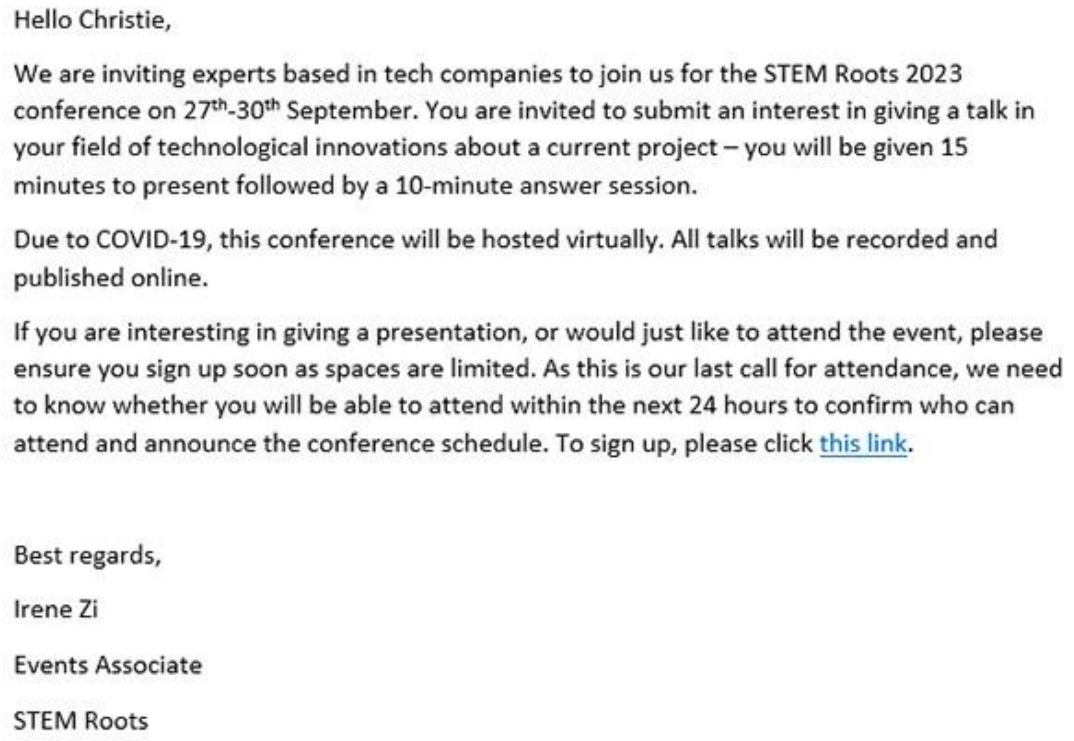
Yours Sincerely,

Jamie Rice

CFO & Co-Founder

Tech Supplies Ltd.

Conference email containing scarcity of quantity and time urgency cues:



Hello Christie,

We are inviting experts based in tech companies to join us for the STEM Roots 2023 conference on 27th-30th September. You are invited to submit an interest in giving a talk in your field of technological innovations about a current project – you will be given 15 minutes to present followed by a 10-minute answer session.

Due to COVID-19, this conference will be hosted virtually. All talks will be recorded and published online.

If you are interesting in giving a presentation, or would just like to attend the event, please ensure you sign up soon as spaces are limited. As this is our last call for attendance, we need to know whether you will be able to attend within the next 24 hours to confirm who can attend and announce the conference schedule. To sign up, please click this link.

Best regards,

Irene Zi

Events Associate

STEM Roots

Appendix G – Pairwise comparisons with accompanying visualisations for probability judgements between conditions in Study 9.

Probability Judgements: Differences between Persuasion Techniques

Conference emails – the email with no persuasion cues was deemed to be significantly more likely to be phishing than genuine compared to the authority cues (z = -11.489, *sig.*), scarcity cues (z = -7.350, *sig.*), time urgency cues (z = -5.546, *sig.*), authority combined with time urgency cues (z = -8.406, *sig.*) and scarcity combined with time urgency cues (z = -7.068, *sig.*). The authority cue email was believed to be significantly more genuine than those with scarcity (z = -8.267, *sig.*), time urgency (z = -9.348, *sig.*), authority with time urgency (z = -6.438, *sig.*), and scarcity with time urgency cues (z = -7.545, *sig.*). Time urgency cues were significantly less likely to be deemed as genuine compared to authority and time urgency combined (z = -3.989, *sig.*), and marginally less likely to be deemed genuine compared to scarcity and time urgency combined – though not significantly due to the Bonferroni correction (z = -3.084, *p* = 0.002042).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **conference emails containing different persuasion techniques** in Study 9. Read the persuasion technique from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The conference email containing no persuasion technique cues was deemed less likely to be genuine compared to the conference time urgency email / the time urgency email was deemed more likely to be genuine compared to the conference email with no persuasion cues.

	None	Time Urgency	Authority	Scarcity	Authority + Time Urgency	Scarcity + Time Urgency
None	▒	🟧	🟧	🟧	🟧	🟧
Time Urgency	🟩	▒	🟧	⬜	🟧	🟧●
Authority	🟩	🟩	▒	🟩	🟩	🟩
Scarcity	🟩	⬜	🟧	▒	⬜	⬜
Authority + Time Urgency	🟩	🟩	🟧	⬜	▒	⬜
Scarcity + Time Urgency	🟩	🟩●	🟧	⬜	⬜	▒

Note. Green = For the persuasion technique in the row title on average people believed the email was ***more likely to be genuine*** *compared to the persuasion technique in the column title. Orange = For the persuasion technique in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the persuasion technique in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Invoice emails – the email with no persuasion cues was deemed to be significantly more likely to be genuine than phishing compared to the scarcity cues (z = -4.987, *sig.*), and significantly less likely to be genuine then phishing compared with time urgency cues (z = -2.443, *p* = .015, *sig.*). Scarcity was less likely to be deemed as genuine compared to time urgency (z = -7.108, *sig.*), authority with time urgency (z = -5.663, *sig.*), and scarcity with time urgency (z = -4.018, *sig.*). Time urgency was deemed to be significantly more likely to be genuine compared to scarcity with time urgency (z = -4.018, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **invoice emails containing different persuasion techniques** in Study 9. Read the persuasion technique from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The invoice email containing no persuasion technique cues was deemed less likely to be genuine compared to the invoice time urgency email / the time urgency email was deemed more likely to be genuine compared to the invoice email with no persuasion cues.

	None	Time Urgency	Authority	Scarcity	Authority + Time Urgency	Scarcity + Time Urgency
None	▨	🟧		🟩		
Time Urgency	🟩	▨		🟩		🟩
Authority			▨			
Scarcity	🟧	🟧		▨	🟧	🟧
Authority + Time Urgency				🟩	▨	
Scarcity + Time Urgency		🟧		🟩		▨

Note. *Green = For the persuasion technique in the row title on average people believed the email was* ***more likely to be genuine*** *compared to the persuasion technique in the column title. Orange = For the persuasion technique in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the persuasion technique in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Loss of access emails – No persuasion cue emails were marginally deemed to be more likely to be phishing than genuine compared to authority and time urgency (z = -2.481, *p* = .013). Scarcity cues alone were marginally deemed to be more likely to be phishing than genuine compared to scarcity combined with time urgency (z = -2.542, *p* = .011), and combined scarcity and time urgency cues more likely to be phishing than genuine compared to authority and time urgency cues combined (z = -3.173, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **loss of access emails containing different persuasion techniques** in Study 9. Read the persuasion technique from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The loss of access email containing no persuasion technique cues showed no significant differences in phishing likelihood perception compared to the loss of access time urgency email.

	None	Time Urgency	Authority	Scarcity	Authority + Time Urgency	Scarcity + Time Urgency
None	▨				🟧 ●	
Time Urgency		▨				
Authority			▨			
Scarcity				▨		🟧 ●
Authority + Time Urgency	🟩 ●				▨	🟩
Scarcity + Time Urgency				🟩 ●	🟧	▨

Note. Green = For the persuasion technique in the row title on average people believed the email was ***more likely to be genuine*** *compared to the persuasion technique in the column title. Orange = For the persuasion technique in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the persuasion technique in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Personal finance emails – The no persuasion technique cues email was marginally less likely to be deemed as genuine compared to authority (z = -2.281, p = .023), significantly less likely to be deemed as genuine compared to scarcity (z = -7.454, *sig.*), time urgency (z = -5.897, *sig.*), and authority combined with time urgency (z = -6.062, *sig.*). Authority was significantly less likely to be deemed as genuine compared to scarcity (z = -4.920, *sig.*), time urgency (z = -5.016, *sig.*), and authority combined with time urgency (z = -3.311, *sig.*). Scarcity was deemed to be significantly more likely to be genuine compared to scarcity with time urgency (z = -7.537, *sig.*). Time urgency was deemed to be significantly more likely to be genuine compared to scarcity with time urgency (z = -5.980, *sig.*). Authority with time urgency was significantly more likely to be deemed as genuine compared to scarcity with time urgency (z = -6.028, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **personal finance emails containing different persuasion techniques** in Study 9. Read the persuasion technique from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The personal finance email containing no persuasion technique cues was deemed less likely to be genuine compared to the personal finance time urgency email / the time urgency email was deemed more likely to be genuine compared to the personal finance email with no persuasion cues.

	None	Time Urgency	Authority	Scarcity	Authority + Time Urgency	Scarcity + Time Urgency
None	⬛	🟧	🟧 ●	🟧	🟧	⬜
Time Urgency	🟩	⬛	🟩	⬜	⬜	🟩
Authority	🟩 ●	🟧	⬛	🟧	🟧	⬜
Scarcity	🟩	⬜	🟩	⬛	⬜	🟩
Authority + Time Urgency	🟩	⬜	🟩	⬜	⬛	🟩
Scarcity + Time Urgency	⬜	🟧	⬜	🟧	🟧	⬛

Note. Green = For the persuasion technique in the row title on average people believed the email was ***more likely to be genuine*** *compared to the persuasion technique in the column title. Orange = For the persuasion technique in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the persuasion technique in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Survey emails – The email with no persuasion technique was significantly less likely to be deemed as genuine compared to authority (z = -4.964, *sig.*), significantly more likely than scarcity (z = -8.761, *sig.*), significantly less likely than time urgency (z = -7.267, *sig.*), significantly more likely to be deemed as genuine than authority with time urgency (z = -3.357, *sig.*), and significantly more likely than scarcity with time urgency (z = -11.003, *sig.*). Authority was significantly more likely to be deemed as genuine compared to scarcity (z = -11.481, *sig.*), time urgency (z = -10.196, *sig.*), authority with time urgency (z = -6.886, *sig.*), and scarcity with time urgency (z = -12.712, *sig.*). Scarcity was significantly more likely to be deemed to be phishing then genuine compared to authority with time urgency (z = -5.334, *sig.*), but significantly less likely to be deemed to be phishing than scarcity with time urgency (z = -4.420, *sig.*). Time urgency was significantly less likely to be deemed as phishing compared to scarcity with time urgency (z = -6.221, *sig.*). Authority with time urgency was significantly more likely to be deemed as genuine compared to scarcity with time urgency (z = -8.594, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **survey emails containing different persuasion techniques** in Study 9. Read the persuasion technique from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The survey email containing no persuasion technique cues was deemed less likely to be genuine compared to the survey time urgency email / the time urgency email was deemed more likely to be genuine compared to the survey email with no persuasion cues.

	None	Time Urgency	Authority	Scarcity	Authority + Time Urgency	Scarcity + Time Urgency
None	▨	🟧	🟧	🟩	🟩	🟩
Time Urgency	🟩	▨	🟧			🟩
Authority	🟩	🟩	▨	🟩	🟩	🟩
Scarcity	🟧		🟧	▨	🟧	🟩
Authority + Time Urgency	🟧		🟧	🟩	▨	🟩
Scarcity + Time Urgency	🟧	🟧	🟧	🟧	🟧	▨

Note. *Green = For the persuasion technique in the row title on average people believed the email was* ***more likely to be genuine*** *compared to the persuasion technique in the column title. Orange = For the persuasion technique in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the persuasion technique in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Probability Judgements: Differences between Email Contexts

Emails containing no persuasion cues – The conference email was significantly less likely to be deemed as genuine compared to the invoice (z = -9.976, *sig.*), personal finance (z = -4.214, *sig.*), and survey emails (z = -8.084, *sig.*). The invoice email was significantly more likely to be deemed as genuine compared to the loss of access (z = -9.524, *sig.*), personal finance (z = -6.607, *sig.*), and survey emails (z = -4.219, *sig.*). The loss of access email was significantly less likely to be deemed as genuine compared to the personal finance (z = -5.138, *sig.*) and survey emails (z = -7.167, *sig.*). The personal finance email was marginally less likely to be deemed as genuine compared to the survey email (z = -2.890, *p* = 0.003857).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **emails containing no persuasion technique cues across different email contexts** in Study 9. Read the email context type from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The conference email containing no persuasion technique cues was deemed less likely to be genuine compared to the invoice email containing no persuasion technique cues / the invoice email containing no persuasion technique cues was deemed more likely to be genuine compared to the conference email with no persuasion cues.

	Conference	Invoice	Loss of Access	Personal Finance	Survey
Conference	▨	🟧		🟧	🟧
Invoice	🟩	▨	🟩	🟩	🟩
Loss of Access		🟧	▨	🟧	🟧
Personal Finance	🟩	🟧	🟩	▨	🟧 ●
Survey	🟩	🟧	🟩	🟩 ●	▨

Note. Green = For the email context in the row title on average people believed the email was ***more likely to be genuine*** *compared to the email context in the column title. Orange = For the email context in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the email context in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Emails containing authority cues – The conference email was significantly more likely to be deemed genuine than the loss of access (z = -9.898, *sig.*) and personal finance emails (z = -5.352, *sig.*). The invoice email was significantly more likely to be deemed as genuine compared to the loss of access (z = -10.480, *sig.*) and personal finance emails (z = -5.750, *sig.*), and marginally more than the survey email (z = -2.622, *p* = 0.008732). Loss of access was significantly less likely to be deemed as genuine compared to the personal finance (z = -5.141, *sig.*) and survey emails (z = -9.305, *sig.*). Personal finance was significantly less likely to be deemed as genuine compared to the survey email (z = -4.464, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **emails containing authority cues across different email contexts** in Study 9. Read the email context type from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The conference email containing authority cues showed no significant differences in phishing likelihood perception compared to the invoice email with authority cues.

	Conference	Invoice	Loss of Access	Personal Finance	Survey
Conference	▨		🟩	🟩	
Invoice		▨	🟩	🟩	🟩 ●
Loss of Access	🟧	🟧	▨	🟧	🟧
Personal Finance	🟧	🟧	🟩	▨	🟧
Survey		🟧 ●	🟩	🟩	▨

Note. *Green = For the email context in the row title on average people believed the email was* ***more likely to be genuine*** *compared to the email context in the column title. Orange = For the email context in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the email context in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Emails containing scarcity cues – The conference email was marginally less likely to be deemed as genuine compared to the invoice email (z = -2.993, *p* = 0.002765), marginally more likely to be deemed as genuine compared to the loss of access email (z = -3.073, *p* = 0.002118), significantly less likely than the personal finance email (z = -6.428, *sig.*), and significantly more likely than the survey email (z = -6.545, *sig.*). The invoice email was significantly more likely to be deemed as genuine compared to the loss of access email (z = -5.834, *sig.*), significantly less than the personal finance email (z = -4.528, *sig.*), and significantly more than the survey email (z = -8.013, *sig.*). The loss of access email was significantly less likely to be deemed as genuine compared to the personal finance email (z = -9.712, *sig.*). The personal finance email was significantly more likely to be deemed as genuine compared to the survey email (z = -10.002, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **emails containing scarcity cues across different email contexts** in Study 9. Read the email context type from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The conference email containing scarcity technique cues was deemed marginally less likely to be genuine compared to the invoice email containing scarcity technique cues / the invoice email containing scarcity technique cues was deemed marginally more likely to be genuine compared to the conference email with scarcity cues.

	Conference	Invoice	Loss of Access	Personal Finance	Survey
Conference	▒	🟧 ●	🟧 ●	🟧	🟩
Invoice	🟩 ●	▒	🟩	🟧	🟩
Loss of Access	🟩 ●	🟧	▒	🟧	
Personal Finance	🟩	🟩	🟩	▒	🟩
Survey	🟧	🟧		🟧	▒

Note. *Green = For the email context in the row title on average people believed the email was* ***more likely to be genuine*** *compared to the email context in the column title. Orange = For the email context in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the email context in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Emails containing time urgency cues – The conference email was significantly less likely to be deemed as genuine compared to the invoice email (z = -9.468, *sig.*), significantly more likely than the loss of access email (z = -4.627, *sig.*), significantly less likely than the personal finance email (z = -5.684, *sig.*), and significantly more likely than the survey email (z = -3.729, *sig.*). The invoice email was significantly more likely to be deemed genuine compared to the loss of access (z = -12.033, *sig.*), personal finance (z = -3.826, *sig.*), and survey emails (z = -11.872, *sig.*). The loss of access email was significantly less likely to be deemed as genuine compared to the personal finance email (z = -9.193, *sig.*). The personal finance email was significantly more likely to be deemed as genuine compared to the survey email (z = -7.797, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **emails containing time urgency cues across different email contexts** in Study 9. Read the email context type from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The conference email containing time urgency cues was deemed less likely to be genuine compared to the invoice email containing time urgency technique cues / the invoice email containing time urgency cues was deemed more likely to be genuine compared to the conference email with time urgency cues.

	Conference	Invoice	Loss of Access	Personal Finance	Survey
Conference	▨	🟧	🟩	🟧	🟩
Invoice	🟩	▨	🟩	🟩	🟩
Loss of Access	🟧	🟧	▨	🟧	⬜
Personal Finance	🟩	🟧	🟩	▨	🟩
Survey	🟧	🟧	⬜	🟧	▨

Note. *Green = For the email context in the row title on average people believed the email was* ***more likely to be genuine*** *compared to the email context in the column title. Orange = For the email context in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the email context in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Emails containing authority and time urgency cues – The conference email was significantly less likely to be deemed to be genuine compared to the invoice email (z = -5.166, *sig.*), more likely compared to the loss of access email (z = -6.153, *sig.*), marginally less like than the personal finance email (z = -2.264, *p* = 0.023545), and marginally more likely compared to the survey (z = -3.115, *p* = 0.001837). The invoice email was significantly more likely to be deemed as genuine compared to the loss of access email (z = -9.284, *sig.*), marginally more likely compared to the personal finance email (z = -3.028, *p* = 0.002464), and significantly more likely than the survey email (z = -7.787, *sig.*). Loss of access was significantly less likely to be deemed as genuine compared to the personal finance email (z = -9.078, *sig.*), and the survey email (z = -3.586, *sig.*). Personal finance was significantly more likely to be deemed as genuine compared to the survey email (z = -5.471, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **emails containing authority and time urgency cues across different email contexts** in Study 9. Read the email context type from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The conference email containing authority and time urgency cues was deemed less likely to be genuine compared to the invoice email containing authority and time urgency technique cues / the invoice email containing authority and time urgency cues was deemed more likely to be genuine compared to the conference email with authority and time urgency cues.

	Conference	Invoice	Loss of Access	Personal Finance	Survey
Conference	⬛	🟧	🟩	🟧 ●	🟩 ●
Invoice	🟩	⬛	🟩	🟩 ●	🟩
Loss of Access	🟧	🟧	⬛	🟧	🟧
Personal Finance	🟩 ●	🟧 ●	🟩	⬛	🟩
Survey	🟧 ●	🟧	🟩	🟧	⬛

Note. *Green = For the email context in the row title on average people believed the email was **more likely to be genuine** compared to the email context in the column title. Orange = For the email context in the row title on average people believed the email was **less likely to be genuine** compared to the email context in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Emails containing scarcity and time urgency cues – The conference email was significantly less likely to be deemed as genuine compared to the invoice email (z = -6.132, *sig.*), but more likely compared to the loss of access (z = -5.905, *sig.*) and survey emails (z = -10.098, *sig.*). The invoice email was significantly more likely to be deemed as genuine compared to the loss of access (z = -10.863, *sig.*), personal finance (z = -6.571, *sig.*), and survey emails (z = -11.879, *sig.*). The loss of access email was significantly less likely to be deemed as genuine compared to the personal finance email (z = -5.662, *sig.*), but marginally more likely than the survey email (z = -3.247, *p* = 0.001166). The personal finance email was significantly more likely to be deemed as genuine compared to the survey email (z = -7.051, *sig.*).

Matrix highlighting the significant differences between pairwise comparisons for probability judgements of phishing for **emails containing scarcity and time urgency cues across different email contexts** in Study 9. Read the email context type from the row to compare with the column title to interpret the significance and direction of the comparison. E.g., The conference email containing scarcity and time urgency cues was deemed less likely to be genuine compared to the invoice email containing scarcity and time urgency technique cues / the invoice email containing scarcity and time urgency cues was deemed more likely to be genuine compared to the conference email with scarcity and time urgency cues.

	Conference	Invoice	Loss of Access	Personal Finance	Survey
Conference	▨	🟧	🟩	⬜	🟩
Invoice	🟩	▨	🟩	🟩	🟩
Loss of Access	🟧	🟧	▨	🟧	🟩 ●
Personal Finance	⬜	🟧	🟩	▨	🟩
Survey	🟧	🟧	🟧 ●	🟧	▨

Note. Green = For the email context in the row title on average people believed the email was ***more likely to be genuine*** *compared to the email context in the column title. Orange = For the email context in the row title on average people believed the email was* ***less likely to be genuine*** *compared to the email context in the column title. White = No significant differences (p > .1). Black dot = Difference was in the direction of significance (p < .1 but p > .0006849315).*

Appendix H – *Table of means and standard deviation for the VAS probability estimations of emails being genuine/phishing (Definitely phishing = -100, definitely genuine = +100) from Study 9.*

Condition	Mean	Standard Deviation
Conference: Authority + Time Urgency	32.52	58.39
Invoice: Authority + Time Urgency	54.51	51.70
Loss of Access: Authority + Time Urgency	3.90	67.34
Personal Finance: Authority + Time Urgency	45.99	55.10
Survey: Authority + Time Urgency	19.53	65.98
Conference: Authority	55.83	48.59
Invoice: Authority	58.17	51.60
Loss of Access: Authority	-.38	70.91
Personal Finance: Authority	28.42	68.18
Survey: Authority	51.78	48.20
Conference: No Persuasion Cues	-6.63	66.36
Invoice: No Persuasion Cues	50.23	57.66
Loss of Access: No Persuasion Cues	-5.05	68.08
Personal Finance: No Persuasion Cues	17.57	66.47
Survey: No Persuasion Cues	34.50	60.40
Conference: Scarcity + Time Urgency	25.40	58.87
Invoice: Scarcity + Time Urgency	49.75	54.68
Loss of Access: Scarcity + Time Urgency	-6.87	69.38
Personal Finance: Scarcity + Time Urgency	18.35	65.81
Survey: Scarcity + Time Urgency	-22.73	60.65

Conference: Scarcity	20.46	58.91
Invoice: Scarcity	33.93	56.63
Loss of Access: Scarcity	2.39	67.84
Personal Finance: Scarcity	51.35	50.92
Survey: Scarcity	-4.69	62.98
Conference: Time Urgency	17.84	60.27
Invoice: Time Urgency	60.14	49.03
Loss of Access: Time Urgency	-6.59	68.15
Personal Finance: Time Urgency	44.60	58.62
Survey: Time Urgency	2.23	63.98

Appendix I – *Study 9 binary logistic regressions for each of the 30 email conditions examining whether probability estimations of phishing likelihood were associated with behavioural responses (respond/not respond).*

Conference with no persuasion cues: The binary logistic regression model was statistically significant, $X^2(1) = 127.52$, $p < .001$. The model explained 56% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 85.2% of cases. Those who chose to respond were 1.038 times more likely to rate the email as likely being genuine than those who chose not to respond.

Conference with authority cues: The binary logistic regression model was statistically significant, $X^2(1) = 88.45$, $p < .001$. The model explained 39.4% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 83% of cases. Those who chose to respond were 1.032 times more likely to rate the email as likely being genuine than those who chose not to respond.

Conference with scarcity cues: The binary logistic regression model was statistically significant, $X^2(1) = 105.54$, $p < .001$. The model explained 44.3% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 77.1% of cases. Those who chose to respond were 1.032 times more likely to rate the email as likely being genuine than those who chose not to respond.

Conference with time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 125.96$, $p < .001$. The model explained 50.6% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 78.6% of cases. Those who chose to respond were 1.036 times more likely to rate the email as likely being genuine than those who chose not to respond.

Conference with authority and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 114.76$, $p < .001$. The model explained 46.1% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 76.4% of cases. Those who chose to respond were 1.033 times more likely to rate the email as likely being genuine than those who chose not to respond.

Conference with scarcity and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 104.09$, $p < .001$. The model explained 42.9% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 76.8% of cases. Those who chose to respond were 1.031 times more likely to rate the email as likely being genuine than those who chose not to respond.

Invoice with no persuasion cues: The binary logistic regression model was statistically significant, $X^2(1) = 183.76$, $p < .001$. The model explained 82.4% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 95.9% of cases. Those who chose to respond were 1.063 times more likely to rate the email as likely being genuine than those who chose not to respond.

Invoice with authority cues: The binary logistic regression model was statistically significant, $X^2(1) = 130.25$, $p < .001$. The model explained 66.7% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 92.6% of cases. Those who chose to respond were 1.047 times more likely to rate the email as likely being genuine than those who chose not to respond.

Invoice with scarcity cues: The binary logistic regression model was statistically significant, $X^2(1) = 170.27$, $p < .001$. The model explained 66.4% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 89.3% of cases. Those who chose to respond were 1.048 times more likely to rate the email as likely being genuine than those who chose not to respond.

Invoice with time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 126.81$, $p < .001$. The model explained 70.5% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 94.1% of cases. Those who chose to respond were 1.054 times more likely to rate the email as likely being genuine than those who chose not to respond.

Invoice with authority and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 142.88$, $p < .001$. The model explained 73% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 93.7% of cases. Those who chose to respond were 1.058 times more likely to rate the email as likely being genuine than those who chose not to respond.

Invoice with scarcity and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 148.69$, $p < .001$. The model explained 68.6% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 93.4% of cases. Those who chose to respond were 1.035 times more likely to rate the email as likely being genuine than those who chose not to respond.

Loss of access with no persuasion cues: The binary logistic regression model was statistically significant, $X^2(1) = 187.07$, $p < .001$. The model explained 68.1% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 87.1% of cases. Those who chose to respond were 1.039 times more likely to rate the email as likely being genuine than those who chose not to respond.

Loss of access with authority cues: The binary logistic regression model was statistically significant, $X^2(1) = 178.13$, $p < .001$. The model explained 64.6% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 88.6% of cases. Those who chose to respond were 1.027 times more likely to rate the email as likely being genuine than those who chose not to respond.

Loss of access with scarcity cues: The binary logistic regression model was statistically significant, $X^2(1) = 146.81$, $p < .001$. The model explained 55.9% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 84.1% of cases. Those who chose to respond were 1.03 times more likely to rate the email as likely being genuine than those who chose not to respond.

Loss of access with time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 201.66$, $p < .001$. The model explained 70.8% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 89.3% of cases. Those who chose to respond were 1.043 times more likely to rate the email as likely being genuine than those who chose not to respond.

Loss of access with authority and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 205.97$, $p < .001$. The model explained 71% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 89.3% of cases. Those who chose to respond were 1.043 times more likely to rate the email as likely being genuine than those who chose not to respond.

Loss of access with scarcity and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 143.56$, $p < .001$. The model explained 56% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 83% of cases. Those who chose to respond were 1.03 times more likely to rate the email as likely being genuine than those who chose not to respond.

Personal finance with no persuasion cues: The binary logistic regression model was statistically significant, $X^2(1) = 161.58$, $p < .001$. The model explained 59.9% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 83.4% of cases. Those who chose to respond were 1.034 times more likely to rate the email as likely being genuine than those who chose not to respond.

Personal finance with authority cues: The binary logistic regression model was statistically significant, $X^2(1) = 223.99$, $p < .001$. The model explained 80% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 93% of cases. Those who chose to respond were 1.053 times more likely to rate the email as likely being genuine than those who chose not to respond.

Personal finance with scarcity cues: The binary logistic regression model was statistically significant, $X^2(1) = 120.48$, $p < .001$. The model explained 54% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 90.4% of cases. Those who chose to respond were 1.04 times more likely to rate the email as likely being genuine than those who chose not to respond.

Personal finance with time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 162.42$, $p < .001$. The model explained 68.7% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 90% of cases. Those who chose to respond were 1.046 times more likely to rate the email as likely being genuine than those who chose not to respond.

Personal finance with authority and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 123.60$, $p < .001$. The model explained 52.9% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 87.8% of cases. Those who chose to respond were 1.035 times more likely to rate the email as likely being genuine than those who chose not to respond.

Personal finance with scarcity and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 196.25$, $p < .001$. The model explained 69.3% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 88.6% of cases. Those who chose to respond were 1.033 times more likely to rate the email as likely being genuine than those who chose not to respond.

Survey with no persuasion cues: The binary logistic regression model was statistically significant, $X^2(1) = 117.96$, $p < .001$. The model explained 47.1% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 76.8% of cases. Those who chose to respond were 1.033 times more likely to rate the email as likely being genuine than those who chose not to respond.

Survey with authority cues: The binary logistic regression model was statistically significant, $X^2(1) = 74.65$, $p < .001$. The model explained 33.9% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 78.6% of cases. Those who chose to respond were 1.028 times more likely to rate the email as likely being genuine than those who chose not to respond.

Survey with scarcity cues: The binary logistic regression model was statistically significant, $X^2(1) = 94.79$, $p < .001$. The model explained 45.7% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 82.3% of cases. Those who chose to respond were 1.033 times more likely to rate the email as likely being genuine than those who chose not to respond.

Survey with time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 114.5$, $p < .001$. The model explained 51% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 82.7% of cases. Those who chose to respond were 1.036 times more likely to rate the email as likely being genuine than those who chose not to respond.

Survey with authority and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 112.16$, $p < .001$. The model explained 45.7% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 76% of cases. Those who chose to respond were 1.028 times more likely to rate the email as likely being genuine than those who chose not to respond.

Survey with scarcity and time urgency cues: The binary logistic regression model was statistically significant, $X^2(1) = 91.04$, $p < .001$. The model explained 52.5% (Nagelkerke R^2) of the variance in the choice to respond/not respond to the email and correctly classified 89.7% of cases. Those who chose to respond were 1.04 times more likely to rate the email as likely being genuine than those who chose not to respond.

Appendix J - *Percentage of participants in Study 10, who responded within time constraints, who chose to respond to the email within each persuasion technique and email context condition. Each table corresponds with a time constraint condition: a) 13s, b) 19.5s, c) 26s, d) 32.5s, e) 39s. Numbers in brackets indicates proportion of datapoints for that condition. i.e., (number of participants who chose to respond to the email/total number of participant datapoints for that condition).*

a)

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	40.5% (17/42)	67.5% (27/40)	42.5% (17/40)	47.5% (19/40)	40% (18/45)
Time Urgency	50% (21/42)	84.8% (39/46)	39.1% (18/46)	65.1% (28/43)	42.2% (19/45)
Authority	72.1% (31/43)	87.8% (36/41)	21.1% (8/38)	69.4% (25/36)	72.7% (32/44)
Scarcity	56.8% (25/44)	64.3% (27/42)	31.7% (13/41)	60% (24/40)	33.3% (15/45)
Authority + Time Urgency	37.8% (17/45)	69.2% (27/39)	45.2% (19/42)	56.1% (23/41)	76.3% (29/38)
Scarcity + Time Urgency	38.6% (17/44)	59.5% (22/37)	37.2% (16/43)	66.7% (26/39)	40.5% (17/42)

b)

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	36.5% (19/52)	83.3% (45/54)	39.6% (21/53)	50% (23/46)	34.6% (18/52)
Time Urgency	34.6% (18/52)	89.1% (49/55)	36.4% (22/55)	88.7% (47/53)	27.8% (15/54)
Authority	57.7% (30/52)	86.5% (45/52)	41.2% (21/51)	77.6% (38/49)	70.4% (38/54)
Scarcity	47.1% (24/51)	76.9% (40/52)	30% (15/50)	59.3% (32/54)	13.5% (7/52)
Authority + Time Urgency	42.3% (22/52)	75.5% (40/53)	41.2% (21/51)	49.1% (26/53)	94% (47/50)
Scarcity + Time Urgency	39.6% (21/53)	67.3% (37/55)	39.6% (21/53)	62% (31/50)	26.4% (14/53)

c)

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	23.1% (12/52)	72.5% (37/51)	40% (20/50)	58.8% (30/51)	50% (26/52)
Time Urgency	41.2% (21/51)	92.6% (50/54)	51.9% (28/54)	88.5% (46/52)	33.3% (17/51)
Authority	75.5% (40/53)	94.4% (51/54)	44.2% (23/52)	75% (36/48)	56.6% (30/53)
Scarcity	44.2% (23/52)	80.4% (41/51)	36% (18/50)	62% (31/50)	18.9% (10/53)
Authority + Time Urgency	53.8% (28/52)	81.5% (44/54)	52.8% (28/54)	62.7% (32/51)	80.4% (41/51)
Scarcity + Time Urgency	37.7% (20/53)	72% (36/50)	49% (25/51)	79.2% (42/53)	20.8% (11/53)

d)

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	21.8% (12/55)	72.7% (40/55)	37% (20/54)	58.5% (31/53)	44.4% (24/54)
Time Urgency	38.2% (21/55)	85.5% (47/55)	47.3% (26/55)	68.5% (37/54)	32.7% (18/55)
Authority	74.1% (40/54)	85.2% (46/54)	43.6% (24/55)	71.7% (38/53)	70.4% (38/54)
Scarcity	48.1% (25/52)	76.4% (42/55)	76.4% (42/55)	58.5% (31/53)	18.9% (10/53)
Authority + Time Urgency	34.5% (19/55)	69.1% (38/55)	50.9% (28/55)	49% (25/51)	81.5% (44/54)
Scarcity + Time Urgency	41.5% (22/53)	66% (35/53)	29.1% (16/55)	72.7% (40/55)	30.2% (16/53)

e)

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	28.6% (16/56)	76.8% (43/56)	41.1% (23/56)	58.2% (32/55)	48.2% (27/56)
Time Urgency	38.2% (21/55)	90.9% (50/55)	41.1% (23/56)	80.4% (45/56)	26.8% (15/56)

Authority	73.2% (41/56)	87.3% (48/55)	42.9% (24/56)	76.8% (43/56)	65.5% (36/55)
Scarcity	55.6|% (30/54)	83.3% (45/54)	44.4% (24/54)	54.7% (29/53)	10.9% (6/55)
Authority + Time Urgency	43.6% (24/55)	61.1% (33/54)	49.1% (27/55)	42.6% (23/54)	86.8% (46/53)
Scarcity + Time Urgency	36.4% (20/55)	61.8% (34/55)	49.1% (27/55)	78.2% (43/55)	23.6% (13/55)

Appendix K - *Average probability estimations (%) participants in Study 10, who responded within time constraints, indicated the likelihood emails were genuine across persuasion technique and email context conditions. Each table corresponds with a time constraint condition: a) 13s, b) 19.5s, c) 26s, d) 32.5s, e) 39s. Numbers in brackets indicates proportion of datapoints for that condition.*

a)

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	47.9% (47)	63.4% (48)	45.8% (48)	52.7% (46)	54.4% (46)
Time Urgency	55.4% (48)	78.9% (48)	40.5% (48)	64.9% (49)	48.3% (49)
Authority	73.6% (49)	75.8% (47)	36.1% (48)	63.8% (45)	69.8% (48)
Scarcity	61.1% (46)	64.7% (47)	37.6% (49)	57.3% (47)	41.3% (48)
Authority + Time Urgency	47.3% (48)	62.4% (46)	57.4% (46)	58.6% (48)	73.2% (48)
Scarcity + Time Urgency	46.7% (49)	58.9% (49)	39.9% (47)	63.1% (46)	49.2% (47)

b)

Persuasion Technique	**Email Context**				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	46% (54)	74.3% (55)	45.5% (55)	54.5% (52)	53.4% (55)
Time Urgency	51.5% (53)	83.8% (53)	43.1% (55)	76.7% (54)	47.2% (55)
Authority	60.6% (55)	76.9% (54)	47.7% (55)	65.7% (53)	72.5% (54)
Scarcity	56.2% (55)	68.2% (54)	43.8% (53)	52.4% (55)	28.8% (55)
Authority + Time Urgency	50.3% (53)	67.7% (54)	60.6% (53)	59.7% (54)	82.4% (54)
Scarcity + Time Urgency	54.8% (54)	62.8% (55)	45.4% (55)	65.7% (55)	45% (55)

c)

Persuasion Technique	Email Context				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	37.5% (54)	69% (53)	46.7% (54)	60.3% (54)	66.8% (53)
Time Urgency	51.6% (54)	77.5% (54)	54.7% (54)	74.5% (54)	49.4% (53)
Authority	74.3% (53)	79.1% (54)	46.8% (54)	69.5% (54)	67.2% (54)
Scarcity	58.4% (54)	73.8% (51)	41.6% (51)	64.5% (51)	37.4% (53)
Authority + Time Urgency	65.1% (54)	76.9% (54)	66.8% (53)	66.6% (54)	75.1% (53)
Scarcity + Time Urgency	47.9% (54)	64% (51)	50.9% (54)	72.3% (54)	39.2% (54)

d)

Persuasion Technique	Email Context				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	40% (55)	68.6% (55)	48.4% (55)	62.2% (55)	62.5% (54)
Time Urgency	56.2% (55)	79.3% (55)	52.5% (55)	70.9% (55)	55.5% (55)
Authority	76.1% (55)	78.5% (55)	43.8% (55)	64.1% (55)	76.9% (55)
Scarcity	61.4% (54)	66.3% (55)	48.3% (55)	58.2% (53)	41.9% (55)
Authority + Time Urgency	51.8% (55)	70.2% (55)	63.6% (55)	63.7% (54)	74.2% (55)
Scarcity + Time Urgency	55% (55)	60.1% (55)	41.4% (55)	74.3% (55)	53.1% (55)

e)

Persuasion Technique	Email Context				
	Conference	Invoice	Loss of Access	Personal Finance	Survey
None	44.3% (56)	69.6% (56)	46.3% (56)	60.5% (55)	64.9% (56)
Time Urgency	49.7% (55)	82.5% (55)	50.1% (56)	72% (56)	43.2% (56)

Authority	72.6% (56)	77.2% (56)	52.5% (56)	69.8% (56)	77.8% (56)
Scarcity	61.2% (54)	72% (54)	47.6% (55)	54.9% (54)	28.8% (55)
Authority + Time Urgency	47.5% (55)	61.5% (54)	64% (55)	58% (54)	73.4% (53)
Scarcity + Time Urgency	48.1% (55)	59.7% (55)	47.5% (56)	74.2% (55)	40.9% (55)