AHFE 2023: Vol. XX, 2023
doi: 10.54941/ahfeXXXX

Maladaptive Behaviour in Phishing Susceptibility: How Email Context Influences the Impact of Persuasion Techniques

George Raywood-Burke[1,2,3,4], Dylan M. Jones[1,2], and Phillip L. Morgan[1,2,3,5]

[1]Human Factors Excellence Research Group, School of Psychology, Cardiff University, Tower Building, 70 Park Place, Cardiff, CF10 3AT, UK

[2]Centre for Artificial Intelligence, Robotics and Human Machine Systems, Cardiff University, Tower Building, 70 Park Place, Cardiff, CF10 3AT, UK
[3]Airbus Central R&T, The Quadrant, Celtic Springs Business Park, Newport, NP10 8FZ, UK
[4]Trimetis, 59 Queen Square, Bristol, BS1 4JZ, UK
[5]Lulea University of Technology, Psychology, Division of Health, Medicine & Rehabilitation, Sweden

ABSTRACT

With over 80-90% of cyber incidents occurring in businesses and home settings often due to human errors in decision making (CybSafe, 2020; World Economic Forum, 2022; Verizon, 2022), a human-centric approach to cyber-security is needed to understand mechanisms behind maladaptive behaviours. One key area is susceptibility to phishing emails. Whilst some have investigated the success of different persuasion techniques in phishing susceptibility – most notably use of authority, urgency, and scarcity – less is known about how the wider context of the email (e.g., financial vs a work-related event) could influence the success of such techniques. The current paper presents initial findings from a repeated measures experiment where 271 participants included in the final analysis, recruited via Prolific (2022), judged whether they would or would not respond to presented email content containing a range of contexts and persuasion techniques. Diverging from previous research, participants were not necessarily more likely on average to respond to emails containing a persuasion technique, with large differences in persuasion success greatly depending upon the email context – with the proportion of response likelihood varying from 13.3% to 87.5% of participants choosing to respond. From this, not only do we demonstrate the successful impact of the main persuasion techniques and email context combinations upon phishing, but how overreliance on available information can bias individuals to engage in maladaptive cyber security behaviours.

Keywords: Cyberpsychology, Phishing, Persuasion, Urgency, Availability Bias, Human Factors

INTRODUCTION

How phishing has changed over time is key to understanding why people may be falling susceptible to this type of cyber threat. Whilst mass phishing – sending such emails to as many people as possible – is one method adopted by cyber criminals posing a very serious cyber threat, a more recent trend appears to indicate a focus on quality over quantity (Proofpoint, 2020). Spear phishing, i.e., phishing emails which are more targeted to individuals, organisations, or business, is a technique

which appears to be highly experienced with increasing reported rates in recent years (Proofpoint, 2020; Griffiths, 2023).

In order for such emails to be designed, they need to appear more convincing to individuals rather than being generically written for a mass audience; for example, by personalising them. Adopting persuasion techniques such as the six principles of persuasion detailed in Cialdini (2009) – authority, scarcity, liking, social proof, reciprocity, and commitment and consistency – in email content, for example, is being adopted to encourage a greater response rate. The more successful of these appear to be including cues which indicate the email is from an authoritative figure or includes authoritative language, instilling a need to respond urgently, or provide the impression on the scarce availability of something which could be desired (De Bona & Paca, 2020; Williams, Hinds, & Joinson, 2018; Akbar, 2014; Butavicus et al., 2015).

However, there are two key factors which need to be explored further in this line of research in order to more clearly identify significant risks of cyber security through phishing. First, the extent to which each major persuasion technique is successful should be compared. Given that time urgency appears to be even more successful in eliciting responses compared to authority (De Bona & Paci, 2020) – whereby authority has previously been thought to be the most successful method of persuasion (Akbar, 2014), and conflicting findings being found for scarcity (e.g., Lin et al., 2019; Parsons et al., 2019) – we were also interested in combining time urgency with authority and availability scarcity to establish whether combining techniques further increases susceptibility.

The second factor which we investigated we believed could also be of great importance to understand susceptibility was email context. The subjective utility to replying/not replying, to an email could largely depend up the perceived potential outcomes for each email. The utility of replying/not replying to a conference invitation may not be equal to the same decision faced when encountering an email describing the need to change a password with the risk of losing access to work-related shared folders, which in turn may not be equal to an email calling for the need to review payroll details to check for errors. Such weighting of differences in subjective utility could subsequently alter user cost-benefit analysis in deciding which action to take that provides the greatest probability of achieving the most desirable outcome. Thus, differences in email context could explain the variance in success rates for different persuasion techniques in phishing. Considering the dearth in previous research appearing to have not controlled for email context when examining the success of persuasion techniques in phishing, this present research is intended to address such a gap.

Through manipulating persuasion techniques and context, we created a paradigm in which participants would be asked to decide whether to respond, or not respond, to emails presented to them in a randomised order. We predicted, in line with previous research, that the adoption of at least one persuasion technique would result in higher response rates compared to emails containing no cues to potential malevolence. We also predicted significant differences in response rates between differing email contexts and inclusion of persuasion techniques due to differences in subjective utility. As this appears to be the first study to consider a range of persuasion techniques across multiple contexts in a controlled experiment, there is little basis to predict the direction of differences between each persuasion

technique adopted combined with differing contexts – though we did explore what differences may occur due to included manipulations.

METHODS

Participants

A UK representative sample of 300 participants was recruited online via Prolific (2022), though 29 were excluded due to missing/incomplete data – resulting in 271 datasets included in the final analysis. Ages ranged between 18-89-years (*M* 45.91, *SD* 16.10), and an almost even balance between sexes (137 female, 133 male, 1 preferred not to say). Participants well educated (all at least UK GCSE standard) with 85.3% holding at least UK A Levels or equivalent qualifications, and 60.9% an undergraduate degree. Participants reported spending ~6 hours online per day (*M* 5.98, *SD* 3.11), 84.1% indicated previously having experienced phishing emails, and nearly half of participants had suspected an email of being phishing up to a fortnight before taking part in the study (49.8%). Informed consent was obtained from all participants, and upon completion they were provided with a full debrief. Participants received £8 for taking part. The experiment was approved by the Cardiff University School of Psychology Research Ethics Committee (CU-SREC).

Design and Materials

A 5x6 repeated measures experimental design was adopted. One independent variable (IV) was email context with five levels: conference (invitation), invoice (confirm or review a purchase order on behalf of self or company), personal finance (notification of being at risk of losing leave days or incurring loss of payment due to errors), loss of access (notification of being at risk of losing access to a work-related computer account or shared folders), and survey (request to complete a survey which may consist of providing personal information or feedback).

The second IV was persuasion technique included within emails with six variations – authority (included authoritative language and cues such as titles indicating sender authority), time urgency (calls for the need to reply within a limited time), scarcity of quantity (included 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 (email was passively written, no cues to indicate any degree of malevolence).

Images of 30 emails were created – one for each combination of persuasion condition and context condition. Each email consisted of only text content (no email addresses, links, attachments, images etc.), and would always refer to the need to click a link or attachment in the text; however, referenced links/attachments could not be viewed (e.g., to see a contents preview or full link). Word count of each email was constrained to between 100-150 words and followed a uniform structure (introduction – e.g., dear xyz, main content, email signature). Images were then presented in a program developed in *Psychopy* one

at a time in the centre of the screen, with the question "Would you respond or not respond to this email?" positioned below the email along with buttons for respond/not respond. The dependant variable (DV) for the initial findings reported in this paper was the proportion of participants who had chosen to respond/not respond to each of the 30 emails.

Procedure

Upon signing up to the study on *Prolific* (2022), participants were provided with a link to a survey developed in *Qualtrics* © and presented with a consent form. After providing demographic information, participants were provided with a link to the email task created in *Psychopy* and run online in the browser via *Pavlovia*. From clicking the link and opening the new tab, the task interface would expand across the full screen to avoid any potential onscreen distractors. On first opening the email task, participants would be instructed for the purpose of the study to imagine they were an individual called "Christie" who worked as an employee for a company called "Tech Supplies Ltd." as part of their south west division. Christie was involved in daily business operations and worked on technology-based projects within the company. Participants were asked to imagine themselves and complete the task as though they were this person.

Participants were informed they would be presented with 30 emails, one at a time, for which they had to read and indicate whether they would respond or not respond. After confirming understanding of the instructions and completing a practice trial, participants would then work through the 30 main email trials. Emails were presented to all participants in a random order, and they were able to complete the task in their own time with no time constraints. After completing the task, participants were instructed to return to the *Qualtrics* survey and read a debriefing form with information about the experimental manipulations.

RESULTS

All 271 participants included in the analysis provided responses for all email trials. Data was collected on the number of participants who had indicated they would respond/not respond to each email (see Table 1 for descriptive summary). A Bonferroni correction was adopted to reduce susceptibility to statistical errors from the 146 total tests which were carried out across the same data, with p = 0.00034246575 being calculated as the new p value for determining statistical significance.

From chi-squared tests of independence, analyses found there were significant differences in response proportions across all emails context conditions for each persuasion technique condition – Authority (x^2 (4, N = 271) = 112.293), Scarcity (x^2 (4, N = 271) = 319.704), Time Urgency (x^2 (4, N = 271) = 232.780), Authority + Time Urgency (x^2 (4, N = 271) =167.153), Scarcity + Time Urgency (x^2 (4, N = 271) = 279.377), and no technique (x^2 (4, N = 271) = 208.327). Significant differences were found for response proportions across all persuasion technique conditions within the Conference (x^2 (5, N = 271) = 127.463), Invoice (x^2 (5, N = 271) = 34.179), Personal Finance (x^2 (5, N = 271) = 69.964), and Survey (x^2 (5, N = 271) = 244.113) context conditions. For the Loss of Access context, no

significant differences between persuasion techniques were found in response proportions (x^2 (5, N = 271) = 12.447, p = .029).

Table 1. Percentage of participants 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%

Differences between persuasion techniques

Conference emails – when no technique was adopted, significantly fewer participants responded to the email compared to emails containing authority cues (x^2 (1, N = 271) = 112.044), authority with time urgency (x^2 (1, N = 271) = 28.143), scarcity cues with time urgency (x^2 (1, N = 271) = 18.426), and fewer choosing to respond when the conference email contained no technique compared to containing time urgency cues was in the direction of significance as determined by the Bonferroni correction (x^2 (1, N = 271) = 11.771, p = 0.000602). Significantly more participants responded to emails containing authority cues compared to those with scarcity cues (x^2 (1, N = 271) = 62.657), time urgency cues (x^2 (1, N = 271) = 54.913), authority with time urgency combined (x^2 (1, N = 271) = 31.009), and scarcity combined with time urgency (x^2 (1, N = 271) = 43.192).

Invoice emails – when the email adopted scarcity cues, significantly fewer participants responded compared to authority cues (x^2 (1, N = 271) = 16.183), time urgency cues (x^2 (1, N = 271) = 23.505), authority with time urgency (x^2 (1, N = 271) = 18.1), and fewer participants responded compared to no technique in the direction of significance (x^2 (1, N = 271) = 11.953, p = 0.000545).

Personal finance emails - when no technique was adopted significantly fewer participants responded compared to emails containing authority cues (x^2 (1, N = 271) = 20.949), scarcity cues (x^2 (1, N = 271) = 36.956), time urgency cues (x^2 (1, N = 271) = 40.563), and authority + time urgency (x^2 (1, N = 271) = 25.394). Significantly more participants responded emails containing scarcity cues alone compared to scarcity + time urgency (x^2 (1, N = 271) = 20.913). Significantly more participants responded to the email containing time urgency cues alone compared to scarcity + time urgency (x^2 (1, N = 271) = 23.705). More participants responded to the email containing authority and time urgency cues combined than an email which contained scarcity + time urgency, although this

difference was marginally non-significant (x^2 (1, N = 271) = 12.356, p = 0.000439).

Survey emails - when no technique was adopted, significantly fewer participants responded compared to emails containing authority cues (x^2 (1, N = 271) = 27.254), but significantly more participants responded with no technique than scarcity (x^2 (1, N = 271) = 39.071), time urgency (x^2 (1, N = 271) = 27.883), and scarcity cues + time urgency (x^2 (1, N = 271) = 72.653). The email containing authority cues had significantly more participants responding compared to scarcity (x^2 (1, N = 271) = 123.953), time urgency (x^2 (1, N = 271) = 104.875), authority + time urgency (x^2 (1, N = 271) = 44.163), and scarcity + time urgency (x^2 (1, N = 271) = 173.723). Significantly fewer participants responded for scarcity compared to authority + time urgency (x^2 (1, N = 271) = 23.325). Significantly more participants responded to the email containing authority + time urgency than time urgency alone (x^2 (1, N = 271) = 14.756), and for scarcity + time urgency (x^2 (1, N = 271) = 51.335). More participants responded to the email containing time urgency cues alone compared to scarcity + time urgency in the direction of significance (x^2 (1, N = 271) = 12.184, p = 0.000482).

Differences between email contexts

Emails containing no persuasion technique – significantly fewer participants chose to respond to conference emails than invoice (x^2 (1, N = 271) = 187.597), personal finance (x^2 (1, N = 271) = 41.808), and survey emails (x^2 (1, N = 271) = 29.942). Significantly more participants responded to the invoice email than loss of access (x^2 (1, N = 271) = 121.575), personal finance (x^2 (1, N = 271) = 63.08), and survey emails (x^2 (1, N = 271) = 79.14).

Emails containing authority cues – significantly fewer participants responded to the conference email compared to the invoice email (x^2 (1, N = 271) = 17.679), but significantly more participants responded for the conference email compared to the loss of access email (x^2 (1, N = 271) = 38.907). Significantly more participants responded to the invoice email than the loss of access (x^2 (1, N = 271) = 102.28), personal finance (x^2 (1, N = 271) = 16.183), and survey emails (x^2 (1, N = 271) = 19.226). Significantly fewer participants responded to the loss of access email compared to the personal finance (x^2 (1, N = 271) = 41.181), and survey emails (x^2 (1, N = 271) = 36.707).

Emails containing scarcity cues – significantly fewer participants responded to the conference email compared to the invoice (x^2 (1, N = 271) = 68.744) and personal finance emails (x^2 (1, N = 271) = 90.643), but more compared to the survey email (x^2 (1, N = 271) = 13.743). Significantly more participants responded to the invoice email than the loss of access (x^2 (1, N = 271) = 32.106), and survey emails (x^2 (1, N = 271) = 131.412). Significantly fewer participants responded to the loss of access email compared to the personal finance (x^2 (1, N = 271) = 51.095), and survey emails (x^2 (1, N = 271) = 38.047). Significantly more

participants responded to the personal finance email than the survey email (x^2 (1, N = 271) = 163.925).

Emails containing time urgency cues – significantly fewer participants responded to the conference email compared to the invoice (x^2 (1, N = 271) = 141.703) and personal finance emails (x^2 (1, N = 271) = 86.574). Significantly more participants responded to the invoice email than the loss of access (x^2 (1, N = 271) = 127.456) and survey emails (x^2 (1, N = 271) = 214.153). Significantly fewer participants responded to the loss of access email compared to the personal finance (x^2 (1, N = 271) = 74.881) and survey emails (x^2 (1, N = 271) = 15.423). Significantly more participants responded to the personal finance email compared to the survey email (x^2 (1, N = 271) = 148.911).

Emails containing authority and time urgency cues – significantly fewer participants responded to the conference email compared to the invoice (x^2 (1, N = 271) = 93.957) and personal finance emails (x^2 (1, N = 271) = 38.514). Significantly more participants responded to the invoice email compared to the loss of access (x^2 (1, N = 271) = 83.652), personal finance (x^2 (1, N = 271) = 14.396), and survey emails (x^2 (1, N = 271) = 117.94). Significantly fewer participants responded to the loss of access email than the personal finance email (x^2 (1, N = 271) = 31.628). Significantly more participants responded to the personal finance email than the survey email (x^2 (1, N = 271) = 55.509).

Emails containing scarcity and time urgency cues – significantly fewer participants responded to the conference email compared to the invoice (x^2 (1, N = 271) = 90.999), personal finance (x^2 (1, N = 271) = 14.288), and survey emails (x^2 (1, N = 271) = 54.878). Significantly more participants responded to the invoice email than the loss of access (x^2 (1, N = 271) = 108.504), personal finance (x^2 (1, N = 271) = 35.812), and survey emails (x^2 (1, N = 271) = 253.259). Significantly fewer participants responded to the loss of access email compared to the personal finance email (x^2 (1, N = 271) = 22.369), but more replied compared to the survey email (x^2 (1, N = 271) = 42.347). Significantly more participants responded to the personal finance email than the survey email (x^2 (1, N = 271) = 117.811).

All other comparisons resulted in finding no significant differences in response rates.

DISCUSSION

The main aim of the present experiment was to examine potential differences in phishing susceptibility for a range of known successful persuasion techniques across multiple email contexts. From initial findings, analyses indicate the context of the email significantly influences the likelihood of falling susceptible to potential phishing emails – with noted differences in the success of different persuasion techniques across each email context. Findings – in general – do not support the hypothesis that persuasion techniques would increase the likelihood

of responding to emails; instead – it seems that success (that could be described as failure in terms of cyber security) is dependent upon the context of the email. For example, authority cues increased responses to the conference email but not in the case of loss of access. Despite having the highest response rate of 87.5%, time urgency cues did not increase response rates compared to using no technique in the context of invoices. Invoices, however, on average had very high response rates regardless of persuasion techniques compared to all other contexts.

Furthermore, when examining differences between combining authority and scarcity with time urgency, vs each of these methods individually, it appears as though across the contexts studied the combination conditions do not appear to be more successful than their respective individual counterpart conditions; with patterns suggesting the level of success of both combined could be weighted upon the success of the individual persuasion techniques in the given context (e.g., in the survey email context – authority had 69% response rate, 25.1% for time urgency, but 40.5% for authority and time urgency combined). Although, in one instance combining two persuasion techniques resulted in a lower response than both techniques individually – scarcity, time urgency, and scarcity + time urgency in the context of personal finance.

Despite previous research on the inclusion of time urgency cues in phishing emails consistently indicating a high risk to cyber security (De Bona & Paci, 2020; Cui et al., 2020; Marett & Wright, 2009; Parsons et al., 2015; Vishwanath et al., 2011; Williams, Hinds, & Joinson, 2018), we found success rates for time urgency cues varied from 87.5% to 25.1% across different email contexts – with similar varied findings for authority and scarcity. Our findings build upon this previous research threefold: First, we demonstrate that the context of emails can also be a significant factor in increasing phishing email susceptibility. Second, that susceptibility to phishing persuasion techniques can be dependent upon the context in which they are used – thus suggesting both should be considered when developing awareness training for susceptibility factors. Third, we highlight the serious problem of availability bias in phishing susceptibility.

Unlike previous research, our paradigm allowed for a high level of control and manipulation over what information was presented. Participants were presented with only the manipulated content of emails which, whilst referring to them as part of the decision to respond, hid email addresses, links, attachments, and other cues which could be used to judge whether presented emails were genuine or phishing. In reality, the main body text content of an email alone has no real indication of whether an email is genuine or phishing (e.g., authority cues could appear in both genuine and phishing emails), and yet our findings show large differences in response likelihood purely on the basis of the information available to them – thus demonstrating how easily subjective utility could be manipulated by cyber criminals. However, people can, and do, use other cues to determine whether emails are genuine or not (e.g., Sturman et al., 2023) – thus our findings simply detail the worst-case scenarios in which people are relying too heavily upon information not predictive of phishing risk. Interventions to aid the reduction in phishing susceptibility should focus less upon awareness of cues in

email content, and instead focus upon other cues which may be more predictive of phishing susceptibility.

This experiment forms part of a larger project. Future experiments in this series will further examine subjective utility and probability judgements in relation to phishing, whilst controlling for the influence of other key variables influencing cyber security attitudes and engagement in maladaptive behaviour. Subsequently, this conglomeration of information could highlight where the weightings of risky decision making may lie within and between individuals in respect to phishing susceptibility.

To conclude, analysis of behaviour has clearly shown phishing susceptibility can be greatly manipulated by the use of targeted persuasion techniques across email contexts. To address these concerns, not only should future research and training focus on spotting these persuasion cues with their associated contextual importance, but how other critical cues outside of email content could (and should) be used to avoid the overreliance upon unreliable available information putting individuals, organisations, and businesses at risk to phishing threats.

ACKNOWLEDGMENT

This research was supported through an Endeavr Wales funded PhD studentship awarded to the first author held by the School of Psychology at Cardiff University. Other support was provided by Airbus whereby the first author was a member of the Human Factors and Cyberpsychology team under the technical supervision of the last author who led this team and is now Director of the Airbus Centre of Excellence in Human-Centric Cyber Security at Cardiff University. The authors thank Dr David Greeno (also at Cardiff University) for technical support with the materials. We dedicate this AHFE paper to our dearly departed colleague and friend - Professor Dylan M Jones OBE (1948-2022) for his unparalleled support and mentorship.

REFERENCES

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

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.

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.*

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

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/

Griffiths, C. (2023). The Latest 2023 Phishing Statistics (Updated January 2023). AAG.

https://aag-it.com/the-latest-phishing-statistics/

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.

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

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.*

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

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

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.

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

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.

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.

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