Exploring workers' subjective experiences of habit formation in cyber-security: A qualitative survey

Dr Emily I M Collins[1]* and Dr Joanne Hinds[2]

[1] Human Factors Excellence (HuFEx), School of Psychology, Cardiff University, Cardiff, CF10 3AT, UK

[2] Information, Decisions and Operations (IDO), School of Management, University of Bath, Claverton Down, Bath, Somerset, BA2 7AY

*corresponding author: collinse6@cardiff.ac.uk, +44 (0)29 208 70716

Acknowledgements

We would like to thank Dr Katarzyna Stawarz for her very helpful comments and suggestions on a previous draft of this manuscript.

Author Contribution

Both authors planned the research and obtained the funding. The first author led the analysis and drafted the manuscript. The second author double-coded and contributed to the analysis, and edited and contributed to the manuscript.

Author Disclosure Statement

The authors have no competing interests to disclose

Funding Statement

This work was funded by the Research Institute in Science of Cyber Security (RISCS) and the UK Home Office, via funding from the National Cyber Security Programme.

Abstract

Employee behaviours remain at the centre of the cyber-security of workplaces, despite the challenges they face in doing so. Time-pressures and competing demands mean users tend to rely on habitual behaviours that often run counter to good cyber-security practice. One possible solution may be to encourage positive habit formation. Designing such interventions, however, relies on knowledge of the perception and experience of habit formation in the context of cyber-security. To this end, a qualitative survey containing open-ended questions was completed by 195 participants (mean age=35.51, 53% female) recruited via an online participant panel. Participants were asked what cyber-security behaviours they perform at work and how they believe any habits were prompted, formed and maintained. Thematic analysis identified three over-arching themes: (1) *forming habits unavoidably or unconsciously* (some were mandated, or formed without conscious awareness), (2) *consciously cultivating habits* (including the roles of intrinsic motivation and external prompts), and (3) *social and organisational influences* (including the influence of occupational culture, social modelling, previous experiences and information gathering practices). Based on these findings, we present guidelines for supporting workplace cyber-security habit formation reflecting these subjective experiences, namely introducing automatic solutions, facilitating external cues, fostering interest in cyber-security issues amongst employees, creating a positive cyber-security occupational culture and highlighting positive behaviour, and providing access to accessible cyber-security information to employees. These results constitute a first step in identifying how habits can be exploited for positive cyber-security behaviour change in a way that accounts for the reliance on habitual behaviours in busy, time-pressured workplaces.

Introduction

Cyber-attacks on organisations can result in huge financial loss, compromised data, and loss of future business [1,2] . Despite attempts to make technology secure by default [3], users remain at the centre of cyber-security [4]. Understanding how users can be supported in making secure choices is therefore vital, especially as traditional approaches, such as workplace training and awareness campaigns are not always successful in promoting secure behaviour [5–7].

One possible explanation for this lack of success is the often high-pressured, time-restricted nature of work tasks and environments. Time pressures and preoccupation with primary tasks (e.g. the work itself) often mean security behaviours or checks are abandoned to prioritise the task at hand [8,9], ignoring cyber-security policies [10,11]. In these environments, individuals are then more likely to rely on habitual, automatic behaviours rather than follow less-ingrained guidelines [12]. Indeed, habits are often argued to be the underlying reason behind unsecure behaviours, for instance unquestioningly clicking "accept" on security pop-ups [13], or rejecting software updates.

Therefore, one way to change cyber-security behaviour may be to focus on changing and forming positive cyber-security habits. Habits can be defined as behaviours automatically prompted by environmental or temporal cues [14], distinct from non-habitual behaviours which require conscious consideration. Although there is a relative lack of research on habit formation for cyber-security behaviours, the formation and adaptation of habits has received substantial attention in health-related behaviours, from washing hands, to healthy eating and exercise routines. In these cases, a habit-based approach is chosen predominantly because habits do not always require the individual to consciously decide to perform the behaviour or rely on feeling motivated to do so [15]**.** As a result, encouraging individuals to develop positive habits has the potential to create longer lasting behaviour change [16]. Interventions that focus on forming positive habits are grounded in the understanding that habits develop as a result of the behaviour being performed in a stable context, with associations between the context and behaviour building over multiple repetitions [17,18].

Interventions designed based on the principles of habit formation therefore tend to provide external cues to prompt or remind the user [19], or provide motivations or incentives to create opportunities for multiple repetitions of the behaviour [20].

However, encouraging cyber-security behaviours in this manner presents a unique challenge. Unlike health behaviours, many workplace security behaviours confer no noticeable, direct benefit to the individual, and motivation tends to come from organisation-level rules that the employee may not understand or care about. Although the development of habits is likely to be the same from a practical perspective (i.e. repetitions of cued behaviours), it is not currently known whether the subjective experiences, motivations and perceptions of the process in cyber-security are different. Considering the importance of habits in workplace security behaviours, and the need to better support employees in making secure choices, there is a clear gap in the understanding of the subjective experiences of habit formation for cyber-security behaviours, which is needed in order to design effective, habit-based interventions in this context. This work therefore aimed to address this gap. To this end, this study used an exploratory, qualitative, online survey to explore the subjective experiences of habit formation for cyber-security behaviours in the workplace.

Method

Participants

A total of 195 participants (aged 18-66, *M*=35.51, *SD*=10.24, median age=36, 53% female) completed the questionnaire though Prolific's survey panel (www.prolific.ac), and were compensated £1.80. All but three participants were based within the UK. The majority always worked from a particular place of work (64.85%), with 34.16% sometimes working remotely, and a breakdown of industry roles can be found in Table 1.

Procedure

Ethical approval was granted by the School of Management, University of Bath, UK. The survey was hosted by Qualtrics (www.qualtrics.com). Participants were informed that they would be awarded an additional payment of 50p if they provided more in-depth responses, in order to incentivise greater detail. Participants were asked open-ended questions covering what cyber-security behaviours participants performed at work, which behaviours they believed constituted habits, what prompted these habits and how they formed them (see Table 2).

Data analysis

Cyber-security behaviours were coded according to content. Answers to the open-ended questions were analysed using inductive thematic analysis [21] due to our exploratory approach, using ATLAS.ti. Coding was therefore data-driven, and codes were assigned based on the sentiments being expressed. Responses were initially coded by the first author, and a subset was then second coded by the second author. This subset of codes was then compared to check for consistency and agreement on the interpretation and categorisation of the statements. In the rare case of discrepancies across the two sets of codes, consensus was reached through discussions and remaining codes were updated in light of discussions. Through discussions between the authors, the codes were grouped into themes.

Results and discussion

In order to contextualise the responses, the behaviours participants reported to perform were collated (see Supplemental Data for the full list). The most popular behaviour was logging off

computers (n=67), with the majority of others centring around passwords: changing passwords regularly (n=64), using complex passwords (n=33) that are not shared between accounts (n=25), written down (n=19), or shared with others (n=34).

Analysis of the open-ended questions identified three over-arching key themes: *forming habits unavoidably or unconsciously* (including the subthemes of *unavoidable behaviours* and *mysterious and automatic habits*)*, consciously cultivating habits* (including *intrinsic motivation* and *external prompts*) and *social and organisational influences* (including *organisational culture, social modelling, previous experiences* and *information gathering*). Quotes are attributed according to the allocated participant number, indicated by the number in brackets following each quote (for example, P1 denotes Participant 1).

Forming habits unavoidably or unconsciously

Unavoidable behaviours

The most common response to the open-ended questions (66 instances) was that the "habit" was forced by their employer, organisational policy, or by technology: *"These aren't so much habits, more requirements"* (P9). As such, the habit was unavoidable: *"[It's] the only way to make the systems work."* (P7).

This reflects the move towards security-by-design, and the notion that removing unsecure options reduces the security risks introduced by a lack of user motivation or knowledge. However, despite this theme, it is important to note that relying entirely on removing choices can result in reduced autonomy, which negatively impacts security policy compliance [22], and encourages the creation of workarounds, especially if the behaviour is arduous [23,24]. It is therefore likely that this approach only works for certain security behaviours, for example, ones that do not disrupt primary tasks, or ones that users do not value control over.

Mysterious and automatic habits

Even for those who felt they had control over their cyber-security behaviours, there was an inability to articulate how the habits had been developed or started. Frequent codes relating to this theme included "I just do them" (44 instances; *"I just started doing them. I did not use any methods to make them a habit",* P1), that they have always done it (23 instances; *"I do these automatically as we have always had to."* P177), or that it's common knowledge, so no habit formation was needed (18 instances; *"Just used my common sense and decided to keep my technology items safe."* P48). These codes correspond well to measures of behavioural automaticity and habit strength [25], suggesting that these behaviours do constitute habits, and that cyber-security habits manifest similarly to others.

Often, there was an acknowledgement that the habit was formed out of repetition (28 instances), a well-established component of habit formation in the literature [15,17,19]. However, these responses tended to imply that starting this process was effortless and a result of the passing of time (*"Do it over and over again, and after the first thirty or so repetitions it tends to stick",* P193). This runs somewhat counter to literature suggesting that habits start with an initial effort, before multiple repetitions can occur [15], although it has been argued that individuals do not always have an awareness of what has prompted their behaviour [26]. This might relate to the previous theme of some behaviours being unavoidable; these will have been initiated out of necessity but still subject to multiple repetitions, causing the behaviour to become habitual even without this effortful action.

Consciously cultivating habits

Intrinsic motivation

For others, their reasons for starting security habits came from intrinsic motivation derived from their own personal awareness or knowledge of cyber-security (11 instances; *"Just an understanding of computer security and safety and also the exploitative methods by criminals"*, P138), or just an interest in cyber-security. Some actively sought out additional information to direct and maintain habits outside of workplace training (4 instances; *"I started watching some video tutorials on YouTube about cyber-security"*, P92). This echoes previous research emphasising the importance of intrinsic motivation in habits [27] and the impact of existing knowledge on cyber-security behaviours [28].

For others, the habit came from a sense of responsibility, an order-oriented personality, or a desire to protect their employer or maintain safety (8 instances, *"I am just a very conscientious by nature, I am a worrier and always double and triple check everything"* P176). Some wanted to protect their own personal security or privacy (16 instances; *"I didn't want people in the office to go on my computer for whatever reason as it is an invasion of privacy. I have personal random documents on the computer also",* P184). One distinguishing feature of cyber-security behaviours (versus health behaviours) is the relative lack of direct, personal impact; this finding suggests that for some, seeing the potential for their work behaviours to affect their personal security creates personal investment. Therefore, highlighting possible outcomes that may impact individuals personally (rather than just the organisation) might be effective in encouraging habit formation.

External prompts

Participants who discussed consciously starting a cyber-security behaviour mostly cited automated solutions (43 instances), either to remind them to do something (*"I setup a reminder in my email calendar to change [my password] every month",* P164), enable a security action to be

done automatically (*"I make notes and I have safety apps and programs automatically update.",* P154), or remove the frictions to a behaviour (*"I've set up shortcuts to our secure file server, rather than save to the laptop's drive, which makes doing the secure thing easier",* P82). This reflects the need for solutions that require minimal input, and that maximise the mental and physical resources available for their primary task, and as literature suggesting that people often select the easiest cues to implement [29].

Others used more visual reminders, such as notes to themselves (*"Before it became a habit we had notes on our monitors to remember to lock our computers",* P18), or using the pertinent item itself as a reminder (*"Tried to build systemic habits by always having things in their certain place, that way if my pass was ever missing or not on my person in work hours it would immediately stand out as obvious*", P177). The use of external cues is well-established, especially in the initial stages of starting a new behaviour [30,31], suggesting that this could be an effective strategy for employees.

Social and organisational influences

Occupational culture

In line with literature [32,33], the wider cyber-security culture in the workplace appeared to play a role in the formation of habits. For some, this consisted of either very clear or well-enforced security processes, expectations or rules (18 instances; *"We are told when we start work what must be done and what rule must be adhered to as security is taken very seriously. it is instilled in us from the start so it becomes second nature very quickly",* P151), punishments or repercussions for deviations (19 instances; *"The IT policy is very strict and I have seen colleagues lose their jobs over it.*" P42), or at least a fear of such punishments (4 instances; *"These habits come from worry and anxiety, of not wanting to be reprimanded or have the concern that I could be disciplined, lose pay or my job",* P176).

For others, there was a softer approach, such as the introduction of more security-aware policies (10 instances; "*New trust-wide policies that automatically lock your PC after 5 mins but we have been encouraged to lock [it] ourselves if we leave our desks",* P59). Habits were maintained through ongoing engagement via general reminders from management (7 instances, *"We are regularly reminded by our employers and they actively monitor the situation on a daily basis."* P131), newsletters and updates (6 instances, *"We receive regular updates form IT about dangerous emails that we should not open",* P123), notices and posters in the workplace (12 instances, "*Sometimes at a work computer a sign is stuck on saying "remember to log off when you leave" etc",* P27) and security meetings (5 instances).

Social modelling

Others reported modelling the behaviour of colleagues (13 instances*; "I saw that others were in the habit of doing this and decided that it was a good precaution to take" P134*), or being supported by colleagues' reminders or through self-policing (*"People helped remind you to do these things.", P5*). Several mentioned the use of joke punishments for violations of security measures (5 instances; *"Most people leave their PCs unlocked. It's even become a running joke to send silly emails from someone else's PC while they're in the bathroom", P156*), which made people more inclined to avoid falling victim. Social modelling has been argued to be important in a variety of behaviours [34], although cyber-security is rarely seen as a social behaviour. This finding suggests that encouraging a few colleagues to start cyber-security habits might in turn encourage others, as might the communication of social trends (e.g. social norms).

Previous experiences

Some habits were supported by previous experiences, particularly those relating to individual or company-wide cyber-attacks or breaches (35 instances; *"Through mistakes and a few*

errors over the years at home on my own [personal] computers, such as downloading files which turned out to be Trojan Horses and getting malware from various websites…This has conditioned me to be more vigilant with how I conduct myself when I use my computer", P162). This experience either highlighted a previously unknown or underestimated risk, or provided more specific motivation to protect themselves against future incidences (*"The main reason though is that in the past I was unaware of these types of emails and unfortunately my personal computer developed a virus after opening one",* P195)

Other experience, such as previous job roles in more security-sensitive workplaces created habits that participants reported to transfer to their present position (11 instances, "*Not sharing passwords with other people was due to working in a bank where it was a serious offence.*" P148). For others, their experiences at home formed these habits (17 instances, *"I started all of these habits by doing them first in my personal life, and it became second nature whenever relevant in business too",* P168). A related code within this theme was also more general experience working with technology (9 instances), with participants finding that being familiar with technology resulted in better habits (*"I have always been aware of computer viruses as long as I have been using devices…and have always tried to remain cyber safe"*, P146) reflecting the impact of previous knowledge on cyber-security behaviours [28].

These incidences likely highlighted the potential consequences and impact of inaction, indicating that for those without these experiences, communicating real examples of what has happened to others might be effective.

Information gathering

Participants also reported to have been prompted (or required) to start or maintain their cyber-security habit through training or security checks offered by their workplace (54 instances, *"I*

have previously written passwords down but after going through a number of security online training programmes at work I no longer do this.", P16).

Interestingly, formal training was not the only source of information; others mentioned being inspired by advice from IT (6 instances), others outside of the workplace (4 instances), or in the news (5 instances): *"…updates from the work IT department about SPAM emails, news stories about security breaches or human error, e.g. doctor leaving patient notes on train",* P114. It therefore appears that providing information and justification for the behaviours (especially through less formal routes) could be influential in initiating habit formation.

General discussion

This qualitative survey aimed to explore the subjective experience of habit formation for cyber-security in the workplace, identifying three over-arching themes based on these responses: *forming habits unavoidably or unconsciously*, *consciously cultivating habits*, and *social and organisational influences*. Our findings support much of the work exploring habit formation in other contexts indicating that established habit-based interventions may be applicable and successful in the context of cyber-security behaviours at work.

More specifically, the themes identified in the present research suggest that to support cyber-security habits, workplaces should: (i) aim to introduce automatic, secure-by-design solutions where appropriate, and facilitate the use of automatic reminders and external, visual cues when it is not, (ii) encourage intrinsic motivation by fostering an interest and investment in cyber-security (including highlighting personal gains), (iii) create a positive cyber-security occupational culture, including showcasing positive employee behaviour, (iv) provide real-world, relatable examples of the consequences of unsecure behaviours and finally, (v) provide access to suitable, accessible information on cyber-security, ideally outside of formal training. Our present findings are not,

however, able to inform on the practical aspects of implementing (and testing the efficacy of) such policies, something we hope future research will address.

Future work should continue to probe the underlying process of cyber-security habits. Our finding that many were not able to articulate the formation of their cyber-security habits reflects literature regarding a lack of awareness of environmental prompts. However, to design effective interventions exploiting successful habit formation strategies, we need to understand what these strategies are. Future work will therefore need to take an innovative, provocative approach to capture this process.

Limitations

It is also important to acknowledge several specific limitations. Our qualitative survey approach allowed for a large, varied sample, but will have also naturally skewed towards those more familiar with technology (and online participation platforms), which restricts generalisability. Our approach also prevented interesting statements being probed for more detail or for clarification. Future work may therefore wish to build upon these findings, conducting more focused, in-depth interviews on specific demographics in order to capture any additional nuance.

Conclusion

In sum, these results constitute a first step in identifying how habits can be exploited for positive cyber-security behaviour change in a way that accounts for the reliance on habitual behaviours in busy, time-pressured workplaces. With an understanding of how habits are currently formed and developed in these contexts, future interventions can explore whether capitalising on these processes can result in automatic security behaviours without the perception of additional burden on the users.

References

1. Acquisto A, Friedman A, Telang R. Is there a cost to privacy breaches? An event study. In: *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems*. ; 2006.

2. Chakraborty R, Lee J, Bagchi-Sen S, Upadhyaya S, Raghav Rao H. Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decis Support Syst*. 2016. doi:10.1016/j.dss.2015.12.007

3. The National Cyber Security Centre. *Secure by Default*.; 2017.

4. Renaud K, Flowerday S. Contemplating human-centred security & privacy research: Suggesting future directions. *J Inf Secur Appl*. 2017. doi:10.1016/j.jisa.2017.05.006

5. Bada M, Sasse MA, Nurse JRC. Cyber security awareness campaigns: Why do they fail to change behaviour? *Proc Int Conf Cyber Secur Sustain Soc*. 2015;(July):118–131.

6. Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: An action research study. *MIS Q Manag Inf Syst*. 2010. doi:10.2307/25750704

7. Ertan A, Crossland G, Heath C, Denny D, Jensen R. Cyber Security Behaviour In Organisations. *arXiv Prepr arXiv200411768*. 2020.

8. Chowdhury NH, Adam MTP, Skinner G. The impact of time pressure on cybersecurity behaviour: a systematic literature review. *Behav Inf Technol*. 2019;38(12):1290-1308. doi:10.1080/0144929X.2019.1583769

9. Kirlappos I, Parkin S, Sasse MA. Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security. *Usec '14*. 2014;(February):1-10. doi:10.14722/usec.2014.23<007>

10. Siponen M, Vance A. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Q Manag Inf Syst*. 2010;34(3):487-502.

11. Chan M, Woon I, Kankanhalli A. Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing , National University of Singapore Atreyi Kankanhalli School of Com. *J Inf Priv Secur*. 2005;1(3):18-41. doi:10.2307/3151312

12. Zafar H, Randolph A, Martin N. Toward a More Secure HRIS: The Role of HCI and Unconscious Behavior. *AIS Trans Human-Computer Interact*. 2017;9(1):59-74. doi:10.17705/1thci.00089

13. Coventry L, Briggs P, Blythe J, Tran M. Using behavioural insights to improve the public's use of cyber security best practices improve the public's use of cyber. *Gov Off Sci UK*. 2014.

14. Wood W, Neal DT. The habitual consumer. *J Consum Psychol*. 2009;19(4):579-592.

15. Lally P, Wardle J, Gardner B. Experiences of habit formation: A qualitative study. *Psychol Heal Med*. 2011;16(4):484-489. doi:10.1080/13548506.2011.555774

16. Gardner B, De Bruijn GJ, Lally P. A systematic review and meta-analysis of applications of the self-report habit index to nutrition and physical activity behaviours. *Ann Behav Med*. 2011;42(2):174-187. doi:10.1007/s12160-011-9282-0

17. Lally P, Van Jaarsveld CHM, Potts HWW, Wardle J. How are habits formed: Modelling habit formation in the real world. *Eur J Soc Psychol*. 2010;40:998-1009. doi:10.1002/ejsp

18. Wood W, Neal DT. A New Look at Habits and the Habit-Goal Interface. *Psychol Rev*. 2007. doi:10.1037/0033-295X.114.4.843

19. Gardner B, Lally P, Wardle J, et al. Making health habitual : the psychology of ' habit-formation ' and general practice. 2012;(December):664-666.

20. Lally P, Gardner B. Promoting habit formation. *Health Psychol Rev*. 2013.

doi:10.1080/17437199.2011.603640

21. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol*. 2006;3(2):77-101. doi:10.1017/CBO9781107415324.004

22. Alzahrani A, Johnson C, Altamimi S. Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. *2018 4th Int Conf Inf Manag ICIM 2018*. 2018:128-132. doi:10.1109/INFOMAN.2018.8392822

23. Dey D, Ghoshal A, Lahiri A. Security Circumvention: To Educate or To Enforce? *Proc 51st Hawaii Int Conf Syst Sci*. 2018;9:5195-5204. doi:10.24251/hicss.2018.648

24. Koppel R, Smith S, Blythe J, Kothari V. Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? *Stud Health Technol Inform*. 2015;208:215-220. doi:10.3233/978-1-61499-488-6-215

25. Gardner B, Abraham C, Lally P, de Brujin G-J. Towards parsimony in habit measurement: Testing the convergent and predictive validity of an automaticity subscale of the Self-Report Habit Index. *Int J Behav Nutr Phys Act*. 2012;9. http://www.embase.com/search/results?subaction=viewrecord&from=export&id=L52190776%5Cnhttp://www.ijbnpa.org/content/9/1/102%5Cnhttp://dx.doi.org/10.1186/1479-5868-9-102.

26. Orbell S, Verplanken B. The automatic component of habit in health behavior: Habit as cue-contingent automaticity. *Heal Psychol*. 2010;29(4):374-383. doi:10.1037/a0019596

27. Gardner B, Lally P. Does intrinsic motivation strengthen physical activity habit? Modeling relationships between self-determination, past behaviour, and habit strength. *J Behav Med*. 2013;36(5):488-497. doi:10.1007/s10865-012-9442-0

28. Wang PA. Assessment of Cybersecurity Knowledge and Behavior : An Anti-phishing Scenario. *ICIMP 2013 Eighth Int Conf Internet Monit Prot*. 2013;(c):1-7.

29. Stawarz K, Gardner B, Cox A, Blandford A. What influences the selection of contextual cues when starting a new routine behaviour? An exploratory study. *BMC Psychol*. 2020;8(1):1-11. doi:10.1186/s40359-020-0394-9

30. Stawarz K, Cox AL, Blandford A. Beyond Self-Tracking and Reminders: Designing Smartphone Apps That Support Habit Formation. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. CHI '15. New York, New York, USA: ACM Press; 2015:2653-2662. doi:10.1145/2702123.2702230

31. McDaniel MA, Einstein GO. The importance of cue familiarity and cue distinctiveness in prospective memory. *Memory*. 1993;1(1):23-41. doi:10.1080/09658219308258223

32. Wiley A, McCormac A, Calic D. More than the individual: Examining the relationship between culture and Information Security Awareness. *Comput Secur*. 2020;88. doi:10.1016/j.cose.2019.101640

33. Van 't Wout MC. Develop and Maintain a Cybersecurity Organisational Culture Develop and Maintain a Cybersecurity Organisational Culture. In: *14th International Conference on Cyber Warfare and Security*. ; 2019:457-466.

34. Higgs S, Thomas J. Social influences on eating. *Curr Opin Behav Sci*. 2016;9:1-6. doi:10.1016/j.cobeha.2015.10.005

Table 1. Breakdown of the industry roles of participants.

Industry Role	Percentage of Participants
Trained professional	20.30%
Administrative staff	20.30%
Middle management	15.84%
Junior management	14.85%
Self-employed	7.93%
Upper Management	6.93%
Support staff	3.96%
Consultant	2.97%
Skilled Labourer	1.98%
Researcher	0.99%
Temporary employees	0.50%
Other	3.47%

Table 2. List of open-ended questions in the online questionnaire

	Question text
1	We all engage in behaviours that make us and our employer safer. We're particularly interested in behaviours you might do in order to be 'cyber-secure' while at work. Please list as many as you can think of below.
2	Which of these behaviours/actions would you say are habits, or that you do automatically (e.g. you don't have to think to do them, and you find yourself doing them without noticing)?
3	What prompted you to start these habits?
4	How did you start this habit?
5	What methods did you use to make it a habit, or something you do automatically?
6	Did or do you use any prompts, reminders, apps, or any other method to try to help you do something to keep yourself or your company safe online?