How do we ensure users engage in secure online behavior?

A psychological perspective

Emma J Williams
School of Experimental Psychology
University of Bristol
Bristol, UK

Jan M Noyes
School of Experimental Psychology
University of Bristol
Bristol, UK

Bogdan Warinschi
Cryptography Research Group
Department of Computer Science
University of Bristol
Bristol, UK

***Abstract*— In the digital age, understanding the factors that determine whether humans engage in secure online behavior is increasingly important. The costs of not doing this are extremely high, in particular on user well-being. Unfortunately, theoretical understanding of this issue remains extremely limited. This paper considers current approaches to human aspects of cyber security and proposes future research directions to move this complex and continually evolving field forward.**

Keywords: cyber security; risk perception; decision-making; cognitive modeling; user behavior.

I. INTRODUCTION

Cyber-attacks are increasing worldwide, with a recent survey of more than 500 information security professionals highlighting that approximately 75% of their organizations had been the victim of a phishing attack in 2016 [1]. Continuing media reports of security breaches by users, such as a spear-phishing attack that targeted employees within the Ukrainian power grid in 2015, highlight the importance of understanding the factors that influence secure human behavior in cyberspace. This paper provides an overview of several factors that are likely to determine whether humans engage in secure online behavior and proposes a future research agenda that will allow the development of theoretically-based psychological models of user decision-making in the future. A sound theoretical understanding of these primary psychological mechanisms will inform and serve as foundation for more effective and targeted interventions to encourage secure behavior in online environments.

II. MAKING DECISIONS ABOUT ONLINE SECURITY

A. Understanding the Context of Secure Online Behavior

From online banking to health information, an individual's work and home life is increasingly governed by the online space. New encryption and authentication technologies offer an ever-increasing range of cyber security products that help users keep their online data secure. However, if emerging security products are to be effective within this setting, then individuals must feel both able and willing to use them. Despite the substantial amount of work that has been conducted regarding people's online security behavior [e.g., 2,3,4,5,6] the field still lacks a theoretical treatment which, in turn, precludes a more nuanced understanding regarding why people choose to engage in secure behavior or, more importantly, why they choose not to do so.

Engaging in secure online behavior takes resources, whether that is increased time or effort. For instance, it can take additional time to understand the protective technologies that are available and to implement them. It can also take time and effort to create and remember multiple complex passwords for an ever-growing number of online accounts. As early as the 1980s, the link between password selection and limitations in the structure of long-term memory was highlighted [7]. This increased effort, combined with the fact that security is often not people's primary goal when completing a task, can mean that secure online behavior can move down the priority list. To minimize the perceived costs to the individual of engaging in secure online behavior, it has been suggested [8] that information systems, and the protective mechanisms that they use, must engender psychological acceptability in users, which is turn will make the use of such protective mechanisms more likely to be considered routine.

When people are under pressure or distracted with other activities, their ability to engage in more resource-intensive, systematic forms of cognitive processing is also reduced. This can lead to a reliance on relatively automatic decision rules (known as heuristics) when making decisions, whereby an in-depth consideration of the potential costs and benefits of various decision options is not undertaken [9]. Recent experimental work conducted by one of the authors [10] investigated the impact of these processing strategies on whether participants chose to accept fraudulent and genuine computer updates in the form of 'pop-ups'. Overall, findings demonstrated that when updates interrupt participants during a challenging primary computer task, their ability to differentiate between fraudulent and genuine messages is reduced compared to when they are not completing any other tasks at the time that the message is viewed. Whereas the situational context was, therefore, found to have an impact on security-related decisions in this study, the potential role of individual differences in sensation seeking and other personality traits were found to be

This work is supported by a Vice Chancellor's Fellowship granted to the first author by the University of Bristol.

limited. The use of more resource-intensive, systematic processing strategies have also been linked with an increased ability to detect fraudulent emails, known as phishing emails, with the heuristic processing that people typically rely on when they are under cognitive pressure diminishing their ability to spot suspicious cues online [11]. It is likely, therefore, that decisions to engage in secure online behavior will be heavily influenced by the cognitive context in which individuals find themselves.

The importance of developing a thorough understanding of the role of cognition in online security behavior has been recently highlighted by [12]. In their consideration of the contribution that cognitive science can make to understanding human aspects of cyber security, the authors advocate for the use of cognitive modeling approaches within the cyber security domain, basing theoretical development on general principles of cognition that can be applied across various contexts. Such approaches have recently been used to explore the challenge of recalling and associating multiple passwords with different accounts [13], as well as understanding the impact of user mental models on security behaviors [14].

Finally, perceptions of risk related to the online world have also been shown to relate to user intentions to engage in secure behavior online. Protection Motivation Theory [15] examines how individual perceptions of threat and coping may impact decisions to engage in a protective behavior and is a well-established approach in the health behavior domain, providing a useful framework to identify areas where interventions can be targeted. The primary facets of Protection Motivation Theory include:

a. The perceived severity of a threatening scenario;

b. An individual's perceived vulnerability to that scenario;

c. The perceived efficacy of the protective behavior in reducing vulnerability to that scenario (response efficacy);

d. The perceived ability of the individual to engage in the relevant protective behavior (self-efficacy).

Protection Motivation Theory has recently been applied to individual intentions to engage in a range of cyber security behaviors, with these facets found to influence intentions to various degrees across a range of contexts, including the use of home wireless security [16], the adoption of anti-spyware software [17] and the use of anti-virus software on mobile phones [18].

B. Applying Psychological Frameworks

Both situational factors and individual factors are likely to impact whether people engage in secure online behavior. For instance, increased perceptions of online threats may motivate people to engage in protective actions, such as using encryption software or making their password stronger. However, higher perceived costs regarding the time and effort involved in understanding and accessing such software may suppress this motivation. Similarly, when faced with the potential option of activating stronger authentication processes on an email account, such as providing a phone number to enable 2-factor authentication, individuals who are currently operating under a high degree of stress, who have competing demands that are considered to be of a higher priority or who find the action itself to be too complex, may all be deterred.

The importance of understanding how users perceive a situation at any given point in time is highlighted in the development of recent frameworks for measuring these issues, such as the CAPTION framework [19]. CAPTION is a recently developed taxonomy of psychological situation characteristics, whereby situations are divided into seven primary categories that differentiate how a situation is subjectively perceived and experienced by individuals. These categories include:

1. How complex the situation is perceived to be (Complexity)
2. How stressful the situation is perceived to be (Adversity)
3. How typical the situation is perceived to be (Typicality)
4. How important the situation is perceived to be (Importance)
5. The positive emotions associated with the situation (Positive valence)
6. The negative emotions associated with the situation (Negative valence)
7. How amusing the situation is perceived to be (humor)

By combining an understanding of user perceptions of risk with an awareness of the situational constraints when an opportunity to enact a particular online security behavior is presented, it will be possible to tease apart the relative impact of these various factors on online security decisions. This will further our understanding and enable the design of more appropriate interventions.

Within the health behavior domain, models such as Protection Motivation Theory provide the basis for tailoring intervention messages to maximize the likelihood that a user will be encouraged to engage in a protective behavior. Message framing approaches, whereby messages that emphasize potential gains of engaging in a protective behavior are compared to messages that emphasize potential losses of not engaging in that behavior, have shown some success, particularly when they are matched with congruent personality types (i.e., people who are more sensitive to losses view loss-framed messages and those who are more sensitive to gains view gain-framed messages) [20]. The use of message framing, however, is thought to be limited when considering cyber security behavior [21,22,23]. This needs further investigation.

Work within the risk communication domain also has suggested that designing interventions in line with the primary constructs of Protection Motivation Theory can be effective. For instance, providing specific information related to the severity of a potential threat has been found to motivate information seeking about that threat, although interventions

based on other facets of Protection Motivation Theory have not been as successful [24].

Current understanding of what motivates people to seek protective information and follow this advice is extremely limited, even though accessing information about protective technologies is likely to be a crucial first step if users are to be persuaded to engage in secure behavior and use appropriate security products. For instance, understanding why it is important to encrypt a computer hard disk and how an individual can easily do this is a likely requirement in choosing to use encryption in the future. In this way, the decision to engage in secure online behavior at any single point in time can be broken down into several decision stages, each influenced by situational characteristics and individual perceptions of risk, which may itself present a 'pre-requisite' for the next decision option. Exploring this possibility is a key aim of our research agenda.

It can be seen, therefore, that further work is needed to determine: (a) the likely barriers of use to emerging security products at particular points in time; (b) whether tailoring messaging and other interventions according to these barriers would be effective in cyber security domains, and (c) at what stage in the decision process these interventions would be most effectively targeted. If individuals do not engage in a protective security behavior because they perceive themselves not to be vulnerable to online threats, for example, are interventions focused on increasing their perceived vulnerability likely to be more effective compared to those focused on reducing the perceived costs of engaging in a protective behavior? And if so, where in the decision cycle should these interventions be targeted?

III. Setting The Research Agenda

Progressing current understanding of secure online behavior remains a key challenge within the field of cyber security. It is, therefore, essential that a rigorous and multi-faceted approach is taken that will facilitate greater theoretical understanding of when people are likely to engage in secure behavior and why that may be, identifying the primary psychological mechanisms that influence these decisions at both the individual difference and situational level. To achieve this objective, the following research agenda is proposed.

A. Establishing Primary Research Principles

1) An Embedded Multidisciplinary Approach

It is increasingly recognized that cyber security is a complex issue that cannot be solved by one discipline alone. Taking a multidisciplinary approach, whereby computer scientists and psychologists/social scientists work in close collaboration, provides an opportunity to develop robust, theoretically based models of human behavior that are relevant to emerging technical challenges. As new technical cyber security solutions emerge, psychological insight and testing can be applied at an early stage. The combination of rigorous experimental psychology methods and human-computer interaction approaches will allow more comprehensive modeling of the decision-making scenario, whereby small changes in likely situational parameters can be explored and relevant improvements to technical systems made in line with these findings. Such an approach would maximize the likelihood that emerging technical solutions will be usable at both the cognitive and behavioral level.

2) Engaging with Data Science Opportunities

The growing field of data science provides a unique opportunity to exploit the vast amounts of data being produced daily regarding online interactions. The extent to which awareness campaigns and other interventions are shared on social media, the proportion of users who 'click-through' for further protective information following online training, and the number of those who choose to download and use security products, all present opportunities for researchers. Collaborating with data scientists and organizations that have access to such data provides an opportunity to test further and refine decision-making models that have been developed in laboratory settings, particularly if such platforms can also be used as a future test bed to examine potential impacts of various awareness and training interventions.

B. Prioritizing Future Research Directions

1) The Development of Evidence-Based Theoretical Models

Focusing on the development of theoretical models based on existing psychological mechanisms and principles will provide a robust theoretical basis for understanding secure online behavior. This will also provide an effective means to explore the impact of various factors on decision-making. Model parameters can be altered to understand the resultant impact on likely behavior and interventions targeted accordingly. By combining laboratory scenarios with field-based studies, predictions developed in more constrained laboratory conditions can then be tested and refined in so-called 'real world' contexts. The development of such models is vital if our understanding of human aspects of cyber security is to become more comprehensive, increasing the possibility that predictive approaches can be developed and exploited.

2) Addressing the Impact of Context

Individual decisions regarding whether to engage in secure behavior at a particular point in time is likely to be influenced by factors related both to the individual and the wider context in which they are operating at the time. Understanding the potential impact of this wider situational context is particularly relevant given that our interactions online are increasingly conducted on the move and via a range of different devices. A 2017 paper by one of the authors [25] provides an initial framework for exploring the interactions between individual differences and context in guiding online behavior, whereas the emergence of situational frameworks, such as CAPTION, provides a means through which these aspects can be further explored and assessed in a cyber security context [19]. By understanding the potential impact of situational factors on cyber security decisions, including how these may interact with individual differences, it may be possible to develop adaptive user interfaces that can adjust both how and when cyber security-related decision scenarios are presented to users in various contexts.

IV. Our Approach

In line with this agenda, our approach aims to identify the primary factors that determine whether humans engage in secure behavior online, investigating the situational and individual factors that have an impact on decision-making through a combination of experimental and field studies. These findings will then be used to develop and advance psychological theory on the primary drivers of secure online behavior, providing guidance on the design of future interventions and contributing to the potential future development of adaptive user interfaces that can effectively encourage secure online behavior in various contexts.

This will be achieved primarily by:

1. Close collaboration between experimental psychology and information security disciplines to identify cyber security scenarios that are directly relevant to current critical issues in cyber security (e.g., when do people choose to use more versus less secure passwords, or to reuse existing ones? When do people consider it worthwhile to use secure authentication processes and encryption?). These scenarios provide the basis for systematic investigation in experimental, laboratory-based studies, allowing various situational factors to be manipulated to examine the resultant impact on behavior.
2. Collaboration with data science disciplines and organizations to develop methods that utilize real-time data to add further insight to the findings of experimental work. For example, the potential to examine how people respond to security updates during real-time tasks in the digital health and smart city research space, or exploiting current data on responses to online cyber security training (such as engagement with materials and 'click-throughs' to further protective information).
3. Engagement with relevant organizations in the public and private sector to disseminate findings and develop collaboration opportunities that may assist in the development and testing of practical interventions.

This research agenda has relevance for the development of secure behavior within both organizations (i.e., the behavior of employees) and the public (i.e., engaging in online activities at home) and will serve as foundations for a rigorous understanding of human aspects of cyber security.

V. Primary Implications

This paper has considered the importance of understanding the context in which secure online behaviour takes place, including how this can be integrated within existing research approaches in this area. Specifically, we suggest that current methods for understanding how individuals perceive particular situations should be adapted and applied to better understand how people make decisions regarding online security. By combining these more subjective measures of situational characteristics with methods that aim to objectively manipulate or measure such aspects (e.g., competing priorities, time available), a thorough understanding of how secure online behaviour varies across contexts, and how this effect is best managed, can be developed.

Overall, this paper aims to stimulate a more theoretically-based research approach, while simultaneously focusing on the development of practical insights. This will ensure that emerging digital innovations can continue to be fully exploited by society in the future, with any emerging safety and security risks effectively managed.

References

[1] Wombat Security Technologies, "State of the Phish Report," accessed from https://info.wombatsecurity.com/ on 20th October 2017, 2017.

[2] M.W. Boyce, K.M. Duma, L.J. Hettinger, T.B. Malone, D.P. Wilson, and J. Lockett-Reynolds, "Human performance in cybersecurity: A research agenda," In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2011, pp. 1115-1119.

[3] H. Rosoff, J. Cui, and R.S. John, "Heuristics and biases in cyber security dilemmas," Environ Sys & Dec, 2013, vol. 33, pp. 517-529.

[4] A. Vishwanath, "Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack," Journal of Computer Mediated-Communication, 2015, vol. 5, pp.570-584.

[5] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, "Who falls for a phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010, pp. 373-382.

[6] S. Egelman, and E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (SeBIS)," In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2015, pp. 2873-2882.

[7] B.F. Barton, and M.S. Barton, "User-friendly password methods for computer-mediated information systems," Computers & Security, 1984, vol. 3, pp. 186–195.

[8] J.H. Saltzer, and M.D. Schroeder, "The protection of information in computer systems," Proceedings of the IEEE, 1975, vol. 63, 9, pp. 1278–1308.

[9] D. Kahneman, Thinking Fast and Slow. London, UK: Penguin, 2011.

[10] E.J. Williams, P. Morgan, and A.N Joinson, "Press accept to update now: individual differences in susceptibility to malevolent interruptions," Decision Support Systems, 2017, vol. 96, pp. 119–129.

[11] A. Vishwanath, B. Harrison, and Y.J. Ng, "Suspicion, cognition, and automaticity model of phishing susceptibility," Communication Research, online pre-print, 2016, pp. 1-21.

[12] I.X. Domínguez, P.R. Goodwin, D.L. Roberts, and R. St. Amant, "Human subtlety proofs: using computer games to model cognitive processes for cybersecurity," International Journal of Human–Computer Interaction, 2017, vol. 33, pp. 44-54.

[13] J. Zhang, X. Luo, S. Akkaladevi, and J. Ziegelmayer, "Improving multiple-password recall: An empirical study," European Journal of Information Systems, 2009, vol. 18 pp. 165–176.

[14] J. Blythe, and L.J. Camp, "Implementing mental models," In Proceedings of 2012 IEEE symposium on Security and privacy workshops, pp. 86–90, San Francisco, CA, 2012.

[15] R.W. Rogers, "A protection motivation theory of fear appeals and attitude change," Journal of Psychology, 1975, vol. 91, pp. 93–114.

[16] I.MY. Woon, G.W. Tan, and R.T. Low, "A protection motivation theory approach to home wireless security." In Proceedings of 26th International Conference on Information Systems, p. 31, 2005.

[17] T. Chenoweth, R. Minch, and T. Gattiker, "Application of protection motivation theory to adoption of protective technologies," In

Proceedings of the 42nd Hawaii International Conference on System Sciences, 2009.

[18] W. Al-Ghaith, "Extending protection motivation theory to understand security determinants of anti-virus software usage on mobile devices," International Journal of Computers, 2016, vol. 10, pp. 125-138.

[19] S. Parrigon, S.E. Woo, L. Tay, and T. Wang, "CAPTION-ing the situation: a lexically-derived taxonomy of psychological situation characteristics," Journal of Personality and Social Psychology, 2017, vol. 112, pp. 642-681.

[20] A.J. Rothman, and A.S. Baldwin, "A person x intervention strategy approach to understanding health behavior," In K. Deaux and M. Snyder (Eds.), The oxford handbook of personality and social psychology, pp.729-752, New York, NY: Oxford University Press, 2012.

[21] D.D. Caputo, S.L. Pfleeger, J.D. Freeman, and M.E. Johnson, "Going spear phishing: Exploring embedded training and awareness," IEEE Security & Privacy, 2014, vol. 12, pp. 28-38.

[22] K. Ivaturi, C. Chua, and L. Janczewski, "Impact of information seeking and warning frames on online deception: A quasi-experiment," Journal of Comp Inf Systems, 2017, vol. 57, pp. 139-147.

[23] M. Kajzer, J. D'Arcy, C.R. Crowell, A. Striegel, and D. Van Bruggen. "An exploratory investigation of message-person congruence in information security awareness campaigns," Computers & Security, 2014, vol. 43, pp. 64-76.

[24] K. Neuwirth, S. Dunwoody, and R.F. Griffin, "Protection motivation and risk communication," Risk Analysis, 2000, vol. 20, pp. 721-734.

[25] E.J. Williams, A. Beardmore, and A.N. Joinson, "Individual differences in susceptibility to malevolent influence online: a theoretical review," Computers in Human Behavior, 2017, vol.72, pp. 412-421.