The Enduring Mystery of the Repeat Clickers

Matthew Canham
University of Central Florida
Orlando, FL 32816 USA
mcanham@ist.ucf.edu

Stephen M. Fiore
University of Central Florida
Orlando, FL 32816 USA
sfiore@ist.ucf.edu

Michael Constantino
University of Central Florida
Orlando, FL 32816 USA
michael.constantino@ucf.edu

Bruce Caulkins
University of Central Florida
Orlando, FL 32816 USA
bcaulkin@ist.ucf.edu

Irwin Hudson
U.S. Army – CCDC Soldier Center
– Orlando, FL 32826
irwin.l.hudson.civ@mail.mil

Lauren Reinerman-Jones
University of Central Florida
Orlando, FL 32816 USA
lreinerm@ist.ucf.edu

Abstract
Individuals within an organization who repeatedly fall victim to phishing emails, referred to as Repeat Clickers, present a significant security risk to the organizations within which they operate. The causal factors for Repeat Clicking are poorly understood. This paper argues that this behavior afflicts a persistent minority of users and is explained as either the main effect of individual traits (personality or others) or is a moderated interaction between traits and other factors such as cultural influences, situational factors, or social engineering techniques. Because Repeat Clickers represent a disproportionate risk, identifying causal factors and developing mitigations for this behavior should provide substantial return on investment to improving the security of an organization. Developing such mitigations will require a better understanding of the individual differences contributing to repeat clicking behavior. We present pilot data and suggest research questions to improve understanding of the contributing factors of repeated victimization by phishing emails.

Author Keywords
Phishing; Repeat Clicking; Individual Differences.

ACM Classification Keywords
H.5.m. Security and privacy: Usability in security and privacy.

Introduction
Phishing is a social engineering technique that leverages email or other communication mediums to influence targeted individuals to take actions advantageous to attackers [6]. The 2018 Verizon Data Breach Investigations report estimates that 94% of all malware is delivered via email [22]. Technologically based solutions, such as disabling hyperlinks embedded in all emails, appear to be an obvious method to counter phishing attacks; but these solutions suffer from several major limitations that malicious actors exploit to compromise accounts [10]. In this paper we focus on a particularly problematic facet of phishing, Repeat Clickers, individuals who repeated fall victim to phishing emails and therefore represent a problematic minority of

users who disproportionately jeopardize the security of an organization.

The Problem of Repeat Clicking

Many organizations send simulated phishing emails to their users as a form of preventative training [3]. These simulations also provide an excellent resource for research data collection because they record which users clicked embedded links or downloaded attachments. A concerning phenomenon, that has emerged a result of these simulated phishing campaigns, is commonly referred to by security staff as "Repeat Clickers" [16]. Repeat Clickers represent a persistent minority of users who repeatedly fall victim to simulated phishing emails and represent a significant risk for most organizations. Exploratory pilot research by the authors found that while Repeat Clickers (users who failed three or more phishing tests) represented a small minority of the total employees in an organization (0.83%), this group was nearly ten times more likely to fail a simulated phishing campaign (failures defined as either clicking a simulated link, downloading an attachment, or replying to the sender) than a user from the general population. Some in the security community have advocated for increasingly harsher punishments for Repeat Clickers [18]. However, as [2] found, many Repeat Clickers already feel anger toward themselves for falling victim to phishing emails. Identifying the underlying causes for this behavior presents an opportunity to develop more effective mitigations to this behavior.

Theories focusing on phishing susceptibility falls into three broad categories. First, are theories that focus on dynamic factors such as contextual factors like cognitive load and cue detection, or the social engineering techniques employed in the phishing attack [17, 21, 20]. Next, are theories that focus on stable factors such as individual traits, or cultural influences on phishing susceptibility [1, 5, 9, 12]. Finally, hybrid perspectives incorporate both the dynamic and stable factors into their explanatory models to describe why some individuals might be more susceptible under specified conditions [20, 23]. In the following sections, we describe these frameworks and then conclude with a series of research questions to point the way forward to better understand the factors causing Repeat Clicking.

Dynamic Factors: Context

A significant contributing factor in falling victim to phishing is the individual's current state when evaluating an email. Users who might not, under "normal" circumstances, be susceptible to a phishing attack may be susceptible when distracted, or under significant cognitive load. Indeed, some research has found that users who click on phishing links often do so without completely reading the email or intending to so [2]. The descriptions these users provided for why they clicked the embedded link very closely approximates Norman's description of "slip errors". These are errors in which an individual is aware of the correct action, but executes the incorrect one because of distraction, habit, or goal fixation [13]. While contextual factors are very likely influential on a case by case basis, by themselves these factors do not explain the persistent nature of repeat clicking. A defining characteristic of Repeat Clickers is their consistency in clicking regardless of external factors. Because context is highly dynamic it is unlikely to account for the persistent aspect of Repeat Clickers. As such, additional factors should also be explored.

Dynamic Factors: Social Engineering Techniques

Dynamic theoretical frameworks focus on the social engineering techniques used in the email message. For example, research has demonstrated that messages that appear legitimate are more likely to result in users clicking links [11, 14, 24]. However, these techniques vary significantly between messages and are therefore unlikely to be the sole causal factor of Repeat Clicking because of the persistent nature of this behavior. What is more likely is that the social engineering technique employed has a moderating effect on an individual trait as [24] suggests.

Stable Factors: Cultural Influences

Theories concentrating on stable factors influencing phishing susceptibility tend to focus on either cultural influences, or individual

traits. Research examining cultural influences on vulnerability accounts for the broader influence that sociological factors can have on attitudes and behavior. For example, one study comparing personality, security knowledge, and cultural orientation, found that cultural orientation (along the individualism versus collectivism spectrum), was the strongest predictor in the identification of malicious emails, with individuals from highly individualistic cultures being better at detection [1]. If cultural influences are to account for Repeat Clicking, it would seem unlikely that this would only affect a small minority. However, it is possible that Repeat Clickers may overlap with an organizational subset (such as a single department) then this could explain cultural influences on this behavior. However, we suggest that, because Repeat Clickers represent a persistent minority, cultural influences are unlikely to be the sole causal factor [16].

Stable Factors: Individual Traits

Because repeat clicking behavior afflicts a persistent minority of users, we argue that individual traits account for the primary factor underlying this behavior. Research on trait related vulnerabilities have examined the influence of individual level factors on phishing susceptibility including personality traits, expertise, among other individual differences. We next discuss how these factors have been related to phishing susceptibility more broadly.

Big 5 Personality. The personality model most commonly examined in phishing research is the standard five factor model of personality (Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) [4]. How these factors influence phishing susceptibility is not always obvious as findings suggest that personality is merely one variable that may interact with others to change responses. For example, people high in conscientiousness might be less susceptible to phishing attempts as their attentional diligence could be an asset [11]. However, conscientiousness might also be leveraged as a vulnerability to make an attack more effective. For example, one study deliberately exploited conscientiousness by sending the target a request to correct an error in an attached timesheet [19].

Other Individual Traits. In addition to the Big 5 personality traits, Narcissism is a personality trait that appears to increase phishing susceptibility, with at least two studies showing positive correlations between levels of self-reported Narcissism and phishing vulnerability [5, 8]. Perhaps counter-intuitively, an individual's self-assessed capability to detect phishing emails appears to be unrelated to their actual susceptibility. Several studies have found no correlation between users' self-assessed ability and their actual detection ability [19, 15, 24].

Hybrid Perspectives

The prior review suggests that, although individual level traits likely play a role in Repeat Clicking, it is also likely that traits interact with contextual factors or social engineering techniques. Because of this likely interaction, some researchers have developed hybrid models for remote online social engineering susceptibility to begin laying a foundation for more systematic studies of phishing vulnerability. The *Social Engineering Personality Framework (SEPT)* [20], proposes that users high or low in certain dimensions of Big 5 personality traits are more (or less) generally susceptible to certain social engineering techniques. Although promising, the SEPT, also predicts that persons at the extremes of these dimensions might also be more (or less) susceptible to specific social engineering techniques. As such, it lacks clarity with regard to specifics of phishing susceptibility. The *Holistic Individual Susceptibility Model (HISM)* proposes that susceptibility results from an additive, or interactive, combination of the individual traits of the target, the target's current state, the context that the target is operating within, and influence mechanisms being employed by the attacker [23]. While the HISM provides a solid basis for future research, in its present form, this model does not address patterns of victimization or susceptibility to phishing. For example, susceptibility may not be a linear combination of factors, but rather certain types of susceptibility (as in susceptibility to repeated clicking of phishing

links) might result from different interactions of individual traits and external factors. In our concluding section, we attempt to redress this gap by providing a set of high-level recommendations to guide research in this area.

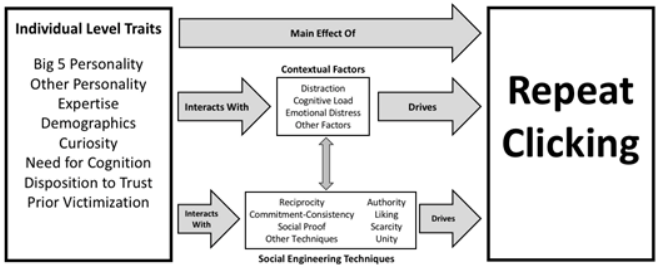

Figure 1: Individual traits research framework for understanding repeated victimization by phishing emails.

Current and Future Work

This review shows the nascent state of research on Repeat Clickers in the area of phishing attacks. The persistent nature of Repeat Clickers suggests that more than just situational factors (which tend to be fluid) are the sole cause of this problem (which seems to be stable and persistent). That this phenomenon afflicts a small subset of users, suggests that it is neither caused by message content nor cultural influence. While some research does suggest that specific individuals may be more generally susceptible to social engineering [24], more empirical work needs to be done to better understand this phenomenon. Building upon the work reviewed, we next present a set of research questions that we are currently studying with the goal of understanding the relationship between individual traits and susceptibility for Repeat Clickers (see Figure 1).

Research Question 1: Does Repeat Clicking result from a main effect of individual trait-related differences?

Research Question 2: Do individual traits interact with social engineering techniques to drive Repeat Clicking behavior?

Research Question 3: Is there an interaction between individual traits and situational factors (such as cognitive load, emotional distress, fatigue, etc.) contributing to Repeat Clicking?

The authors of this work are currently exploring the answers to these research questions through a series of experimental studies. Repeat Clickers, the persistent minority of users who repeatedly fall victim to phishing emails, represent a significant risk for the organizations they occupy. Understanding the factors associated with this phenomenon and developing effective mitigations presents behavioral scientists with an opportunity to make a significant impact in the improvement of information security. Given the lack of understanding of this behavior, an important scientific contribution for future research will be to further investigate the root causes of repeated victimization and possibly the identification of predictors for more susceptible individuals. Future work should seek to understand how cultural influences, individual level traits, contextual factors, and social engineering techniques all contribute to phishing susceptibility, both independently and interactively.

Acknowledgement

This research was in part sponsored by the U.S. Army CCDC Soldier Center and was accomplished under Cooperative Agreement Number W911NF-15-2-0100 for Dr. Irwin Hudson. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of U.S. Army CCDC Soldier Center or the U.S. Government.

The authors would also like to thank Stu Sjouwerman of KnowBe4 for the donation of software licenses to support this work.

References

1. Marcus Butavicius, Kathryn Parsons, Malcolm Pattinson, and Agata McCormac. 2016. "Breaching the human firewall: Social engineering in phishing and spear-phishing emails." arXiv preprint arXiv:1606.00887.
2. Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman, and M. Eric Johnson. 2013. "Going spear phishing: Exploring embedded training and awareness." IEEE Security & Privacy 12, no. 1 (2013): 28-38.
3. Anthony Carella, Murat Kotsoev, and Traian Marius Truta. 2017. "Impact of security awareness training on phishing click-through rates." In 2017 IEEE International Conference on Big Data (Big Data), pp. 4458-4466. IEEE, 2017.
4. Paul T. Costa Jr, Robert R. McCrae. 1992. "The five-factor model of personality and its relevance to personality disorders." Journal of personality disorders 6, no. 4 (1992): 343-359.
5. Shelby R. Curtis, Prashanth Rajivan, Daniel N. Jones, and Cleotilde Gonzalez. 2018. "Phishing attempts among the dark triad: Patterns of attack and vulnerability." Computers in Human Behavior 87 (2018): 174-182.
6. Christopher Hadnagy, Michele Fincher. 2015. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. John Wiley & Sons, 2015.
7. Tzipora Halevi, Jim Lewis, and Nasir Memon. 2013. "Phishing, personality traits and Facebook." arXiv preprint arXiv:1301.7643.
8. Tzipora Halevi, Nasir Memon, and Oded Nov. 2015. "Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks." Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015).
9. Brynne Harrison, Arun Vishwanath, and Raghav Rao. 2016. "A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing." In 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 5628-5634. IEEE.
10. InfoSec Institute. 2017. How Phishing Attacks Bypass Spam Filters. Retrieved August 1, 2018, from https://resources.infosecinstitute.com/please-volunteer/
11. Patrick Lawson, Olga Zielinska, Carl Pearson, and Christopher B. Mayhorn. 2017. "Interaction of Personality and Persuasion Tactics in Email Phishing Attacks." In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 61, no. 1, pp. 1331-1333. Sage CA: Los Angeles, CA: SAGE Publications.
12. Gregory D. Moody, Dennis F. Galletta, and Brian Kimball Dunn. 2017. "Which phish get caught? An exploratory study of individuals' susceptibility to phishing." European Journal of Information Systems 26, no. 6 (2017): 564-584.
13. Don Norman. 2013. The design of everyday things: Revised and expanded edition. Basic books, 2013.
14. Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram. 2015. "The design of phishing studies: Challenges for researchers." Computers & Security 52 (2015): 194-206.
15. Malcolm Pattinson, Cate Jerram, Kathryn Parsons, Agata McCormac, and Marcus Butavicius. 2012. "Why do some people manage phishing e-mails better than others?" Information Management & Computer Security 20, no. 1 (2012), 18-28.
16. PhishMe. 2015. Enterprise Phishing Susceptibility Report. Retrieved August 1, 2018, from https://cofense.com/wp-content/uploads/2017/10/PhishMe_EnterprisePhishingSusceptibilityReport_2015_Final.pdf
17. Robert W. Proctor, Jing Chen. 2015. "The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace." Human factors 57, no. 5 (2015): 721-727.
18. Spiceworks, 2018. Best practices for punishing repeat offenders of phishing. Spiceworks Community. Retrieved from https://community.spiceworks.com/topic/2142279-best-practices-for-punishing-repeat-offenders-of-phishing
19. Frantisek Sudzina, Antonin Pavlicek. 2017. "Propensity to Click on Suspicious Links: Impact of Gender, of Age, and of Personality Traits." In Bled eConference, p. 10.
20. Sven Uebelacker, Susanne Quiel. 2014. "The social engineering personality framework." In 2014 Workshop on Socio-Technical Aspects in Security and Trust, pp. 24-30. IEEE.

21. Arun Vishwanath, Brynne Harrison, and Yu Jie Ng. 2018. "Suspicion, cognition, and automaticity model of phishing susceptibility." Communication Research 45, no. 8 (2018): 1146-1166.
22. Verizon RISK Team. 2019. Data breach investigations report (DBIR).
23. Emma J. Williams, Amy Beardmore, and Adam N. Joinson. 2017. "Individual differences in susceptibility to online influence: A theoretical review." Computers in Human Behavior 72 (2017): 412-421.
24. Michael Workman. 2008. "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security." Journal of the American Society for Information Science and Technology 59, no. 4 (2008): 662-674.