Repeat Clicking:
A Lack of Awareness Is Not the Problem

Matthew Canham[1[0000-0001-7638-2023]]

[1] Beyond Layer Seven, LLC, Oviedo, FL, USA
mcanham@belay7.com

Abstract. Although phishing is the most common social engineering tactic employed by cyber criminals, not everyone is equally susceptible. An important finding emerging across several research studies on phishing is that a subset of employees is especially susceptible to social engineering tactics and is responsible for a disproportionate number of successful phishing attempts. Sometimes referred to as *repeat clickers,* these employees habitually fail simulated phishing tests and are suspected of being responsible for a significant number of real-world phishing related data breaches. In contrast to repeat clickers, *protective stewards* are those employees who never fail simulated phishing exercises and habitually report phishing simulations to their security departments. This study explored some of the potential causes of these persistent behaviors (both good and bad) by administering six semi-structured interviews (three repeat clickers and three protective stewards). Surprisingly, both groups were able to identify message cues for identifying potentially malicious emails. Repeat clickers reported a more internally oriented locus of control and higher confidence in their ability to identify phishing emails, but also described more rigid email checking habits than did protective stewards. One unexpected finding was that repeat clickers failed to recall an identifier which they were explicitly informed that they would need to later recall, while the protective stewards recalled the identifier without error. Due to the small sample and exploratory nature of this study additional research should seek to confirm whether these findings extrapolate to larger populations.

Keywords: Phishing, Security Awareness, Repeat Clickers, Protective Stewards.

1 Repeat Clickers and Protective Stewards

1.1 Phishing Susceptibility

Phishing describes an email-based social engineering attack which attempts to manipulate the recipient into downloading malware, unintentionally disclosing credentials, or otherwise taking action that is not in their own (or their organization's) best interest. As the most common tactic that cybercriminals employ against system users, phishing poses a serious security threat to the human attack surface (Hadnagy, 2018; Verizon, 2023).

Establishing the ground truth of online social engineering susceptibility can be extremely difficult (if not impossible) because cyber threat actors often undertake significant measures to conceal their presence on a network. To counter the phishing threat, many organizations have incorporated simulated phishing email attacks as a part of their security awareness training activities (Greene et al., 2018; Steves et al., 2019). Examples of currently available commercial off the shelf (COTS) phishing simulation platforms are PhishMe (now Cofense), Wombat Security Awareness, and KnowBe4.

While this form of training is very realistic and can be an effective way to prepare users to avoid real phishing attacks (Carella et al., 2017), it also provides researchers with a rich data source because they record several user actions under realistic conditions. These simulated phishing campaigns are likely to be effective proxies for studying real-world phishing attacks because users are not typically warned about an impending email campaign, and the simulated phishing emails often closely mimic actual attacks. In fact, simulated phishing emails are sometimes ‘de-fanged’ versions of real-world attacks. By analyzing simulated phishing datasets, the research community can build a better understanding of user susceptibility patterns.

Phishing simulation software often provides four types of high-level behavioral metrics for each employee’s actions during each phishing campaign; (1) clicking on an embedded hyperlink, (2) replying to the address from which an email originated, (3) entering data after a recipient clicked on the hyperlink, and/or (4) reporting the email the information security department as a suspected phishing attack (Canham et al., 2021). A campaign *failure* is often defined as occurring when an employee performs one or more of the first three actions. Conversely, an employee might report the email as suspicious (without taking the first three actions) and thus providing a protective shield for their organizations against such attacks. There is also the possibility that an employee may both commit a potentially dangerous action *and* then also report that same suspicious email to security staff.

1.2 Repeat Clickers and Protective Stewards

Empirical studies suggest that individuals might be differentially susceptible to phishing (Canham et al., 2019; Canham et al., 2021). Previous work examining repeated interactions between employees and simulated phishing emails, over the course of 20 separate email campaigns, reveals substantial differences in susceptibility patterns (see Figure 1). This work revealed that approximately half (51%) of all employees who were sent simulated phishing emails never failed a single simulated campaign, while a little less than half (44%) failed between one to three simulated phishing emails (i.e., occasional clickers) out of twenty. Finally, a small segment of employees (approximately 6%) fell prey to four or more of the 20 phishing simulations. If each individual simulation campaign failure is counted as a separate event, then the occasional clickers (again 1-3 failures) account for a total of 71% of the total simulation failures, while the ‘repeat clickers’ (>3 failures) account for 29% of the total clicks. It is also noteworthy that three employees failed 12 of 20 campaigns during the one-year period, illustrating the seriousness of this security exposure. Taking the ratios of these numbers, we may create a ‘risk factor’ for each group. The occasional clickers account for approximately 44%

of the employee population yet account for approximately 71% of the total simulation failures, leading to a risk factor of 1.62. More surprisingly, while repeat clickers account for approximately 6% of the population, they tallied approximately 29% of the total failures, leading to a risk score of 4.84. These calculations suggest that repeat clickers present nearly three times more risk to the organization's social engineering attack exposure than occasional clickers (Canham et al., 2021), demonstrating the importance for the security community to better understand the repeat clicking phenomenon.

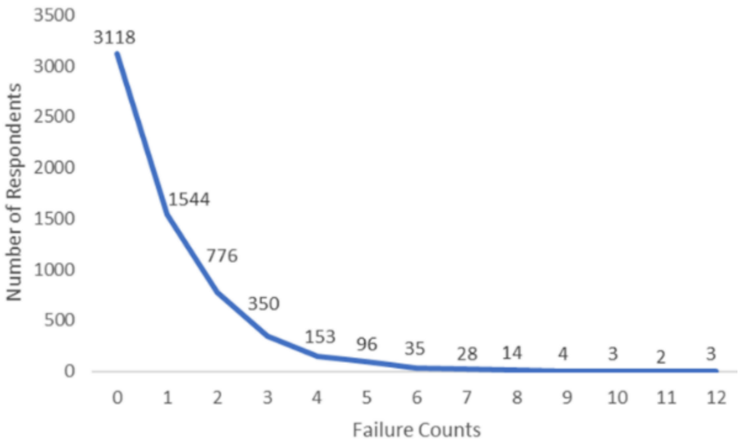

Fig. 1. Distribution of employees by phishing simulation failure counts. (Adapted from Canham et al, 2021).

By contrast, employees who never fail simulated phishing emails, but do report multiple campaigns, are termed protective stewards. Protective stewards provide an enhancement to their organization's security posture by providing an early warning system, alerting their security departments of ongoing social engineering attacks targeting employees. Figure 2 depicts the distribution of employees who did not fail a single phishing simulation. Note that the majority of employees (1,550) did not report nor fail any phishing campaigns, 250 employees reported one simulated campaign, and 6 employees reported 20 of 20 phishing campaigns over the course of the year. In contrast to the 'risk factor' presented by repeat clickers, it is also possible to calculate a 'security enhancement' factor for protective stewards (who never failed any phishing simulations). For example, the occasional reporters comprised approximately 17% of the employee population, and reported approximately 8% of the total reported emails, resulting in a security enhancement factor of 0.47. The protective stewards (employees who reported four or more campaigns) accounted for approximately 92% of the total reported simulation campaigns while only accounting for 33% of the employees who never clicked a simulated phishing email, results in a security enhancement factor of 2.79, approximately five times higher than the occasional reporters.

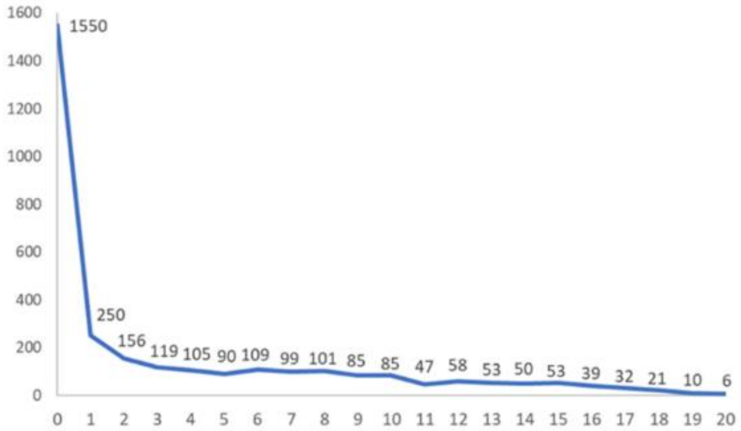

Fig. 2. Distribution of employees by phishing simulation report counts. (Adapted from Canham et al, 2021).

1.3 Research on Repeated Victimization

Other research has uncovered similar patterns. For example, (Li et al., 2020) found that the best predictor of phishing susceptibility was having previously fallen prey to a phishing email. Another study supported these findings in observing that "a small number of employees… (fell) for phishing emails multiple times" (Lain et al., 2022, p. 8). At least two studies have found a tendency for a small number of cybercrime victims to be repeat victims, accounting for a disproportionate number of victimization. One study which analyzed data produced by the Office for National Statistics (ONS), based on the Crime Survey for England and Wales (CSEW), found that repeat cybercrime victims accounted for approximately twice the number of reported cybercrimes than one-time victims (Correia, 2020). Another study found that 45% of cyber-fraud victims were repeat victims (Whitty, 2019). When combined, these findings suggest that such repeat victim susceptibility extends beyond the limits of phishing.

A limitation of this earlier study (Canham et al, 2021) was that it did not provide insight into *why* the sub-groups of repeat clickers and protective stewards emerge or address the root causes of behaviors. One study that explored causal factors found three clicking patterns which they dubbed 'all-clickers', 'non-clickers', and 'everyone else'. The researchers were unable to modify persistent behaviors even after implementing a training intervention (Caputo et al., 2013). Follow-up interviews indicated that the two most common reasons provided by the all-clickers for falling for phishing emails were "an interest in the subject matter and lack of careful attention" (Caputo et al., 2013, p. 35). For example, users would often state that "if an email looked interesting, they would click a link without thinking". Importantly, most had no memory of identifying anything suspicious in the emails. Similarly, the non-clicker group also had no clear memory for the simulated phishing emails and indicated that they "probably deleted the emails immediately without reading them", and that their default behavior was to conduct their own web searches and generally did not click on links in email messages

(Caputo et al., 2013, p. 35). These responses suggest that these two patterns of behavior might default to habituated responses to email, rather than being driven by security knowledge. As elaborated on later, these interaction patterns align with the findings of the current study.

Theoretical Perspectives. As described in previous work, five categories of theories are emerging to provide potential explanations for repeat clicker behavior (Canham et al., 2019). These five categories Social Influence Techniques, Situational Factors, Cultural Influences, Individual Differences, and finally hybrid theories (Canham et al., 2019). Theories emphasizing the impact of social influence techniques suggest that repeat clickers may be especially susceptible to such methods (Workman, 2008). Theories focused on situational factors emphasize transitory factors such as workload and other environmental or situations such as distraction or time pressure (Greene et al., 2018; Hassold, 2018). Theories focusing on the influence of culture on phishing susceptibility, account for the broader influence that sociological factors can have on attitudes and behavior (Butavicius et al., 2016; Posey & Canham, 2018); however, because repeat clicking behavior appears to only afflict a small portion of user populations, it seems unlikely that this behavior is being driven by cultural influences. Theories focusing on individual differences have examined the influence of individual level factors on phishing susceptibility such as personality traits, expertise, and other individual differences (Halevi et al., 2015; Lawson et al., 2017; Pattinson et al., 2012; Sackett & Walmsley, 2014; Sudzina & Pavlicek, 2017, 2020; Uebelacker & Quiel, 2014; Welk et al., 2015; Zhao & Smillie, 2015). Repeat clicking behavior will most likely involve an explanation drawing from an interaction between individual traits and social influence techniques, or situational factors, or a combination of the three of these factors, and thus hybrid theories (Harrison et al., 2016; Uebelacker & Quiel, 2014; Williams et al., 2017) are the most promising potential explanation of factors driving the repeat clicking phenomenon.

Current Study. As this review demonstrates, a coherent theoretical framework for repeat clicking behavior remains elusive. With the objective of gaining insight into the causes of repeat clicking behavior, this study recruited volunteers selected from the study described in (Canham et al., 2021) to participate in interview sessions with researchers. Because there is currently very little understanding for the causal factors relating to repeated victimization in cybercrime victims (Correia, 2020), the current study was exploratory in nature and thus relied heavily on qualitative data collection.

2 Method

2.1 Participants

After the study protocol was reviewed and approved by the university human subjects review board, six employees from the organization studied in (Canham et al., 2021) were recruited to participate in a follow up interview. Three of these employees were from the repeat clickers group and three were from the protective stewards group. Both groups of volunteers were recruited from their respective distribution tails by virtue of committing eight or more actions relative to their category. For example, the recruited repeat clickers had all failed a minimum of eight simulated campaigns, and the protective stewards had all reported a minimum of eight simulated campaigns (without a single failure), in the previous one-year period. Volunteers were notified that they were being invited to participate because of their performance in the simulated phishing trainings, but they were not informed from which group (repeat clickers or protective stewards) that they were being sampled. Study volunteers were compensated $50 US for an approximately one-hour interview, and the completion of a short online survey which required approximately 15 minutes to complete.

2.2 Procedure

Online Surveys. After providing informed consent, the volunteers completed an online survey which assessed their anxiety in using the Internet, confidence in detecting phishing emails, and whether they had been previous victims of online fraud. The scales used included Internet Anxiety (Joiner et al., 2007), Phishing Confidence (Canham et al, in development), Need for Cognition (Cacioppo & Petty, 1982), Curiosity (Collins et al., 2004), Tolerance for Ambiguity (Herman et al., 2010), Risk Taking Index (Nicholson et al., 2005), Risk Avoidance (Tellegen, 1995), Distrust (Tellegen, 1995), and Locus of Control (Levenson, 1981). At the conclusion of this online survey, volunteers were asked to enter a “code word” which would later be used to connect their answers to the interview, as a means of minimizing the chances for identification of the collected data.

Interviews. The interviews were conducted in person either in a lab, or in a quiet conference room at the employee’s place of work. The interviews followed a semi-structured format with a prepared list of questions which the interviews loosely followed, with the latitude of pursuing interesting conversational tangents as encountered. Six categories of questions (listed below) were adapted from (Conway et al., 2017). The six question categories included: Techniques and Strategies (analyzing email, links, domain, sender, etc.), Actions in Response to suspicious email (clicking, downloading, opening, forwarding), Perceived Technological Prowess (self-assessed expertise or knowledge), Phishing Simulations (performance and actions taken), and Workload and Email Habits (variation and amount of workload, and how email is managed).

3 Results

3.1 Online Surveys

Due to the small sample size, no statistical tests were performed to compare the mean scores between the repeat clickers and protective stewards; however, the mean scores for the two groups are included in the table below for review. It is interesting to note that the repeat clickers reported higher scores on the Internet Anxiety, Phishing Confidence, Need for Cognition, Tolerance for Ambiguity, and Locus of Control scales, while reporting lower scores on the Curiosity, Risk Avoidance, and Distrust scales. Mean scores on the Risk-Taking Index were nearly identical. It is also noteworthy that all three of the repeat clickers reported using a desktop computer as their primary means of accessing online resources, while all three of the protective stewards reported using a mobile device (either a laptop or cell phone), as their primary device.

Table 1. Mean scores for Repeat Clickers and Protective Stewards in online surveys.

Scale	Repeat Clickers	Protective Stewards
Internet Anxiety	1.8	1.0
Phishing Confidence	3.0	2.0
Need For Cognition	2.5	1.8
Curiosity	2.6	2.9
Tolerance For Ambiguity	3.2	2.9
Risk Taking Index	1.5	1.6
Risk Avoidance	1.7	2.3
Distrust	2.8	4.2
Locus Of Control	2.4	1.7

Table 2. Mean number of hours reported in response to the question
"How many hours per week do you do the following online?

Activity	Repeat Clickers	Protective Stewards
Shopping	0.3	3.7
Social Media	13.7	8.7
Email	15.0	9.3
Watching Videos	1.7	4.0
Gaming	0.0	0.0
Work	31.0	34.0
School Work	1.7	0.0

In addition to the scales scores summarized in Table 1, the volunteers were specifically asked about prior online fraud victimization and methods for detecting phishing emails.

Table 3. Online Question: Have you ever been the victim of online fraud before?

Number	Repeat Clickers	Protective Stewards
1	Definitely yes	Probably not but not sure
2	Definitely yes	Definitely not
3	Definitely not	Probably not but not sure

Table 4. Online Question: How are you able to detect whether an email is a phishing scam?

Number	Repeat Clickers	Protective Stewards
1	Common sense	Unusual sender's email address; frequent typos and grammatical errors; suspicious requests for money or favors.
2	By the format of the email and the content or misspelling.	Senders email address
3	From what I have read and learn what to look for.	I check the sender's email address. I make sure the email makes sense and follows the organization's policies. For instance, I know it's a phishing scam if my bank emails me asking for my personal information because this is against their policy.

3.2 Interview Responses

Interviews spanned approximately one hour for each session and while including a full transcript is beyond the scope of this work, representative sample excerpts are included here for each topic category. The sample responses are listed for each volunteer (number 1, 2, or 3), within each group (Repeat Clickers or Protective Stewards). Example questions are included in the bullet point items below each topic category heading.

Techniques and Strategies (analyzing email, links, domain, sender, etc.).

- How would you spot an email that came from outside the organization or outside of your area?
- What would you do, step by step, if you got a suspicious email?
- What are the characteristics of a phishing email?

Table 5. Exemplar responses to Techniques and Strategies questions.

Number	Repeat Clicker	Protective Steward
1	I really don’t click on the link because I worry about it, it’s like a virus. Especially when I receive a [WORK] email—first of all I look at it, “Where does it come from?” Make sure it’s	I just think if it doesn’t look like any of the other emails I received, it just looks a little different, then I check the (report) button.

	[ORGANIZATION’S EMAIL REDACTED], that means it’s internal. But if it’s from an outsider, like a Gmail, Hotmail, other things, I always think “maybe it’s other people scam.” And if they have a link, I don’t open that-- it’s a test alert. I send that to the IT department.	
2	maybe like... like misspelling, I notice just like some phishing emails have a misspelling in them or the font can be different in one part of an email vs another part.	if the email address looks funky or it’s just like a weird request for a favor or money. Something like that. Or if just it’s like, kind of an erratic message with weird grammar and spelling—like umm this doesn’t seem right.
3	I would (check) the email itself, it tells you where it’s from, if it’s coming from Google, from a Gmail, wherever.	It’s quite a few things that could be suspicious. For one, any email from someone that is asking for something that normally isn’t my job. I think that one of the examples that I reported was someone asking me to buy gift cards or something.

Actions in Response to suspicious email (clicking, downloading, opening, forwarding).

- What do you do if you receive a suspicious email? (Hover over links, etc.)
- When you get an email, just any type of email, and it has a link in it, what do you think about when you think about clicking that link?

Table 6. Exemplar responses to Actions in Response to suspicious email questions.

Number	Repeat Clickers	Protective Stewards
1	I review, look at it, print out the paperwork, ask my friend, I say, “Hey, do you think this is real or what?” My friend says, “This looks like it’s real because a [ORGANIZATION’S EMAIL DOMAIN REDACTED]” Then I take it to my assistant director, I say, “First I wanna ask your opinion if it’s real or not.” He said, “Yeah, it’s real.”	I check the (report) button. Whether someone else is actually gonna look at it, I don’t know.

2	when I get those e-mails, I send it, to CERT (information security department). But like some of them look just like very legitimate... There's a button on the right-hand side of the e-mail that says report to CERT, and I just click it and it gets sent to CERT.	We have a small IT department here. I'd probably just got to our Help Desk person first and they can take it up the chain.
3	one of the things I pride myself on is I send it to my ISAT (information security) group, they send it back say, "This is a phishing" and then I pass on to anybody else. If it they don't look right I send it to them and let them get back to me.	part of the [ORGANIZATION REDACTED]'s process is when someone does report it, if IT looks at it and says, "This really is a phishing," they'll send out an email to the foundation saying, "Hey, just an FYI, we're getting hit with this. If you get this email, don't click on it." They'll kinda tell you either delete it or "Let us know that you received it," or something.

Perceived Technological Prowess (self-assessed expertise or knowledge).

- How would you describe your knowledge level in terms of being able to use computers or information technology?

Table 7. Exemplar responses to Perceived Technological Prowess questions.

Number	Repeat Clickers	Protective Stewards
1	No (training). But I think it's common sense.	I'm Microsoft certified in databases.
2	It was like a very long time ago like freshman year... I think one of them is programming because it was in [WORK SITE]. So, I think it was like something with keyboarding. And then another one was like programming, I think. So very basic.	I just did the Credit Card training and there might've been something similar like that for the Phishing training. Like an online, PowerPoint, click through thing. But I don't recall, that was a while ago.
3	I know how to function. Especially… online courses, I know all the pushes and buttons. It's just like my iPhone. My daughter uses... sometimes she has to teach me.	(it)'s always been second nature-- I came from the department of revenue before this. And they had very strict policies on like, locking your computer screen and having a clean desk policy.

Phishing Simulations.

- Do you get any feedback from the (phish alert button) when you clicked it?
- Can you tell me about anything that you remember about reporting any of the emails that you reported?

Table 8. Exemplar responses to Phishing Simulations questions.

Number	Repeat Clickers	Protective Stewards
1	I don’t think so. Usually— if... HR send over a training, yes, but if a scammer, no.	I noticed that... you still get that email that says, “Thank you for reporting.” So, the message will pop up.
2	Yeah. Well, saw like the oops page. Maybe like a couple, say, like three, two to three.	they all seem to be the simulated ones. I always seem to get that message that says, “Congratulations you detected a scam” or whatever. I can’t recall one that I would’ve reported, that said anything else.
3	I have one time. Matter of fact something happened, and you guys might check periodically.	Well, the one’s that I have reported have all been a part of the program. And it was immediate, as soon as you sent it, you get what the button says but as soon as you sent it over, it was an immediate: “Good job, this is a part of the program.” So, it was an immediate response.

Workload.

- Regarding the amount of email that you get; how much would you say that your overall workload will fluctuate?
- Do you normally only check your work email at work?
- Do you ever feel stressed/overwhelmed at work?

Table 9. Exemplar responses to Workload questions.

Number	Repeat Clickers	Protective Stewards
1	Usually—to me I’m always busy. Because I do accounting and finance, I’m always busy. I have to do the internal things, people who have trouble, purchasing. I have to review and then look at the budget, approve, the people using the P card, I have to review and make sure the P card is right.	we’re constantly overwhelmed, constantly with eyes burning from too much screen time. We’re very behind on everything.
2	It can be it just depends on the day. Like how busy it is. Overall, I feel like I can, but if it's like very busy with [CLIENTS] nonstop, which happens sometimes, my work might go into the next day.	I knew other people in the team that are [overwhelmed] on a constant basis, but for me, I haven’t. It’s usually just the clients-- the internal clients that I’m working on—actively working on their tickets. So, it’s only a handful of tickets at a time. And as I closed them out, I’ll open up more. But it’s usually just the same people.

3	(My workload fluctuates) a lot now.	Most days are pretty steady, I would say, for me. In my current position. This is my third position since I’ve been here. So when there’s a big project, you can be overwhelmed pretty quickly. But otherwise, it’s kinda less, I guess.

Email Habits.

- Do you regularly check email outside of working hours (Nights/Weekends)?
- Which device(s) do you use when checking email?

Table 10. Exemplar responses to Email Habits or Workflow Habits questions.

Number	Repeat Clickers	Protective Stewards
1	90% is on the office. 2% would be at home. *Author acknowledges that this does not add to 100%, this was the subject's response.	Yes
2	mobile would be like 10 percent... more so weekends.	Yes. Probably 90/10 on the laptop.
3	when I leave work Friday after I check my email that is my day. Okay. I turn my computer back on Sunday to look at my things to do list, but I still check my email.	90% of the time is definitely on the PC. And then 10%... on the cell phone. *Phones were used for checking email during off hours.

4 Discussion

One of the most interesting, and unexpected findings of this study was not directly related to the explicit data collection. Upon completion of the online survey portion of the study, the final question asked volunteers to provide a “code word” which would later be used to match their answers to the interview transcripts, for the purpose of minimizing the likelihood of revealing the identity of volunteers. Volunteers were explicitly instructed that they would need to later provide this “code word” to the interviewers and that they should choose something that they would easily recall. All participants from the protective stewards group accurately recalled their code word, and all the repeat clickers failed to recall their code word. The research team was still able to match online responses to the interviews based on the timing of each.

4.1 Analysis of Online Survey Responses

While scores from the online surveys were not statistically compared between the groups due to the small sample sizes investigated, some of the differences are noteworthy. For example, repeat clickers reported higher confidence in their ability to detect phishing emails, which is consistent with some studies which have found that unjustified high levels of confidence are related to increased susceptibility to phishing. In particular, that study's findings indicate that "overclaimers", people who grossly overestimate their phishing detection ability, are more vulnerable than other individuals (Jones, 2023). It is also worth drawing attention to the higher level of anxiety reported by repeat clickers when accessing online services. It is unclear why this discrepancy exists, but higher levels of internet anxiety might be due to prior victimization. Two of the three repeat clickers reported previously being victimized by online fraud.

In considering the number of hours spent online conducting various activities, protective stewards reported spending approximately 12 times more time shopping online, and twice as much time watching videos, than did the repeat clickers. In contrast, the repeat clickers spent almost twice as much time on social media and email compared to protective stewards. Additional research should examine whether these findings extend to larger samples, but these insights to point toward additional research efforts which might focus on non-email usage behaviors that might predict, or help explain, repeat clicker behavior patterns.

The differences in the mean scores on the Need for Cognition, Curiosity, Tolerance for Ambiguity, Risk Taking Index, and Risk Avoidance scales should be treated cautiously because of the small sample sizes involved. Additional research and theoretical support will make the findings related to the Distrust and Locus of Control scales more interesting.

The Distrust Scale (Tellegen, 1995) assesses the subject's propensity to distrust or be suspicious of others, "I suspect hidden motives in others" being an example item. Several research studies on susceptibility to phishing point toward suspicion as being a major factor in susceptibility (Vishwanath, 2022). The higher levels of distrust reported by the protective stewards may be an indication of higher suspicion levels in this population of users and this is something which should be explored in more depth in future research.

The higher Locus of Control scores among repeat clickers indicates that this group feels more in control of their own destiny and ability to improve performance than the protective stewards. This finding is somewhat puzzling and deserves more exploration. Other studies have found that individuals with a high locus of control were more likely to be the victims of cyber-scams (Whitty, 2019). The findings of this study agree with those findings as well as the findings of an associated study (Canham et al, under review). These findings also deserve more research focus. A potential explanation is that there is a relationship between an internally oriented locus of control and a higher level of confidence for detecting phishing emails, and this commonality might be driving the repeat clicker behavior pattern.

4.2 Analysis of Interview Responses

Phishing Simulation Training. None of the interviewees initially admitted to clicking the embedded hyperlinks in the simulated phishing emails. It should be noted that the KnowBe4 phishing simulation platform used in the initial study (Canham et al., 2021) provided immediate feedback in the form of an "oops" landing page which advised an employee that they had fallen prey to a simulated phishing email and provided an explanation for indicators they could have used to identify the email as a potential phish. It is unknown whether this reluctance was motivated by a desire for prosocial responding, embarrassment, a lack of memory, or a combination of these factors. However, when coaxed, all of repeat clickers admitted to clicking the links in "one or two" emails, none reported clicking the hyperlinks in more than three emails. Recall that all the volunteers from this group had clicked eight or more hyperlinks. This point deserves more attention because there is reason to believe that memory might be a factor in this reluctance to account for clicking more hyperlinks.

While this is currently speculative, the lack of recalling falling prey to simulated phishing emails and the inability to recall their own "code words" is suggestive of a common cognitive factor driving both observed results. Considering that previous research studies also found that neither habitual clickers nor habitual non-clickers recalled clicking the links within simulated phishing emails (or ignoring them), suggests that both groups are handling potential phishing emails through automated cognitive processes (Caputo et al., 2013). If these findings replicate in future studies, it could have significant implications for security awareness training. For example, for repeat clickers, training which reinforces automatic processes may be more successful than training regimens which exclusively focus on security awareness or knowledge.

An interesting finding from the protective stewards group was that they seemed to identify the simulated phishing tests as coming from the information security department and acknowledged that this was reinforced by the feedback that they received which indicated that the attempt had been a simulation. Security awareness trainers might consider withholding immediate feedback when simulated phishing exercises are correctly identified and reported. In contrast to failed training simulations, providing immediate feedback on reported emails might inadvertently train higher performing employees to identify emails which "look" like training emails, potentially making these employees more susceptible to actual malicious emails. Other studies have found that in fact protective stewards enjoy identifying simulated phishing emails that are very difficult to detect, particularly when this is contextualized within a gamified competition (Canham et al., 2022).

Workload and Email Habits. One potential explanation for the repeated victimization of a subgroup of employees is that this subset is overworked or overloaded and are thus more susceptible to phishing emails due to situational factors (because they are distracted or under a heavier cognitive load). The interviewees from both groups reported high levels of workload with heavy fluctuations, making workload an unlikely explanation for repeat clicking.

There were differences reported in the email habits between the two groups. Even though both groups reported checking email primarily during work hours, repeat clickers reported much higher aversion to checking work email during off hours. One interviewee from the repeat clickers group reported that s/he refused to check email during the weekends. Protective stewards by contrast have much more fluidity in checking work email on or off work hours.

Techniques and Strategies. In describing actions taken to determine whether an email is legitimate, both groups reported looking for similar cues (email domain name, misspelling, odd grammar, or unrelated to job), suggesting that both groups possessed the relevant knowledge required to identify and avoid suspicious email.

Actions in Response to suspicious email. In response to receiving a suspicious email, both groups also reported taking similar actions to report the email to the security department (CERT). One interviewee from the repeat clicker sample reported printing suspicious emails on paper when evaluating them. It was unclear what benefit this was supposed to impart. Both groups appeared to know the suspicious email policy.

Perceived Technological Prowess. There were some interesting differences in the self-assessed technical knowledge between the two groups of interviewees. Technical knowledge in this context referred to information technology knowledge and capability, but not necessarily security related knowledge. All the protective stewards reported having previously received some security related training, with one of the repeat clickers reporting receiving training sometime previously. One of the protective stewards reported being a certified Microsoft database administrator.

5 Conclusion

This work represents one of the first efforts to uncover insights into the factors driving repeat clicker behavior. The exploratory nature of the study and small sample size limit the inferences which can be drawn from findings; however, this study points toward several potentially fruitful lines of future research which should be explored.

Perhaps the most interesting finding of this study was not intentionally sought, but instead discovered accidentally. The inability to recall “code words” by repeat clickers, combined with an inability to recall simulated phishing failures, and rigid email habits are suggestive of an underlying common cognitive factor at play with repeat clickers. A potential reason that repeat clickers have more rigid habits is that they are compensating for a cognitive deficiency that is also contributing to less effective recall. This is something that needs to be explored in future research efforts.

All the volunteers in this study had received some form of limited security awareness training from the organization. All but one of the protective stewards recalled receiving this training, and none of the repeat clickers recalled receiving it. This finding leads to the question of whether the training was effective even though it was not explicitly recalled. Both groups were able to identify multiple indicators of suspicious email messages, and so it is likely that some of the lessons from the training were retained. This knowledge withstanding, the protective stewards unquestionably had more general technology-related knowledge and were more capable at articulating technically related concepts than the repeat clickers.

Future research should also seek to understand the relationship between higher internal locus of control and cybercrime susceptibility. The findings of this study are consistent with those of (Whitty, 2019) and another unpublished study. It is unclear whether there is a relationship between more internally oriented locus of control and higher reported confidence in phishing detection, but this warrants additional exploration. The organization participating in the study requested that age not be collected from the volunteers, so it is unknown whether this is a contributing factor to these findings.

The termination of employees in this category is not always feasible; therefore, it is critical to better understand the causal factors for repeat clicking behavior in to enable security professionals to effectively address this critical security risk.

6 Acknowledgements

The author wishes to thank Dr. Clay Posey, Michael Constantino, Dr. Shanee Dawkins, and Alexandra Figueroa for their assistance in collecting and analyzing the data for this study. The author also wishes to acknowledge the support of the National Institute of Standards and Technology (NIST) under Financial Assistance Award Number: 60NANB19D123. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of NIST or the U.S. Government.

7 References

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. *ArXiv:1606.00887 [Cs]*. http://arxiv.org/abs/1606.00887

Cacioppo, J. T., & Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology*, *42*(1), 116–131. https://doi.org/10.1037/0022-3514.42.1.116

Canham, M., Fiore, S. M., Constantino, M., Caulkins, B., & Reinerman-Jones, L. (2019). *The Enduring Mystery of the Repeat Clickers*.

Canham, M., Posey, C., & Constantino, M. (2022). Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks. *Frontiers in Education*, *6*. https://www.frontiersin.org/articles/10.3389/feduc.2021.807277

Canham, M., Posey, C., Strickland, D., & Constantino, M. (2021). Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards. *SAGE Open*, *11*(1), 215824402199065. https://doi.org/10.1177/2158244021990656

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security Privacy*, *12*(1), 28–38. https://doi.org/10.1109/MSP.2013.106

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *2017 IEEE International Conference on Big Data (Big Data)*, 4458–4466. https://doi.org/10.1109/BigData.2017.8258485

Collins, R. P., Litman, J. A., & Spielberger, C. D. (2004). The measurement of perceptual curiosity. *Personality and Individual Differences*, *36*(5), 1127–1141. https://doi.org/10.1016/S0191-8869(03)00205-8

Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S., & Chen, F. (2017). *A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing*. 115–129. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/conway

Correia, S. G. (2020). Patterns of online repeat victimisation and implications for crime prevention. *2020 APWG Symposium on Electronic Crime Research (ECrime)*, 1–11. https://doi.org/10.1109/eCrime51433.2020.9493258

Greene, K., Steves, M., Theofanos, M., & Kostick, J. (2018). User Context: An Explanatory Variable in Phishing Susceptibility. *Proceedings 2018 Workshop on Usable Security*. Workshop on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2018.23016

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (1st ed.). Wiley. https://doi.org/10.1002/9781119433729

Halevi, T., Memon, N., & Nov, O. (2015). *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks* (SSRN Scholarly Paper ID 2544742). Social Science Research Network. https://doi.org/10.2139/ssrn.2544742

Harrison, B., Vishwanath, A., & Rao, R. (2016). A User-Centered Approach to Phishing Susceptibility: The Role of a Suspicious Personality in Protecting Against Phishing. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5628–5634. https://doi.org/10.1109/HICSS.2016.696

Hassold, C. (2018). Life After Phishing: What's Next? *InfoSec World 2018*. InfoSec World 2018, Orlando, FLl USA.

Herman, J. L., Stevens, M. J., Bird, A., Mendenhall, M., & Oddou, G. (2010). The Tolerance for Ambiguity Scale: Towards a more refined measure for international management research. *International Journal of Intercultural Relations*, *34*(1), 58–65. https://doi.org/10.1016/j.ijintrel.2009.09.004

Joiner, R., Brosnan, M., Duffield, J., Gavin, J., & Maras, P. (2007). The relationship between Internet identification, Internet anxiety and Internet use. *Computers in Human Behavior*, *23*(3), 1408–1420. https://doi.org/10.1016/j.chb.2005.03.002

Jones, D. (2023). *Protecting the overclaimers in cybersecurity w/ Dr. Daniel N. Jones | CSI Talks #7*. https://www.youtube.com/watch?v=lsly2Q_74V4

Lain, D., Kostiainen, K., & Čapkun, S. (2022). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. *2022 IEEE Symposium on Security and Privacy (SP)*, 842–859. https://doi.org/10.1109/SP46214.2022.9833766

Lawson, P., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *61*(1), 1331–1333. https://doi.org/10.1177/1541931213601815

Levenson, H. (1981). Differentiating Among Internality, Powerful Others, and Chance. In H. M. Lefcourt (Ed.), *Research with the Locus of Control Construct* (pp. 1–15). Academic Press.

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020, January 7). *Experimental Investigation of Demographic Factors Related to Phishing Susceptibility*. https://doi.org/10.24251/HICSS.2020.274

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research*, *8*(2), 157–176. https://doi.org/10.1080/1366987032000123856

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18–28. https://doi.org/10.1108/09685221211219173

Posey, C., & Canham, M. (2018). A Computational Social Science Approach To Examine The Duality Between Productivity And Cybersecurity Policy Compliance Within Organizations. *2018 International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction and Behavior Representation in Modeling and Simulation, BRiMS 2018*. https://stars.library.ucf.edu/scopus2015/7904

Sackett, P. R., & Walmsley, P. T. (2014). Which Personality Attributes Are Most Important in the Workplace? *Perspectives on Psychological Science*, *9*(5), 538–551. https://doi.org/10.1177/1745691614543972

Steves, M. P., Greene, K. K., & Theofanos, M. F. (2019). A Phish Scale: Rating Human Phishing Message Detection Difficulty. *Proceedings 2019 Workshop on Usable Security*. Workshop on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2019.23028

Sudzina, F., & Pavlicek, A. (2017). Propensity to Click on Suspicious Links: Impact of Gender, of Age, and of Personality Traits. *Digital Transformation – From Connecting Things to Transforming Our Lives*, 593–601. https://doi.org/10.18690/978-961-286-043-1.41

Sudzina, F., & Pavlicek, A. (2020). Virtual Offenses: Role of Demographic Factors and Personality Traits. *Information*, *11*(4), 188.

Tellegen, A. (1995). *Multidimensional personality questionnaire-276 (MPQ-276) test booklet* (1st ed., Vol. 1). University of Minnesota Press.

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 24–30. https://doi.org/10.1109/STAST.2014.12

Verizon. (2023). *2023 Data Breach Investigations Report (DBIR)*. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

Vishwanath, A. (2022). *The weakest link: How to diagnose, detect, and defend users from phishing*. The MIT Press.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the “Phisher-Men” Reel You In?: Assessing Individual Differences in a Phishing Detection Task. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, *5*(4), 1–17. https://doi.org/10.4018/IJCBPL.2015100101

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Workman, M. (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*(4), 662–674. https://doi.org/10.1002/asi.20779

Zhao, K., & Smillie, L. D. (2015). The Role of Interpersonal Traits in Social Decision Making: Exploring Sources of Behavioral Heterogeneity in Economic Games. *Personality and Social Psychology Review*, *19*(3), 277–302. https://doi.org/10.1177/1088868314553709