KSU Proceedings on Cybersecurity Education, Research and Practice

2020 KSU Conference on Cybersecurity Education, Research and Practice

Oct 23rd, 2:00 PM - 2:30 PM

Towards an Assessment of Pause Periods on User Habituation in Mitigation of Phishing Attacks

Amy Antonucci
Nova Southeastern University, aa2539@mynsu.nova.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Martha Snyder
Nova Southeastern University, smithmt@nova.edu

Laurie Dringus
Nova Southeastern University, laurie@nova.edu

Antonucci, Amy; Levy, Yair; Snyder, Martha; and Dringus, Laurie, "Towards an Assessment of Pause Periods on User Habituation in Mitigation of Phishing Attacks" (2020). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 2.
https://digitalcommons.kennesaw.edu/ccerp/2020/Research/2

Abstract

Social engineering is the technique in which the attacker sends messages to build a relationship with the victim and convinces the victim to take some actions that lead to significant damages and losses. Industry and law enforcement reports indicate that social engineering incidents costs organizations billions of dollars. Phishing is the most pervasive social engineering attack. While email filtering and warning messages have been implemented for over three decades, organizations are constantly falling for phishing attacks. Prior research indicated that attackers use phishing emails to create an urgency and fear response in their victims causing them to use quick heuristics, which leads to human errors. Humans use two types of decision-making processes: a heuristic decision, which is a quick, instinctual decision-making process known as 'System One', and a second, known as 'System Two,' that is a slow, logical process requiring attention. 'System Two' is often triggered by a pause in the decision-making process. Additionally, timers were found in other research fields (medicine, transportation, etc.) to affect users' judgement and reduce human errors. Therefore, the main goal of this work-in-progress research study is to determine through experimental field study whether requiring email users to pause by displaying a phishing email warning with a timer, has any effect on users falling to simulated phishing attacks. This paper will outline the rationale and the process proposed for the validation of the field experiments with Subject Matter Experts (SMEs). Limitations of the proposed study and recommendation for further research are provided.

Location

Zoom Session 1 (Main Papers Track)

Disciplines

Information Security | Management Information Systems | Technology and Innovation

Comments

Keywords: Cybersecurity, phishing emails, heuristic in cybersecurity, habituation in cybersecurity, phishing email warnings

INTRODUCTION

Phishing and other types of social engineering incidents cost organizations billions of dollars a year (FBI, 2018; Musuva et al., 2019; Salahdine & Kaabouch, 2019; Thomas, 2018). In addition, phishing continues to present a significant threat to users in both their personal and professional lives leading to personal or corporate data as well as significant financial loss (Carlton et al., 2018). Social engineering attacks continue to inflict significant damages to organizations including the recent high-profile attack against Twitter (Iyengar, 2020). The number of phishing email campaigns detected by the Anti-Phishing Working Group (2020) in the first quarter of 2020 was 139,685, up from the previous quarter, and the number of email users worldwide is over 3.8 billion and expected to increase to 4.3 billion by the end of 2022 (Clement, 2019). In 2018, 85% of 1001 respondents to a survey of white-collar workers stated that they use their smartphones to check their email (Clement, 2019).

Attackers use phishing to create a fear or excited response in their victims (Goel et al., 2017; Jain et al., 2016) which causes victims to use a quick, emotional response using heuristics rather than a logical, thought-through response. Even when warned, users choose to put aside security concerns when deciding whether or not to follow links presented in an email (Vance et al., 2018). A possible explanation for this is that users do not properly evaluate the risk involved in clicking on an unknown link, especially when overworked (Bravo-Lillo et al., 2011). Furthermore, users also move to a heuristic process as they become more fatigued (Arazy et al., 2017), and it appears that this is also the case when they are deciding whether a displayed link is safe to follow or not. By requiring the user to pause, the user's thought stream may be interrupted, and the user may be switched to logical thinking. Jensen et al. (2017) suggested that requiring the user to pause will encourage the user to reflect on the content of an email message. Users are likely to engage logical thinking the first time they see a warning (Anderson et al., 2016), but tasks that are repeated appear to be processed using heuristics. This pattern of action often results in an error in judgement regarding the safety of a displayed link (Anderson et al., 2016). Repetitive tasks are recognized by the brain and the effort extended to accomplish these tasks is diminished. Because of the diminished effort put forth by the brain, static warnings lose effectiveness over time (Anderson et al., 2016) and heuristics take over (Kahneman, 2011). Additionally, countdown timers have been found to be effective in different research fields, including medicine (Marto et al., 2016) and in pedestrian crosswalks (Keegan & O'Mahony, 2003). Count-up timers have been used to measure vigilance and appear to be valuable to help reduce human error in other contexts (Lo et al., 2019). However, it appears that very limited attention has been provided to the role of counters and pause levels for users when provided with potentially malicious emails. It is our assumption and the aim of this study to investigate if a countdown or count-up timer will move users from a heuristic, System One thought process to a logical, System Two thought process to reduce clicking on potentially malicious links in emails.

The overarching research problem that this study will address is that users make judgement errors when evaluating the risks involved in clicking on an unknown link in an email. The need for this work is demonstrated by the works of Anderson et al. (2016), who used functional Magnetic Resonance Imaging (fMRI) to demonstrate that users quickly habituate to static warnings, and by Amran et al. (2018) who stated that users will often consider security warnings irrelevant or even try to evade them. This proposed study builds on previous research by Ball et al. (2015) and by Kahneman (2011). Ball et al. (2015) suggested that additional studies are required to understand what factors lead to habit as well as the relationship between habit and practice in the context of information security. They found that awareness of risks was not a significant influence over practice, and rather that habit was a stronger influence. Moreover, little is known on the specific amount of time users should be asked to pause to adjust their habit in the context of phishing emails Therefore, this study is attempting to investigate if requiring the user to pause before taking any actions such as clicking on a link or an attachment will have an impact on the amount of successful phishing emails sent to employees. In this paper we outline the first part of a larger research study in which we focus on validating a proposed set of field experiments by a panel of Subject Matter Experts (SMEs). Specifically, the main research question that this study will address is: According to cybersecurity SMEs, at what level should the countdown or count-up timer be set, as well as what level of functional correctness and validity is sufficient for the proposed set of field experiments? Specifically, the proposed Research Questions (RQs) are:

RQ1. What are the three timer levels to require the user to pause that should be used to assess users' ability to identify malicious links in email according to cybersecurity SMEs?

RQ2. What level of functional correctness and validity of the proposed set of field experiments is sufficient according cybersecurity SMEs?

LITERATURE REVIEW

Social Engineering

Social engineering is one of the most under researched and most effective cybercrimes (Jain et al., 2016). Social engineering is defined as "the art of exploiting the weakest link of information security systems: the people who are using them" (Jain et al., 2016, p. 94). Mihelič et al. (2019) called the human factor in social engineering a lever that is exploited by social engineers. Salahdine and Kaabouch (2019) defined four stages of a social engineering attack: (1) information gathering; (2) hook relationship; (3) play exploitation and execution; as well as (4) out. In the information gathering stage, the social engineer collects information about their target, also known as reconnaissance. In the hook relationship phase, the social engineer baits the victim with fear or excitement (Goel et al., 2017). In the play exploitation and execution phase, the attacker executes the attack, while in the out phase, the attacker leaves with actions taken to remove any traces of the attack.

Technical solutions to combat social engineering typically don't work (Krombholz et al., 2015). Jain et al. (2016) went as far as to say that there are no technical solutions to the problem of social engineering. Prior literature also documented that users are often too confident in their ability to detect a social engineering attack (Krombholz et al., 2015), partially because social engineers are becoming more devious. This means that suggestions for countering social engineering just two years ago don't appear to be useful nowadays. For example, in 2018, Abass gave the advice to look for the Hyper Text Transfer Protocol Secure (HTTPS) in a Universal Resource Locator (URL) within suspected phishing emails, but in 2020, the Anti-Phishing Working Group advised not to rely on presence of the HTTPS protocol since up to 75% of attackers now use websites that includes the HTTPS protocol (Anti-Phishing Working Group, 2020).

While phishing is only one of 20 different kinds of social engineering defined by Salahdine and Kaabouch (2019), it is the most common type of social engineering attack. Salahdine and Kaabouch (2019) organized phishing attacks into five categories: spear, whaling, vishing, interactive voice response, and Business Email Compromise (BEC). A spear phishing attack is one in which the attacker targets a particular group of people, such as employees of a particular company or users of a particular website (Krombholz et al., 2015). A whaling attack is a subset of a spear phishing attack in which the high-profile members of the target group are targeted (Krombholz et al., 2015). A vishing attack is a phone attack in which the attacker convinces the victim to give up some piece of confidential information, and an interactive voice response attack is a subset of a vishing attack in which the attacker pretends to be an interactive voice-controlled computer (Salahdine & Kaabouch, 2019). A BEC attack is one in which the attacker pretends to be a high-ranking member of the victim's organization and asks for a secure transaction, such as a wire transfer of funds. When the victim completes the transfer, the funds are wired to the attacker's account instead of a legitimate customer or vendor's account (Salahdine & Kaabouch, 2019).

Thompson (2012) stated that many attacks start with a bad user decision or a result of human error, while anyone can be tricked by a phishing attack. Many attackers use what users know against them. For instance, many phishing emails warn the reader not to click on any links, but instead go to a website and download a document (Thompson, 2012). Attackers count on users taking into account only static information about what they have learned on phishing and not to think critically about the actions they are being asked to do (Thompson, 2012). Moreover, human error as a result of not paying close attention or being in a distracted environment may cause users further to fall for phishing attacks (Jensen et al., 2017).

A number of studies used university communities (students, staff, faculty, & surrounding communities) as participants for their research which may limit somewhat the validity of their results for the typical organizational employee at a business or government entity when it comes to phishing (Brustoloni & Villamarín-Salomón, 2007; Goel et al., 2017; Jensen et al., 2017; Musuva et al., 2019). Goel et al. (2017) used third- and fourth-year undergraduate students as participants in their study, while Jensen et al. (2017) and Musuva et al. (2019) used students, faculty, and staff as their study participants. Brustoloni and Villamarín-Salomón (2007) uses the entire university community as their participants.

Finn and Jakobsson (2007) categorized phishing studies into three groups: survey, closed-lab experiment, and simulations. A survey study presents the participants with a survey asking what their reaction to an event would be. Bravo-Lillo et al. (2011) used an interview survey to understand perception of risk of a chosen action. A closed-lab experiment is one in which participants are aware of the focus of the study, and, therefore, the results may be somewhat skewed (Finn & Jakobsson, 2007). An example of a closed-lab experiment is Algarni et al. (2017)'s study, where they used a role-play questionnaire in which participants were shown Facebook profiles and then asked about the trustworthiness of those profiles, Algarni et al. (2017) acknowledged that participant reaction may be skewed because the participants were aware of the study.

The third kind of study according to Finn and Jakobsson (2007) is a simulation study in which the research design mimics a real-world scenario. Finn and Jakobsson (2007) discussed ethical considerations with regards to simulation studies. Simulation studies seem to be the most widely used of the three types of studies, as they have been used to understand phishing behavior (Burns et al., 2019; Goel et al., 2017; Gordon et al., 2019). Musuva et al. (2019) used a simulation study which had to be curtailed because a social media activist sent out an alert regarding the phishes in the investigation which caused the university to end the study. Musuva et al. (2019) stated that the viral nature of the alert and the alert itself illustrates the power of vigilant and informed users.

Heuristics

Kahneman (2011) introduced the concepts of System One and System Two as methods of describing human cognition. System One represents an instinctual thought process that comes quickly and automatically and requires little or no effort. Examples of System One are the ability to orient to a sudden sound or to detect if one object is closer than another (Kahneman, 2011). System Two is a slow, methodical thought process that requires deliberate effort. Examples of System Two are solving a complex mathematical equation or monitoring one's behavior in a social situation (Kahneman, 2011). For typical, daily activities, System One is active, and System Two is in a low-effort mode. When System One encounters a more difficult task, it activates System Two. As a difficult task becomes more familiar, System One is able to take over the task. Kahneman (2011) stated that, given multiple ways to solve a problem, people will typically choose the path that requires the least amount of effort. As an illustration, he referenced a study in which college students were asked to solve a simple mathematical problem with an intuitive answer that was incorrect. They indicated that the students did not check their work, although checking their work would have been easy to do. Kahneman (2011) also stated that task-switching is difficult, but that System Two can program the memory to override habit.

Tversky and Kahneman (1974) introduced the idea of a heuristic decision-making process that does not follow Bayesian probability. Kahneman (2011) describes a heuristic as an assumption made to simplify a decision. According to Tversky and Kahneman (1974), if Bayesian probability were used, there would be evidence of using prior probabilities when making a decision. They referenced a study in which participants were given a description of a person in a group and asked if they thought that that person was a librarian or an engineer. In the study, some participants were told that there were more engineers than librarians in the group, and some were told that there were more librarians than engineers in the group. The result was that only the description of the person affected the participant's decision. Tversky and Kahneman (1974) explained this departure from Bayesian probability by stating that decision-makers tend to use heuristic, intuitive judgement although that judgement may be wrong.

Gigerenzer (1991) countered Tversky and Kahneman (1974) by arguing that errors in judgement are not violations of probability theory. Gigerenzer (1991) questioned the methods of Tversky and Kahneman (1974), stating that Tversky and Kahneman (1974) used too narrow a definition of norm and too highly selected a sample to be used in traditional probability and statistics. Kahneman and Tversky (1996) answered Gigerenzer (1991), stating that only two of the 12 biases they referenced in 1974 apply to Gigerenzer's argument, and they countered Gigerenzer's claim that judgement heuristics are independent of context. In turn, Gigerenzer (1996) stated that the problem with heuristics is that it can be fit to any situation yet is too vague. Gigerenzer (1996) also countered the number of biases referenced by Kahneman and Tversky (1996), stating that he found thirteen biases and that five apply to his former argument. Vranas (2000) attempted to clear up misunderstandings in the debate between Kahneman and Tversky and Gigerenzer. He stated that Gigerenzer preferred to look at cognitive processes underlying decision making. Vranas (2000) stated that Gigerenzer was not stating that single-case judgements are invalid but that Gigerenzer wanted Kahneman and Tversky to present a proof that they are valid. Vranas (2000) stated that he did not think a proof was necessary and that Gigerenzer was assuming a frequentist view of statistics when it was likely that a subjectivist view was more appropriate. Both Kahneman and Gigerenzer reviewed Vranas (2000) before it was published.

A third model of decision making called the Recognition-Primed Decision (RPD) model was introduced by Klein (1993). Klein (1993) described the RPD model as a model in which the decision maker does not make a choice between two or more options, but instead acts based on prior experience. Klein (1993) used the example of a firefighter chief in action at a fire. Asked afterwards how he chose what to do, the chief stated that he made no conscience choice and simply sprang into action.

There have been many studies regarding how heuristics may affect user decision-making when faced with a computer security decision (Anderson et al., 2016; Bravo-Lillo et al., 2011; Gerlach et al., 2019). Many of the studies regarding heuristics used some kind of role-playing methodology in which the participants were given a scenario and asked for their response, either through interview (Arazy et al., 2017; Bravo-Lillo et al., 2011) or through action (Anderson et al., 2016; Gerlach et al., 2019).

Students appeared to be a common sample in these types of investigations (Anderson et al., 2016; Arazy et al., 2017; Bravo-Lillo et al., 2011), and one study used a professional firm to recruit participants (Gerlach et al., 2019). Two of the studies (Arazy et al., 2017; Bravo-Lillo et al., 2011) distinguished between novice and advanced users. Bravo-Lillo et al. (2011) distinguished advanced users by whether they had taken at least one computer security course or had worked in the computer security field for at least a year. Arazy et al. (2017) used professional university librarians as advanced users.

In general, the results of the studies regarding heuristics showed that some level of misjudgment occurs when heuristics are used (Bravo-Lillo et al., 2011; Gerlach et al., 2019). Bravo-Lillo et al. (2011) noted that advanced users differ from novice users in that advanced users judge risk before taking action while novice users judge risk after taking an action. Anderson et al. (2016) stated as an implication that methods that reduce habituation should be used when displaying a warning. The stated implication of Arazy et al. (2017) was that measuring heuristics is difficult. For future research, Gerlach et al. (2019) encouraged further research on how heuristics affects privacy-related beliefs.

METHODOLOGY

This study is the first in a sequence of several studies that will investigate whether requiring email users to pause by displaying an email warning with a timer (countdown, count-up, or no counter as a control) when they are presented with a potentially malicious email has any effect on the percentage of them falling to phishing attacks. This research phase of the larger study will start with the collection of qualitative and quantitative data from SMEs (Straub, 1989). The objective of this study is to find a validated timer level at which to set the countdown or count-up timer to display in the mobile app that will later be developed based on the initial findings of the level of pausing from the SMEs. The Delphi method will be utilized with multiple rounds until a consensus is reached (Ramim & Lichvar, 2014). The objective of the next step of this on-going research study will be to develop, test, and validate a custom mobile app. The mobile app will be a Gmail-like client. In the proposed app, a dialog will overlay any email that has a link, and the dialog will not be dismissible. The dialog will have a countdown or count-up timer set to a value that will be determined by the first research question. The independent variables that will be used in the app for the treatment groups are timer level and the type of timer (countdown or count-up) determined by the SMEs. A quantitative and qualitative survey will be developed to capture the SMEs' feedback that will include a step-by-step process of what users will eventually see, however, in this initial assessment, the SMEs will be asked in the quantitative portion of the survey the recommended level of timer to use within the app. Moreover, they will be provided with a set of experimental protocols and be asked whether to (1) "Keep", (2) "Adjust", or (3) "Remove" each step of the experiments. If the SME proposes "Adjust" or "Remove", they will be asked in the qualitative part of the survey to provide feedback on how to adjust or why to remove that step. Averages of the proposed pause time to use within the app will be calculated and Kendal W nonparametric statistics will be assessed to ensure SMEs consensus is reached or additional Delphi rounds needed to further refine the agreement among the SMEs.

Proposed Field Experiments

As part of this study, the SMEs will be asked to validate the protocol of the proposed field experiments. The two proposed field experiments, upon validation from the SMEs, will be coded into an app to be used later with participants in future research. This proposed study is the first in a series of studies that offer promise to address this problem because the polymorphic techniques proposed are designed to engage the slow, logical thought process of the email user on a mobile device. Engaging the email user in a logical thought process is promising because errors in judgement have been found to occur when people use heuristics (Gerlach et al., 2019; Tversky & Kahneman, 1974). Using a countdown or count-up timer as part of the warning message is promising because it has been shown that people often assess timed events as important (Acquisti et al., 2017). Brustoloni and Villamarín-Salomón (2007) found that polymorphic warnings help to mitigate unjustified risk, as well as Anderson et al. (2016) and Egelman et al. (2008) both found polymorphic warnings to be more effective than static warnings. De Keukelaere et al. (2009) presented a machine-learning algorithm in a custom app that received as input the user's experience and outputted a custom warning message. They also presented a dialog that gave feedback to the participant. They found that participants who were given the custom message took more time to decide on a potentially unsafe action than participants who were given a static warning dialog.

During the field studies, participants, who will have been recruited via Facebook and LinkedIn, will be asked to check a Gmail-like account through the app. A special email will be created for the users with indication that some promotions and added-value benefits will be provided via that email. Yan et al. (2015) studied user behavior for one week. Since this study is also analyzing user behavior, participants will be asked to check their newly created "promotional" email through the app for seven days. A phishing campaign service will be used to send phishes to the participants along with several legitimate emails including Groupons and other localized promotional benefits. Alert Logic (2018) stated that the average user receives 17 malicious emails per month. Therefore, each participant will receive four phishes through the phishing campaign service during the seven days in which they are participating in this study, which will also incorporate any real phishes received. The list of participants, with demographic information but with no PII, will be used to randomly organize the participants into two evenly sized groups, while the demographic factors will be checked for valid distributions. Both groups will receive the same phishing emails and will be asked to participate for the same length of time such that one group participates in the study before the other group. Since each group of participants will be asked to participate for seven days, the total study duration will be 14 days.

The app will collect and store anonymous data from the participants. When participants download the app, they will be given a User Identification Number (UIN) which will be used to link their anonymous data to their profile, and participants will be asked to take a short survey which will include demographic questions. No PII data will be captured or stored and no linking between an individual user and their data will be done to ensure participants' protection under the Institutional Review Board (IRB) provided for the study. In particular, participant age, gender, education level, attention span, and the amount of email they receive will be stored. Attention span will be measured with an attention span test by Psychology Today (n.d.) which will be embedded in the app survey. For each email with a potentially malicious link opened, the data collected will be: (1) the URL of the link, and (2) whether or not the participant clicked on the link. The data will be stored in Google forms.

Validity and Reliability

External validity refers to the generalizability of results (Sekaran & Bougie, 2016). Since this study uses SMEs to determine the timer level for the mobile app, external validity is increased. In addition, SMEs will be used to test and validate the mobile app itself. Reliability is the measure of how consistent experimental results are as time passes (Sekaran & Bougie, 2016). A study is considered reliable if the same input consistently produces the same output (Ellis & Levy, 2009). In addition, stability reliability refers to how an instrument produces output over a period of time (Ellis & Levy, 2009; Sekaran & Bougie, 2016). Since the mobile app will be tested for functionality by SMEs, reliability will be increased.

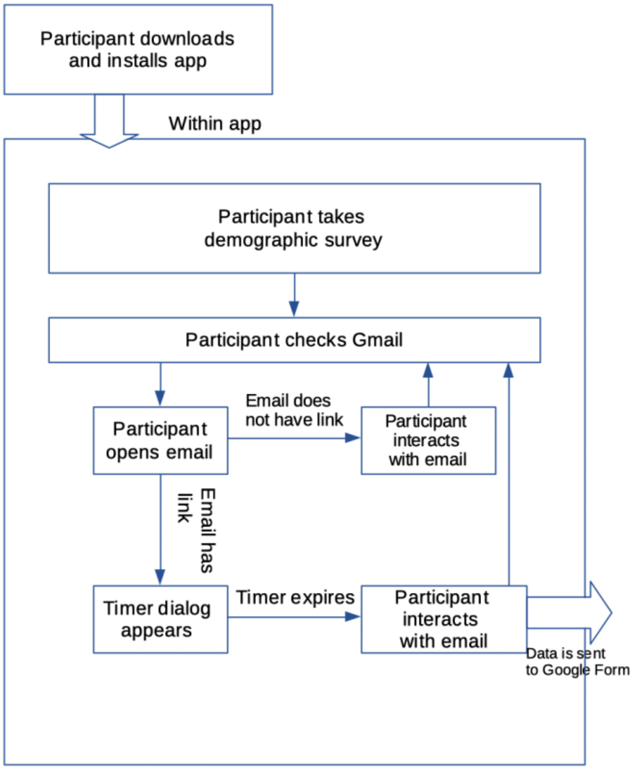
Participant downloads and installs app
Within app
Participant takes demographic survey
Participant checks Gmail
Participant opens email
Email does not have link
Participant interacts with email
Email has link
Timer dialog appears
Timer expires
Participant interacts with email
Data is sent to Google Form

Figure 1: Field Experiment Design

ANTICIPATED RESULTS

This study is expected to collect data from the SMEs on the proposed field experiments and provide support to ensure their validity in order to proceed to the next step of the research. Results are expected to include data from 20 SMEs. Results are expected to give a guideline for timer values for use in the countdown and count-up timers and to validate the custom mobile app that will be used in the subsequent field experiments.

DISCUSSION AND CONCLUSIONS

Phishing is still a significant problem to be solved. Billions of dollars and personal and corporate data are lost to phishing attacks each year (FBI, 2018). This research is the first in a series of research studies that propose to mitigate phishing by requiring the user to pause before opening an email, thus moving the user from a quick, instinctual mindset to a logical, thoughtful mindset. SME opinions will be gathered for timer values, which will be used in a countdown or count-up dialog that requires the user to pause before continuing to read an opened email. SMEs feedback will also be used to validate and verify functionality of a custom mobile app which will be used for subsequent studies. External validity will be controlled in this series of studies since participants will be asked to use a Gmail-like accounts that will be made for them during the experiments.

A limitation of this study is the software life cycle for the custom mobile app. If the app is shown to have serious defects, the time to fix those defects may be lengthy and discourage the users from continuing to participate in the study. As such following the SMEs phase of the study, a pilot study with small group of users will be done to assess any issues in the app that will then be corrected before the full study will engage the participants. Another limitation may be that this research uses Gmail-like email rather than true personal Gmail account and thus the volume of emails received on that email may not be the same as other. In an effort to mitigate this potential limitation, the special email account of all participants will be subscribed for several promotional services such as Yelp, Google Maps, Groupon, Etsy, and several regular retail companies such as Macys, Bloomingdales, William Sonoma, Saks Fifth, Guess, etc. to ensure these accounts generate significant volume of emails to mimic real-life environment. Future research will include using the custom mobile app to test participants' ability to avoid phishes when presented with a countdown or count-up timer. Future work may also include using a timer to mitigate browser users' susceptibility to malicious links in webpages. The results of these future studies will provide further understanding in the body of knowledge of the role heuristics and habit play in phishing mitigation.

REFERENCES

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., & Sleeper, M. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR), 50*(3), 44. https://doi.org/10.1145/3054926

Alert Logic. (2018, August 22). *Must-know phishing statistics 2018*. https://blog.alertlogic.com/must-know-phishing-statistics-2018/

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems, 26*(6), 661-687. https://doi.org/10.1057/s41303-017-0057-y

Amran, A., Zaaba, Z. F., & Mahinderjit Singh, M. K. (2018). Habituation effects in computer security warning. *Information Security Journal: A Global Perspective, 27*(4), 192-204. https://doi.org/10.1080/19393555.2018.1505008

Anderson, B., Vance, A., Kirwan, C., Jenkins, J., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems, 33*(3), 713-743. https://doi.org/10.1080/07421222.2016.1243947

Anti-Phishing Working Group. (2020). *Phishing activities trends report 1st quarter 2020*. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

Arazy, O., Kopak, R., & Hadar, I. (2017). Heuristic principles and differential judgments in the assessment of information quality. *Journal of the Association for Information Systems, 18*(5), 403-432. https://doi.org/0.17705/1jais.00458

Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management, 3*(1), 180-207.

Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy, 9*(2), 18-26. https://doi.org/10.1109/MSP.2010.198

Brustoloni, J. C., & Villamarín-Salomón, R. (2007, 2007, July 18-20). *Improving security decisions with polymorphic and audited dialogs* [Paper presentation]. 3rd Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania.

Burns, A., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce, 29*(1), 24-39. https://doi.org/10.1080/10919392.2019.1552745

Carlton, M., Levy, Y., & Ramim, M. M. (2018). Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool. *Online Journal of Applied Knowledge Management (OJAKM), 6*(1), 107-118. https://doi.org/10.36965/OJAKM.2018.6(1)107-118

Clement, J. (2019). *E-mail usage in the United States - Statistics & Facts*. https://www.statista.com/topics/4295/e-mail-usage-in-the-united-states/

De Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L., & Zurko, M. E. (2009). Adaptive security dialogs for improved security behavior of users. *Proceedings of the IFIP Conference on Human-Computer Interaction*, 510-523. https://doi.org/10.1007/978-3-642-03655-2_57

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1065-1074. https://doi.org/10.1145/1357054.1357219

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology, 6*, 323-337.

FBI. (2018). *Business e-mail comprimise the 12 billion dollar scam*. https://www.ic3.gov/media/2018/180712.aspx

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. *IEEE Technology and Society Magazine, 26*(1), 46-58. https://doi.org/10.1109/MTAS.2007.335565

Gerlach, J., Buxmann, P., & Dinev, T. (2019). “They’re all the same!” Stereotypical thinking and systematic errors in users’ privacy-related judgments about online services. *Journal of the Association for Information Systems, 20*(6), 787-823. https://doi.org/10.17705/1jais.00551

Gigerenzer, G. (1991). How to make cognitive illusions disappear: Beyond “heuristics and biases”. *European Review of Social Psychology, 2*(1), 83-115.

Gigerenzer, G. (1996). On narrow norms and vague heuristics: A reply to Kahneman and Tversky. *Psychological Review, 103*(3), 592-596. https://doi.org/10.1037/0033-295X.103.3.592

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44. https://doi.org/10.17705/1jais.00447

Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association, 26*(6), 547-552. https://doi.org/10.1093/jamia/ocz005

Iyengar, R. (2020, July 16). *Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others*. CNN. https://www.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html

Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., & Kumar, R. (2016). Social engineering: Hacking a human being through technology. *IOSR Journal of Computer Engineering, 18*(5), 94-100. https://doi.org/10.9790/0661-18050594100

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597-626. https://doi.org/10.1080/07421222.2017.1334499

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1996). On the reality of cognitive illusions. *Psychological Review, 103*(3), 582-591. https://doi.org/10.1037/0033-295X.103.3.582

Keegan, O., & O’Mahony, M. (2003). Modifying pedestrian behaviour. *Transportation Research Part A: Policy and Practice, 37*(10), 889-901. https://doi.org/10.1016/S0965-8564(03)00061-2

Klein, G. A. (1993). A recognition-primed decision (RPD) model of rapid decision making. *Decision making in action: Models and methods, 5*(4), 138-147.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Lo, J. C., Twan, D. C., Karamchedu, S., Lee, X. K., Ong, J. L., Van Rijn, E., Gooley, J. J., & Chee, M. W. (2019). Differential effects of split and continuous sleep on neurobehavioral function and glucose tolerance in sleep-restricted adolescents. *Sleep*, *42*(5), 1-10. https://doi.org/10.1093/sleep/zsz037

Marto, J. P., Borbinha, C., Calado, S., & Viana-Baptista, M. (2016). The stroke chronometer—A new strategy to reduce door-to-needle time. *Journal of Stroke and Cerebrovascular Diseases*, *25*(9), 2305-2307. https://doi.org/10.1016/j.jstrokecerebrovasdis.2016.05.023

Mihelič, A., Jevšček, M., Vrhovec, S., & Bernik, I. (2019). Testing the human backdoor: Organizational response to a phishing campaign. *Journal of Universal Computer Science, 25*(11), 1458-1477.

Musuva, P., Chepken, C., & Getao, K. (2019). A naturalistic methodology for assessing susceptibility to social engineering through phishing. *The African Journal of Information Systems, 11*(3), 157-182.

Psychology Today. (n.d.). *Attention span test*. https://www.psychologytoday.com/us/tests/personality/attention-span-test

Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management, 2*(1), 122-136.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. https://doi.org/10.3390/fi11040089

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). John Wiley & Sons, Ltd.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169. https://doi.org/10.2307/248922

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management, 12*(3), 1-23. https://doi.org/10.5539/10.5539/ijbm.v13n6p1

Thompson, H. (2012). The human element of information security. *IEEE Security & Privacy, 11*(1), 32-35. https://doi.org/10.1109/MSP.2012.161

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124

Vance, A., Jenkins, J. L., Anderson, B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly, 42*(2), 355-380. https://doi.org/10.25300/MISQ/2018/14124

Vranas, P. B. (2000). Gigerenzer's normative critique of Kahneman and Tversky. *Cognition, 76*(3), 179-193.

Yan, J., Qiao, Y., Yang, J., & Gao, S. (2015). Mining individual mobile user behavior on location and interests. *Proceedings of the 2015 IEEE International Conference on Data Mining Workshop*, 1262-1269. https://doi.org/10.1109/ICDMW.2015.122