Pilot testing of experimental procedures to measure user's judgment errors in simulated social engineering attacks

Tommy Pollock, Nova Southeastern University, USA, tp809@mynsu.nova.edu

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Wei Li, Nova Southeastern University, USA, lwei@nova.edu

Ajoy Kumar, Nova Southeastern University, USA, akumar@nova.edu

Abstract

Distracted users appear to have difficulties correctly distinguishing between legitimate and malicious emails or search engine results. Additionally, mobile phone users appear to have a more challenging time identifying malicious content due to the smaller screen size and the limited security features in mobile phone applications. Thus, the goal of this research study was to conduct a pilot test and validate a set of field experiments based on Subject Matter Experts (SMEs) feedback to assess users' judgment when exposed to two types of simulated social engineering attacks: phishing and Potentially Malicious Search Engine Results (PMSER), based on the interaction of the environment (distracting vs. non-distracting) and type of device used (mobile vs. computer). This paper provides the results from the pilot test we conducted using recruited volunteers consisting of 10 participants out of 20 volunteers invited. Due to COVID-19 restrictions, all interactions in this pilot testing were conducted remotely. These restrictions somewhat limited our ability to control the testing environment to ensure a completely non-distractive environment during these parts of the study; however, a significant attempt was made to ensure such a non-distractive environment was genuinely adhered to during that part of the study. Our initial pilot testing results indicate that the findings were counterintuitive for the Phishing Intelligence Quotient (IQ) tests. In contrast, results of the PMSER were intuitive with improved detection on a computer compared to mobile. We conclude with a discussion on the study limitations and further research.

Keywords: Social engineering, cybersecurity, judgment error in cybersecurity, phishing email mitigation, distracting environments.

Introduction

Phishing, malware, ransomware infection from emails, and Potentially Malicious Search Engine Results (PMSER) inflict significant financial losses on individuals and organizations (Anderson et al., 2013; Ogbanufe, 2021; Wright & Marett, 2010). Cybercriminals use increasingly ingenious schemes to take advantage of users' judgment errors when dealing with phishing emails and PMSER (Leontiadis et al., 2014). Phishing is a subcategory of Social Engineering and is "a type of cyber-attack that sits at the intersection of social engineering and security technologies" (McElwee et al., 2018, p. 1). The Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3) (2020) phishing campaign defined phishing as "e-mail containing a malicious file or link" (p. 14). These phishing schemes often use official-looking logos to distract the target from the spelling inconsistencies or embed fake links in the email (Wright & Marett, 2010). Phishing continues to be an invasive threat to computer and mobile device users (McElwee et al., 2018; FBI, 2020). Cybercriminals continuously develop new phishing schemes using email and malicious search engine links to gather the personal information of unsuspecting users (Anderson et al., 2013). This information is used for financial gains through identity theft schemes or draining victims' financial accounts (Moody et al., 2017).

Deceptive search engine results pose a significant cybersecurity threat because cybercriminals often manipulate the results algorithms through search poisoning techniques, which promote malicious links to the first page of the search engine results (Leontiadis et al., 2014). Due to the COVID-19 pandemic, such search engine results were increasingly used to attack individuals and organizations. Superficially, the FBI (2020) noted that among the victims of such cyberattacks are "medical workers searching for personal protective equipment, families looking for information about stimulus checks to help pay bills, and many others" (p. 3). Users of mobile phones, in particular, appear to be more vulnerable to phishing attacks than those who use Personal Computers (PCs) due to poor fraudulent website detection of some mobile browsers along with the limitation of the smaller screen (Mavroeidis & Nicho, 2017; Wash & Rader, 2021). Quick Response (QR) code readers, which are mobile phone apps, are also reported to be used as a phishing attack vector due to the difficulty differentiating between a hijacked QR code and an actual one (Focardi et al., 2018). Mobile phones are often the primary platform users utilize nowadays to access various web-based platforms, exposing them to phishing and clickbait schemes (Frauenstein & Flowerday, 2016). Users tend to take their mobile phones with them everywhere, making judgment errors in distracting environments. The term judgment error refers to individuals making a wrong or bad decision that usually involves calculated risks, evaluating options, and executive decision making (Chowdhury, 2016, p. 42). Even in non-distracting environments such as a business office or home-office setting, it was indicated in prior research that users still have a hard time judging the legitimacy of emails and web links on their PC, being a desktop or laptop (Furnell, 2007).

While logical thinking provides the ability to make rational choices in decision making, it often fails due to errors in judgment (Kahneman, 2011). Cybercriminals continue to take advantage of mobile phone or PC users' judgment errors to enrich themselves. A user's vulnerability to phishing attempts is affected by their ability to keep their information secure (Li et al., 2014). While there is abundant literature and training materials on ways to avoid falling for phishing scams, there is also evidence in the literature that users tend to be unmotivated or ignore the visual cues in emails or web links due to security not being their primary concern (Williams et al., 2018). Moreover, it was indicated that "environmental distractions can impact cognitive performance, whether this concerns solving a mathematical problem, maintaining a conversation, or retrieving an experienced event from memory" (Vredeveldt & Perfect, 2014, p. 1).

A distracting environment can occur in any setting with constant interruptions from background noise (Larsby et al., 2008). This distraction will lead to increased vulnerabilities to personal devices and PCs both in public and at work (Halevi et al., 2013). With the added distractions causing judgment errors in the workplace and social environments, due to an ever-increasing reliance on connected devices, it appears that there is a need to assess the role of environment and device type on the success of social engineering attacks (Williams et al., 2018). Thus, the main goal of this research study was to validate further a set of experiments that was initially validated using an expert panel (Pollock et al., 2022) while providing initial empirical validation for the set of experiments with participants to assess if there are statistically significant mean differences in users judgment, when: exposed to two types of simulated social engineering attacks (phishing & Potentially Malicious Search Engine Results (PMSER)), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile vs. computer) using eight mini-Intelligence Quotient (IQ) tests. The Research Questions (RQs) we addressed in this pilot test study are:

RQ1. What are the users' judgments when exposed to two types of simulated social engineering attacks (phishing & PMSER) in two kinds of environments (distracting vs. non-distracting) and two types of devices (mobile phone vs. computer)?

RQ2. Are there any statistically significant mean differences in users' judgments when exposed to two types of simulated social engineering attacks (phishing & PMSER), in two kinds of environments (distracting vs. non-distracting) and two types of devices (mobile phone vs. computer) when controlled by (a) age, (b) gender, (c) level of education, and (d) social media usage?

Literature Review

The nexus of this research builds on prior literature by hypothesizing that differences in the level of distracting environments when it comes to judgment errors in users exposed to two types of simulated social engineering attacks (phishing & PMSER) may be dependent on the kind of environment (distracting vs. non-distracting) and type of device used (mobile phone vs. computer). Users that habitually share web links on their devices tend to have low-security awareness, potentially opening them up to more vulnerabilities that cause significant cybersecurity damage to themselves and the organizations they are working for (Halevi et al., 2013; Levy & Gafni, 2021). Mobile phone usage proves to be too much of a temptation for some people during work and social times, distracting them from whatever tasks they are performing and causing detrimental effects on performance, also known as cyberslacking (Alharthi et al., 2019). The use of mobile phones in the working or learning environment poses a risk of multiple distractions that may affect the ability of users to perform assigned tasks (Drew & Forbes, 2017). These distractions pose an attention conflict that can overload cognitive function, which reduces performance, leading to difficulty completing tasks (Kahneman, 1973; Sanders et al., 1978). Interruptions caused by distractions force people to focus elsewhere instead of their need to perform work tasks (Speier et al., 2003). The time to complete tasks can be significantly affected by interruptions in the work environment (Mansi & Levy, 2013). Distractions from environmental factors are comparable to person-based interruptions due to work time lost from the disturbance (Sanders et al., 1978).

Phishing

Phishing scams are among the oldest and most widely used social engineering methods to gain personal information and infiltrate organizational systems, mainly for financial gain (Moody et al., 2017). "Social engineering consists of persuasion techniques to manipulate people into performing actions or divulging confidential information" (Ferreira et al., 2015, p. 36). Phishing attempts often are email-based attacks but can also occur through spoofed website links (Zhao et al., 2017). Users of PCs are not the only ones susceptible to phishing; those on mobile phones are also targeted as well (Goel & Jain, 2018). Mobile phone users are rich targets for phishing attempts because they take them everywhere and often store significant volume of personal and financial data on them (Li et al., 2014). These attempts are becoming more sophisticated by using distracting features and persuasive elements (Chiew et al., 2018). The content of these messages is often disguised as legitimate companies. It contains rational, emotional, and motivationally appealing elements that tempt users to click on links to gain their personal information to steal their identity or financial assets (Kim & Kim, 2013). Cybercriminals often design phishing schemes to victimize vulnerable targets (Zhao et al., 2017). Some users are more susceptible to phishing attacks than others (Oliveira et al., 2017). Some demographic groups, such as children, teens, and senior citizens, are more susceptible to phishing attacks (Flores et al., 2015). Users are targeted at work and private on their computers and mobile phones to gain personal information that is then used for a larger cyber-attack and cause significant financial damages (Virvilis et al., 2014; Williams et al., 2018). Current research provides strong evidence that users still fall victim to phishing attacks, even when provided with proper cybersecurity training (Albladi & Weir, 2018; Moody et al., 2017). Corporate controls for phishing prevention also often fail (Levy & Gafni, 2021; McElwee et al., 2018; Silic & Back, 2016).

Potentially Malicious Search Engine Results (PMSER)

Manipulation of search engine results to direct users to malicious websites is a troubling trend that can be highly profitable for cybercriminals (Moore et al., 2011). This manipulation often occurs because users mainly just review the first page of the results returned from their search query (Henzinger et al., 2002). Additionally, the top several results are paid-based advertised links, noted in most cases with a tiny “Ad” next to them. These advertising links are facilitated by third-party marketing agencies and are not regulated, allowing cybercriminals to freely purchase advertisement spots, showing initially a non-contaminated site to the third-party marketing agencies, and then shortly after the advertising is active, enabling the malicious payload on these sites causing individuals to fall victim for their malware or ransomware. Furthermore, cybercriminals use methods such as search engine optimization or search engine spam to drive their malicious sites to the top of the search engine results page (Egele et al., 2011; Howard & Komili, 2010). Attackers manipulate search engine optimization algorithms by poisoning the search results through the use of keywords as a means to inject malware into users systems (John et al., 2011; Lu et al., 2011). In search engine spam attackers can also deploy predefined scripts containing search queries that generate clicks to web pages to drive them to the top of the SER page (Chandra & Suaib, 2014). Cybercriminals often will use trending events such as elections or pandemics to deploy their search engine optimization and search engine spam techniques in order to deploy their malware or scareware on unsuspecting users through drive by attacks (Metaxas & Pruksachatkun, 2017; Vukelić, 2022). While search engine companies have made improvements to demote the search engine optimization poisoning and search engine spam, cybercriminals are also adapting their techniques to combat this through other means such as cloaking and search-redirection (Leontiadis et al., 2014).

Environmental Factors

Environmental factors affect how users perform tasks in the workplace, at home, and in public (Vredeveldt & Perfect, 2014). Background noise negatively affects task performance because it distracts and interrupts users (Larsby et al., 2008). However, background music has mixed results (Dalton & Behm, 2007). Instant Messaging (IM) apps in the workplace also pose a distraction in the working environment (Mansi, 2011; Mansi & Levy, 2013). These distractions hurt users' psychological state, causing mental fatigue and reduced working memory capacity (Conway et al., 2001; Zijlstra et al., 1999). When the working memory is overloaded, users' decision-making process causes judgment errors (Gómez-Chacón et al., 2014). Distracting environments can have a negative effect on working and attentional memory (Rodrigues & Pandeirada, 2015). Lapses of attention caused by external distractions interrupt task performance by inhibiting the attentive processes of working memory (Christophel et al., 2017). Rodrigues and Pandeirada (2015) tested the working memory of 40 elderly research participants in distracting and non-distracting environments. They found that the participants performed the tasks better in the non-distracting environment. The use of irrelevant stimuli has been found to distract someone from focusing on a task by disrupting attentional awareness (Unsworth & Robison, 2016). Many of these irrelevant stimuli are used in phishing emails to distract the recipient from other details that may give away the true nature of the email (Ferreira & Teles, 2019; Pearson, 2019). These irrelevant distractors can create involuntary shifts in spatial attention, affecting reaction times by adding a filtering cost to information processing (Folk & Remington, 1999).

Judgment Errors

Many researchers have studied why humans make choices when faced with decisions often under uncertain terms (Fox & Tversky, 1998; Kahneman & Tversky, 1982; Tversky & Kahneman, 1992). Some of these choices are reason-based, belief-based, and involve bias (Ayton & Pascoe, 1995; Fox & Tversky, 1998; Shafir et al., 1993). Human error has been researched for decades by several researchers that have made extensive contributions to the field (Cohen, 1981; Reason, 1990; Tversky & Kahneman, 1974, 1983). Tversky and Kahneman (1974) began researching human judgment when presented with uncertain choices. In the process of this research, they developed System 1 (intuitive) and System 2 (analytical) thinking in the decision-making process (Tay et al., 2016; Tversky & Kahneman, 1983). System 1 and System 2 thinking work hand in hand in human judgment, with analytical thinking either confirming or overriding intuitive thinking (Frankish, 2010). Judgments are often made from multiple cues provided by the information being processed. These judgments, however, can be affected by subconscious cognitive biases (Evans, 2008). Users are subjected to various distractions when interacting with mobile phones and computers; often, these distractions cause errors in judgment (Chowdhury, 2016). Mobile phones cause many distractions by inhibiting the working memory of users (Nicholson et al., 2005). Many users do not understand the risks of using computers and mobile phones (Schneier & West, 2008). Cybersecurity tends to be a low priority for users unless a problem arises (Schneier & West, 2008). Cybersecurity is a low priority because users do not fully understand the losses involved (Schneier & West, 2008; Tversky & Kahneman, 1983). Users will often develop anxiety and coping mechanisms when dealing with potential phishing scams (Wang et al., 2017). Distracted users often have a hard time detecting the elements of phishing emails leading to potential judgment errors (Furnell, 2007; Karakasiliotis et al., 2006). Many users make a judgment on visual and technical cues in phishing emails and will often not be able to detect phishing attempts (Karakasiliotis et al., 2006). Habitually reading emails while distracted by various environmental factors can increase users' susceptibility to phishing scams (Vishwanath et al., 2011). Errors of judgment often have significant consequences involved with them, depending on the context (Chowdhury, 2016).

Methodology

This study is experimental field research and documents the pilot testing phase conducted with research volunteers to further validate the set of experiments that previously were validated with the Subject Matter Experts (SMEs) now with small group of pilot participants (Pollock et al., 2022). Participants were asked to take eight short mini-IQ tests using two types of personal devices: their mobile phones and computers, where four of the test were in non-distracting environments and the other four were in a distracting environments. The mini-IQ tests were distributed through survey links using Qualtrics. The distracting environment was achieved using a distracting background sound file played from a PC via a Zoom session when participants took the two mini-IQ tests set for the distracting environment testing. This pilot testing was essential to finalize the delivery method and data analysis for the mini-IQ tests for the phishing and PMSER experiments. The participants were given a set of instructions that included links for the non-distracting environment phase (on both type of devices) and, due to COVID-19, a Zoom link for the distracting environment phase to be observed, also on both type of devices. This was important to ensure that the distracting sound file was played while participants were taking the surveys on both type of devices. The sound file was developed based on the SMEs' feedback in the earlier Delphi phase of this study (Pollock et al., 2022). Six soundtracks were combined into the sound file using Adobe Audition consisting of crowd noise from an office, two airport sounds, a crying baby, circus music, and a random distracting royalty-free sound found on YouTube.

Data Analysis and Results

Invitation emails to participate in the pilot testing surveys were sent to 20 potential participants with a goal of reaching a 50% response rate or 10 respondents. A group of 10 respondents agreed to participate in this pilot test, answering questions based on the SMEs' validated tasks and procedures. Table 1 provides the descriptive statistics of the 10 participants during the pilot test, which took place in December of 2021. The participants were both males and females, ages 30 to 59. The participants' educational backgrounds included highly educated pilot participants, with 60% with Doctoral/Professional degrees and 40% with Graduate degrees. The participants' social media usage had 50% 'Often', 30% 'Sometimes', 10% 'Occasionally', and 10% 'Never'.

Table 1. Descriptive Statistics of Pilot Test Participants (N=10)

Demographics Indicator	Frequency	Percentage
Age		
18-19	0	0%
20-29	0	0%
30-39	3	30%
40-49	4	40%
50-59	3	30%
Over 60	0	0%
Gender		
Female	4	40%
Male	6	60%
Education		
High School Diploma	0	0%

Demographics Indicator	Frequency	Percentage
2-year College (Associates Degree)	0	0%
4-year College (Bachelor's degree)	0	0%
Graduate degree	4	40%
Doctorate/Professional	6	60%
Social Media Usage		
Never	1	10%
Occasionally	1	10%
Sometimes	3	30%
Often	5	50%
Always	0	0%

The mini-IQ tests were developed based on previous research to include a mixture of phishing emails and potentially malicious and legitimate search engine links. Participants were asked to identify if the image of an email or a search engine link was (a) Legitimate, (b) Phishing/Potentially Malicious Link, or (c) Ask IT Department. There were three legitimate emails, three legitimate links, nine non-legitimate emails, and nine non-legitimate links. For the emails and PMSER links, to avoid user fatigue and to have the user remember the social engineering samples provided, a randomized list was generated to include easy, medium, and hard to detect samples to ensure the level of detection is not constant as it is in confirmed cases of social engineering (See randomization table in Figure 1).

Social Engineering Attack Type

Phishing

Device	**Environment:** Distracting	**Environment:** Non-Distracting
Mobile Phone	Distracted via Mobile Phone • Phishing Hard • Legitimate • Phishing Easy	Not Distracted via Mobile Phone • Legitimate • Phishing Easy • Phishing
Computer	Distracted via Computer • Phishing Easy • Phishing Medium • Phishing Hard	Not Distracted via Computer • Phishing Medium • Phishing Hard • Legitimate

PMSER

Device	**Environment:** Distracting	**Environment:** Non-Distracting
Mobile Phone	Distracted via Mobile Phone • Legitimate • PMSER Easy • PMSER Medium	Not Distracted via Mobile Phone • PMSER Easy • PMSER Medium
Computer	Distracted via Computer • PMSER Medium • PMSER Hard • Legitimate	Not Distracted via Computer • PMSER Hard • Legitimate • PMSER Easy

Figure 1. Randomization Table for the Mini-IQ Tests Difficulty Level (Pollock et al., 2022).

Phishing email and PMSER samples were then created following the three levels of detection (easy, medium, & hard) for each social engineering type and were validated using SMEs. We have coded each response based on the severity of the identified email or link, as indicated in Table 2. Moreover, for each mini-IQ test, three samples were provided, and scoring across all three was summed, indicating a scoring from three (3x1) to 18 (3x6).

Table 2. Scoring of Mini-IQ Responses for Phishing and PMSER Selections

Actual	Participant's Selection	Score
Non-Legitimate	Non-Legitimate	6
Legitimate	Legitimate	5
Non-Legitimate	Ask-IT Department	4
Legitimate	Ask-IT Department	3
Legitimate	Non-Legitimate	2
Non-Legitimate	Legitimate	1

Table 3 summarizes the participant results across all eight mini-IQ tests on the two devices, two environments, and two types of social engineering simulated attacks. The phishing mini-IQ test results do not follow what was initially indicated in prior literature. Specifically, we were surprised to learn that the non-distracting environment results for the phishing mini-IQ tests were overall lower than those of distracting environment, which appears to be counter to what we originally envisioned (See Table 3 & Figure 2a).

Table 3. *Pilot Test Summary of Participant's Results (N=10)*

Phishing IQ

	Distracting		Non-Distracting	
	Mean	St.Dev	Mean	St.Dev
Mobile	14.80	2.10	13.70	1.95
Computer	14.90	3.96	12.40	3.47

PMSER IQ

Distracting		Non-Distracting		
Mean	St.Dev	Mean	St.Dev	
14.00	2.05	14.50	3.14	Mobile
14.00	2.11	15.20	1.81	Computer

We assume that these phishing mini-IQ pilot test results may be due to the fact that during the distracting environment part, participants were monitored over zoom to enable the distracting sound file. Additionally, the small sample size of 10 individuals and the education level of the pilot testing participants could also be impacting factors. In contrast, in the non-distracting environment, they have marked the selections independently and may have rushed to identify the phishing samples. Additionally, counter to the initial expectation from literature, we found that computer users from our pilot results in a non-distracting environment resulted in the lowest scoring. In contrast, computer users in distracting environments appeared to have scored the highest, again counterintuitive results. Clearly, these results require further investigation (See Table 3 & Figure 2b). However, the PMSER mini-IQ test results were somewhat as expected, with overall scores on both mobile and computer in a distracting environment being lower than those in a non-distracting environment. In contrast, PMSER detection on a computer outperformed those on a mobile device. We suspect these results are more accurate as individuals' familiarity with PMSER is much lower. The participants' habituation to such messages is more deficient, causing them to pay closer attention and be more precise in their detections especially as they were under surveillance during the zoom distracting environment sessions. We conducted an Analysis of Variance (ANOVA) on the results. While it appears that some variations do exist, as presented in Table 3 and Figure 2, none of the comparisons were significant for phishing mini-IQ tests by environment (F=3.714, p=0.061) or device type (F=0.380, p=0.541), and PMSER mini-IQ tests by environment (F=1.383, p=0.247) or device type (F=0.228, p=0.636).

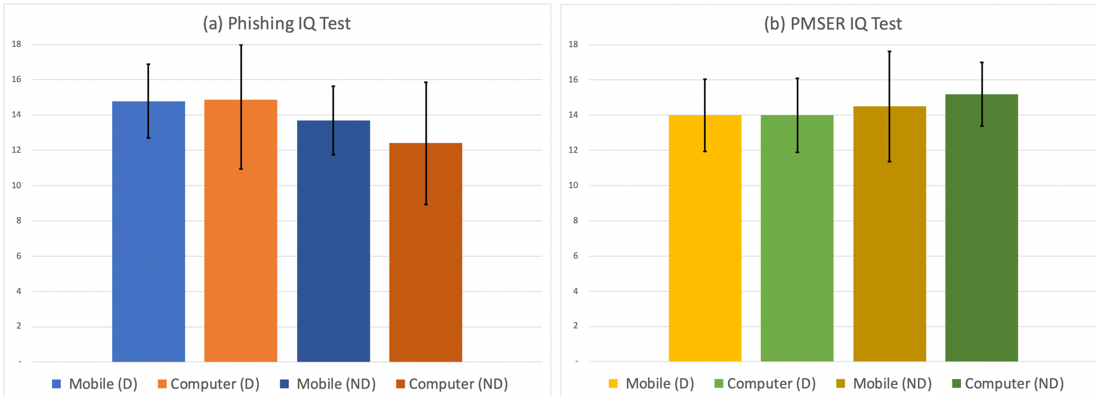

Figure 2. Results of the Pilot Mini-IQ Tests for Phishing (a) and PMSER (b)

We have also conducted an Analysis of Covariance (ANCOVA) on the overall scores of all eight mini-IQ tests based on the demographics indicators and found that, at least from the results of this pilot study, no demographics indicator tested provided any significant differences among the pilot study participants. It must be noted that the sample size of 10 participants in this pilot study was small, which could be a contributing factor to some of the insignificant results.

CONCLUSIONS AND DISCUSSIONS

This study presents the results of the pilot testing for a process previously validated by a group of 42 SMEs to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) during two kinds of environments (distracting vs. non-distracting) and two types of devices (mobile phone vs. computer). This study is relevant as it seeks to identify the vulnerabilities of information systems users exposed to two types of simulated social engineering attacks (phishing & PMSER), which adversaries commonly use to gain access to an individual's personal or organizational accounts, mainly for monetary gain. With the widespread use of mobile phones with Internet-connected applications, phishing attempts have increased through social engineering through scams and clickbait links. Frauenstein and Flowerday (2016) stated that users pick up bad habits by using link-sharing applications that leave them vulnerable to phishing attacks. These bad habits make it harder for people to discern between genuine and malicious links making them more susceptible to phishing attacks. Moreover, the significance of this research is in its potential to advance the current research in cybersecurity by increasing the body of knowledge regarding users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). Distracting environments at work and in public make it easier for a user to have errors in judgment when performing tasks. Attackers craft phishing attacks to try and distort the mental model users form in interacting with online transactions and distract them from the visual cues they usually pick up on. As the number of distractions increases, cognitive cues decrease, affecting decision-making due to cognitive overload (Kahneman, 1973). We feel that the results of this study provide initial input to the body of knowledge of users' susceptibility to social engineering attacks in distracting environments while using mobile phones and computers. While our results noted above indicated no significant difference on all eight experiments, the phishing results, while non-significant, still were somewhat counterintuitive. We can speculate from these results that when individuals are being observed, they may be more prone to think using their System 2 and, thus, their performance in detecting phishing emails is improved, rather than the impact of the distracting environment itself. Such differences in the impact on phishing email susceptibility is certainly requires more research. Like any research study, this study has several limitations. The main limitation of this pilot testing procedure is that all interactions with the participants were conducted remotely due to COVID-19 restrictions. Another major limitation of this study is that the small sample size of 10 participants affected the statistical testing. We have taken all measures to ensure that the distracting and non-distracting environments mimic reality. Still, it is understandably valid that users may be preconditioned during an experiment versus the full impact of such environments in natural settings. Another limitation was that the instructions for the testing procedures had to be changed a few times to ensure that our message was clear to the study participants on what they were asked to do. Our recruitment of research participants that had experience in pilot testing procedures helped mitigate this limitation.

Acknowledgements

We would like to thank the three outstanding reviewers and Prof. Meir Russ, Editor-in-Chief of the OJAKM, for all the time spent to provide us wonderful constructive feedback that helped us improve the quality of the paper greatly.

References

Alarm, S., & El-Khatib, K. (2016). Phishing susceptibility detection through social media analytics. *Proceedings of the 9th International Conference on Security of Information and Networks - SIN '16*, 61–64. https://doi.org/10.1145/2947626.2947637

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1). https://doi.org/10.1186/s13673-018-0128-7

Alharthi, S., Levy, Y., Wang, L., & Hur, I. (2019). Employees' mobile cyberslacking and their commitment to the organization. *Journal of Computer Information Systems*, *00*(00), 1–13. https://doi.org/10.1080/08874417.2019.1571455

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Awh, E., & Jonides, J. (2001). Overlapping mechanisms of attention and spatial working memory. *Trends in Cognitive Sciences*, *5*(3), 119–126. https://doi.org/10.1016/S1364-6613(00)01593-X

Ayton, P., & Pascoe, E. (1995). Bias in human judgment under uncertainty? *The Knowledge Engineering Review*, *10*(1), 21–41. https://doi.org/10.1017/S0269888900007244

Bailey, B. P., Adamczyk, P. D., Chang, T. Y., & Chilson, N. A. (2006). A framework for specifying and monitoring user tasks. *Computers in Human Behavior*, *22*(4), 709–732.

https://doi.org/10.1016/j.chb.2005.12.011

Berti, S., & Schröger, E. (2001). A comparison of auditory and visual distraction effects: Behavioral and event-related indices. *Cognitive Brain Research*, *10*(3), 265–273. https://doi.org/10.1016/S0926-6410(00)00044-6

Brooks, S. (2015). Does personal social media usage affect efficiency and well-being? *Computers in Human Behavior*, *46*, 26–37. https://doi.org/10.1016/j.chb.2014.12.053

Chandra, A., & Suaib, M. (2014). A survey on web spam and spam 2.0. *International Journal of Advanced*, *2*. http://search.proquest.com/openview/61231546566097ed930bd42255c88ca3/1?pq-origsite=gscholar&cbl=1626343

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors, and technical approaches. In *Expert Systems with Applications* (Vol. 106). https://doi.org/10.1016/j.eswa.2018.03.050

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1–16. https://doi.org/10.1145/2335356.2335358

Choo, K.-K. R. (2011). Cyber threat landscape faced by financial and insurance industry. In *Trends & issues in crime and criminal justice* (Issue 408).

Chowdhury, M. F. (2016). Is OHS negligence and evasion an “error of judgment” or “white-collar crime”? An interpretation of apparel manufacturers in Bangladesh. *Journal of Media Critiques*, *2*(8), 41–56. https://doi.org/10.17349/jmc116203

Christophel, T. B., Klink, P. C., Spitzer, B., Roelfsema, P. R., & Haynes, J. D. (2017). The distributed nature of working memory. *Trends in Cognitive Sciences*, *21*(2), 111–124. https://doi.org/10.1016/j.tics.2016.12.007

Cohen, L. J. (1981). Can human irrationality be experimentally demonstrated? *Behavioral and Brain Sciences*, *4*(3), 317. https://doi.org/10.1017/S0140525X00009092

Conway, A. R. A., Cowan, N., & Bunting, M. F. (2001). The cocktail party phenomenon revisited: The importance of working memory capacity. *Psychonomic Bulletin and Review*, *8*(2), 331–335. https://doi.org/10.3758/BF03196169

Dabrowski, A., Krombholz, K., Ullrich, J., & Weippl, E. R. (2014). QR inception. *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices - SPSM ’14*, *1*, 3–10. https://doi.org/10.1145/2666620.2666624

Dalton, B. H., & Behm, D. G. (2007). Effects of noise and music on human and task performance: A systematic review. *Occupational Ergonomics*, *7*, 143–152. http://www.iospress.nl/journal/occupational-ergonomics/

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–590. https://doi.org/10.1145/1124772.1124861

Drew, L., & Forbes, D. (2017). Devices, distractions, and digital literacy: ‘Bring your own device’ to polytech. *Teachers and Curriculum*, *17*(2), 61–70. https://doi.org/10.15663/tandc.v17i2.157

Egele, M., Kolbitsch, C., & Platzer, C. (2011). Removing web spam links from search engine results. *Journal in Computer Virology*, *7*(1), 51–62. https://doi.org/10.1007/s11416-009-0132-6

Enck, W. (2011). Defending users against smartphone apps: Techniques and future directions. *Proceedings of the International Conference on Information Systems Security*, *7093*, 49–70. https://doi.org/10.1007/978-3-642-25560-1_3

Evans, J. S. B. T. (2003). In two minds: Dual-process accounts of reasoning. *Trends in Cognitive Sciences*, *7*(10), 454–459. https://doi.org/10.1016/j.tics.2003.08.012

Evans, J. S. B. T. (2008). Dual-processing accounts of reasoning, judgement, and social cognition. *Annual Review of Psychology*, *59*, 255–278. https://doi.org/10.1146/annurev.psych.59.103006.093629

Evans, J. S. B. T., Clibbens, J., Cattani, A., Harris, A., & Dennis, I. (2003). Explicit and implicit processes in multicue judgment. *Memory and Cognition*, *31*(4), 608–618. https://doi.org/10.3758/BF03196101

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. *Proceedings of the Third International Conference on Human Aspects of Information Security, Privacy, and Trust - Volume 9190*, 36–47. https://doi.org/10.1007/978-3-319-20376-8_4

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human Computer Studies*, *125*, 19–31. https://doi.org/10.1016/j.ijhcs.2018.12.004

Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. *Proceedings of the 16th International Conference on World Wide Web*, 649–656. https://doi.org/10.1145/1242572.1242660

Fisk, J. E. (2002). Judgments under uncertainty: Representativeness or potential surprise? *British Journal of Psychology*, *93*(4), 431–449. https://doi.org/10.1348/000712602761381330

Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security*, *23*(2). https://doi.org/10.1108/ICS-05-2014-0029

Focardi, R., Luccio, F. L., & Wahsheh, H. A. M. (2018). Security threats and solutions for two-dimensional barcodes: A comparative study. In K. Daimi (Ed.), *Computer and Network Security Essentials* (pp. 207–219). Springer. https://doi.org/10.1007/978-3-319-58424-9_12

Folk, C. L., & Remington, R. (1998). Selectivity in distraction by irrelevant featural singletons: Evidence for two forms of attentional capture. *Journal of Experimental Psychology: Human Perception and Performance*, *24*(3), 847–858. https://doi.org/10.1037//0096-1523.24.3.847

Folk, C. L., & Remington, R. (1999). Can new objects override attentional control settings? *Perception and Psychophysics*, *61*(4), 727–739. https://doi.org/10.3758/BF03205541

Forster, S., & Lavie, N. (2008). Attentional capture by entirely irrelevant distractors. *Visual Cognition*, *16*(2–3), 200–214. https://doi.org/10.1080/13506280701465049

Fox, C. R., & Tversky, A. (1998). A belief-based account of decision under uncertainty.

Management Science, *44*(7), 879–895. https://doi.org/10.1287/mnsc.44.7.879

Frankish, K. (2010). Dual-process and dual-system theories of reasoning. *Philosophy Compass*, *10*, 914–926. https://doi.org/10.1111/j.1747-9991.2010.00330.x

Frauenstein, E. D., & Flowerday, S. V. (2016). Social network phishing: Becoming habituated to clicks and ignorant to threats? *Proceedings of the 2016 Information Security for South Africa Conference*, 98–105. https://doi.org/10.1109/ISSA.2016.7802935

Funder, D. C. (1987). Errors and mistakes: Evaluating the accuracy of social judgment. *Psychological Bulletin*, *101*(1), 75–90. https://doi.org/10.1037/0033-2909.101.1.75

Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud and Security*, *2007*(3), 10–15. https://doi.org/10.1016/S1361-3723(07)70035-0

Garrett, R. K., & Danziger, J. N. (2007). IM = Interruption management? Instant messaging and disruption in the workplace. *Journal of Computer-Mediated Communication*, *13*(1), 23–42. https://doi.org/10.1111/j.1083-6101.2007.00384.x

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers and Security*, *73*, 519–544. https://doi.org/10.1016/j.cose.2017.12.006

Gómez-Chacón, I. M., García-Madruga, J. A., Vila, J. Ó., Elosúa, M. R., & Rodríguez, R. (2014). The dual processes hypothesis in mathematics performance: Beliefs, cognitive reflection, working memory and reasoning. *Learning and Individual Differences*, *29*, 67–73. https://doi.org/10.1016/j.lindif.2013.10.001

Groff, B. D., Baron, R. S., & Moore, D. L. (1983). Distraction, attentional conflict, and drivelike behavior. *Journal of Experimental Social Psychology*, *19*(4), 359–380. https://doi.org/10.1016/0022-1031(83)90028-8

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *SSRN Electronic Journal*, 737–744. https://doi.org/10.2139/ssrn.2383427

Henzinger, M. R., Motwani, R., & Silverstein, C. (2002). Challenges in web search engines. *ACM SIGIR Forum*, *36*(2), 11. https://doi.org/10.1145/792550.792553

Hernández, W., Levy, Y., & Ramim, M. (2016). An empirical assessment of employee cyberslacking in the public sector: The social engineering threat. *Online Journal of Applied Knowledge Management*, *4*(2), 93-109. https://doi.org/10.36965/OJAKM.2016.4(2)93-109

Howard, F., & Komili, O. (2010). Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware. In *Sophos Technical Papers* (Issue March).

John, J. P., Yu, F., Xie, Y., Krishnamurthy, A., & Abadi, M. M. M. M. (2011). deSEO: Combating search-result poisoning. *Proceedings of the 20th USENIX Conference on Security*, 1–15. http://dl.acm.org/citation.cfm?id=2028067.2028087

Kahneman, D. (1973). *Attention and effort*. Prentice Hall, Inc.

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

Kahneman, D., & Tversky, A. (1982). Variants of uncertainty. *Cognition*, *11*(2), 143–157.

https://doi.org/10.1016/0010-0277(82)90023-3

Kallinen, K. (2004). The effects of background music on using a pocket computer in a cafeteria: Immersion, emotional responses, and social richness of medium. *Extended Abstracts on Human Factors in Computing*, 1227–1230. https://doi.org/10.1145/985921.986030

Karakasiliotis, A., Furnell, S. M., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing. *Proceedings of 7th Australian Information Warfare and Security Conference*, 60–72. https://doi.org/10.4225/75/57a80e47aa0cb

Khaddage, F., Christensen, R., Lai, W., Knezek, G., Norris, C., & Soloway, E. (2015). A model driven framework to address challenges in a mobile learning environment. *Education and Information Technologies*, *20*(4), 625–640. https://doi.org/10.1007/s10639-015-9400-x

Kim, D., & Kim, J. H. (2013). Understanding persuasive elements in phishing e-mails. *Online Information Review*, *37*(6), 835–850. https://doi.org/10.1108/OIR-03-2012-0037

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *Proceedings of the APWG ECrime Researchers Summit*, 70–81. https://doi.org/10.1145/1299015.1299022

Larsby, B., Hällgren, M., & Lyxell, B. (2008). The interference of different background noises on speech processing in elderly hearing impaired subjects. *International Journal of Audiology*, *47*(SUPPL. 2), S83–S90. https://doi.org/10.1080/14992020802301159

Leontiadis, N., Moore, T., & Christin, N. (2014). A nearly four-year longitudinal study of search-engine poisoning. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*, 930–941. https://doi.org/10.1145/2660267.2660332

Li, X., Ren, S., Cheng, W., Xiang, L., & Liu, X. (2014). Smartphone: Security and privacy protection. *Pervasive Computing and the Networked World*, 289–302. https://doi.org/10.1007/978-3-319-09265-2_30

Lu, L., Perdisci, R., & Lee, W. (2011). SURF: Detecting and measuring search poisoning. *Proceedings of the 18th ACM Conference on Computer and Communications Security - CCS '11*, 467. https://doi.org/10.1145/2046707.2046762

Mansi, G. (2011). An assessment of instant messaging interruptions on knowledge workers' task performance in e-learning-based training. In *ProQuest Dissertations and Theses UMI Number: 3456433*.

Mansi, G., & Levy, Y. (2013). Do instant messaging interruptions help or hinder knowledge workers' task performance? *International Journal of Information Management*, *33*(3), 591–596. https://doi.org/10.1016/j.ijinfomgt.2013.01.011

Marett, K., & Wright, R. (2009). The effectiveness of deceptive tactics in phishing. *Proceedings of the 15th American Conference on Information Systems, San Francisco, California August 6th-9th*, 1–9.

Mavroeidis, V., & Nicho, M. (2017). Quick response code secure: A cryptographically secure anti-phishing tool for QR code attacks. In J. Rak, J. Bay, I. Kotenko, L. Popyack, V.

Skormin, & K. Szczypiorski (Eds.), *Computer Network Security. MMM-ACNS 2017. Lecture Notes in Computer Science.* (Vol. 10446, pp. 313–324). Springer International Publishing. https://doi.org/10.1007/978-3-319-65127-9_25

McElwee, S., Murphy, G., & Shelton, P. (2018). Influencing outcomes and behaviors in simulated phishing exercises. *Proceedings of the SoutheastCon 2018*, 1–6. https://doi.org/10.1109/SECON.2018.8479109

Metaxas & Pruksachatkun. (2017). Manipulation of search engine results during the 2016 US congressional elections. *Department of Computer Science Wellesley Wellesley College*.

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x

Moore, T., Leontiadis, N., & Christin, N. (2011). Fashion crimes: Trending-term exploitation on the web. *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 455–466. https://doi.org/10.1145/2046707.2046761

Mylonas, A., Gritzalis, D., Tsoumas, B., & Apostolopoulos, T. (2013). A qualitative metrics vector for the awareness of smartphone security users. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8058 LNCS*, 173–184. https://doi.org/10.1007/978-3-642-40343-9_15

Nicholson, D. B., Parboteeah, D. V., Nicholson, J. A., & Valacich, J. S. (2005). Using distraction-conflict theory to measure the effects of distractions on individual task performance in a wireless mobile environment. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, *33c*, 1–9. https://doi.org/10.1109/HICSS.2005.657

Oliveira, D., Ebner, N., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., & Lin, T. (2017). Dissecting spear phishing emails for older vs. young adults. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 6412–6424. https://doi.org/10.1145/3025453.3025831

Pearson, E. (2019). The effects of inhibitory control and perceptual attention on cyber security. In *ProQuest Dissertations and Theses UMI Number: 13423953*.

Pollock, T., Levy, Y., Lei, W., & Kunar, A. (2022). Subject matter experts' feedback on experimental procedures to measure user's judgment errors in social engineering attacks. *Journal of Cybersecurity Education, Research and Practice*, *2022*(2), 1–25.

Reason, J. T. (1990). *Human error* (First). Cambridge University Press.

Rodrigues, P. F. S., & Pandeirada, J. N. S. (2015). Attention and working memory in elderly: The influence of a distracting environment. *Cognitive Processing*, *16*(1), 97–109. https://doi.org/10.1007/s10339-014-0628-y

Sanders, G. S., & Baron, R. S. (1975). The motivating effects of distraction on task performance. *Journal of Personality and Social Psychology*, *32*(6), 956–963. https://doi.org/10.1037/0022-3514.32.6.956

Sanders, G. S., Baron, R. S., & Moore, D. L. (1978). Distraction and social comparison as mediators of social facilitation effects. *Journal of Experimental Social Psychology*, *14*(3), 291–303. https://doi.org/10.1016/0022-1031(78)90017-3

Schneier, B., & West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34–40. https://doi.org/10.1145/1330311.1330320

Shafir, E., Simonson, I., & Tversky, A. (1993). Reason-based choice. *Cognition*, *49*(1–2), 11–36. https://doi.org/10.1016/0010-0277(93)90034-S

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, 373–382. https://doi.org/10.1145/1753326.1753383

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior*, *60*, 35–43. https://doi.org/10.1016/j.chb.2016.02.050

Speier, C., Valacich, J. S., & Vessey, I. (1999). The influence of task interruption on individual decision making: An information overload perspective. *Decision Sciences*, *30*(2), 337–360. https://doi.org/10.1111/j.1540-5915.1999.tb01613.x

Speier, C., Vessey, I., & Valacich, J. S. (2003). The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance. *Decision Sciences*, *34*(4), 771–797. https://doi.org/10.1111/j.1540-5414.2003.02292.x

Steinkamp, M. W. (1980). Relationships between environmental distractions and task performance of hyperactive and normal children. *Journal of Learning Disabilities*, *13*(4), 40–45. https://doi.org/10.1177/002221948001300407

Tay, S. W., Ryan, P. M., & Ryan, C. A. (2016). Systems 1 and 2 thinking processes and cognitive reflection testing in medical students. *Canadian Medical Education Journal*, *7*(2), e97-103. https://doi.org/10.36834/cmej.36777

Tsalis, N., Virvilis, N., Mylonas, A., Apostolopoulos, T., & Gritzalis, D. (2015). Browser blacklists: The utopia of phishing protection. *Communications in Computer and Information Science*, *554*, 278–293. https://doi.org/10.1007/978-3-319-25915-4_15

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

Tversky, A., & Kahneman, D. (1983). Extensional versus intuitive reasoning: The conjunction fallacy in probability judgment. *Psychological Review*, *90*(4), 293–315. https://doi.org/10.1037/0033-295X.90.4.293

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, *5*(4), 297–323. https://doi.org/10.1007/Bf00122574

Unsworth, N., & Robison, M. K. (2016). The influence of lapses of attention on working memory capacity. *Memory and Cognition*, *44*(2), 188–196. https://doi.org/10.3758/s13421-015-0560-0

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013). QRishing: The susceptibility of smartphone users to QR code phishing attacks. In A. A. Adams, M.

Brenner, & M. Smith (Eds.), *Financial Cryptography and Data Security* (pp. 52–69). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-41320-9_4

Virvilis, N., Tsalis, N., Mylonas, A., & Gritzalis, D. (2014). Mobile devices: A phisher's paradise. In M. Obaidat, A. Holzinger, & P. Samarati (Eds.), *Proceedings of the 2014 11th International Conference on Security and Cryptography* (pp. 79–87).

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Vredeveldt, A., & Perfect, T. J. (2014). Reduction of environmental distraction to facilitate cognitive performance. *Frontiers in Psychology*, *5*(4), 1008–1013. https://doi.org/10.3389/fpsyg.2014.00860

Vukelić, B. (2022). Manipulacije rezultatima pretraživanja internetskih tražilica povezanima s cjepivom protiv bolesti COVID-19. *Politehnika*, *6*(1), 29–35. https://doi.org/10.36978/cte.6.1.3

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378–396. https://doi.org/10.1287/isre.2016.0680

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*, *120*(June 2017), 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Wright, P. (1974). The harassed decision maker: Time pressures, distractions, and the use of evidence. *Journal of Applied Psychology*, *59*(5), 555–561. https://doi.org/10.1037/h0037186

Wright, R., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273–303. https://doi.org/10.2753/MIS0742-1222270111

Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., Gavett, B., & Yue, C. (2017). Design and evaluation of the highly insidious extreme phishing attacks. *Computers and Security*, *70*, 634–647. https://doi.org/10.1016/j.cose.2017.08.008

Zijlstra, F. R. H., Roe, R. A., Leonora, A. B., & Krediet, I. (1999). Temporal factors in mental work: Effects of interrupted activities. *Journal of Occupational and Organizational Psychology*, *72*(2), 163–185. https://doi.org/10.1348/096317999166581

Authors Biographies

Tommy Pollock, Ph.D. is the IT programs coordinator for the Tidewater Community College Center for Workforce Development in Suffolk Virginia. He is responsible for the development of IT certification courses and teaching the CompTIA Security+ certification course. He was named a class of 2022 Presidential Management Finalist (PMF) and appointed as a data analytics program analyst with the Bureau of Alcohol, Tobacco, Firearms, and Explosives.

Yair Levy, Ph.D. is a Professor of Information Systems and Cybersecurity at the College of Computing and Engineering at Nova Southeastern University, the Director of the Center for Information Protection, Education, and Research (CIPhER) (https://infosec.nova.edu/), and chair of the Cybersecurity curriculum committee at the college along with serving as the director of the M.S. and Ph.D. programs in Cybersecurity. He conducts innovative research from the 'human factor' of cybersecurity, primarily focusing on social engineering research. Levy authored numerous peer reviewed journal, conference proceedings, book chapters, and other publications. His scholarly research has been cited over 7,200 times. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and FDLE South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics and actively serves as a board member on the South Florida FBI/InfraGard. He consults federal agencies, state and local government groups on cybersecurity topics. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Read more about Dr. Levy via: https://sites.nova.edu/levyy/

Wei Li, Ph.D. joined NSU in 2005, after completing his Ph.D. at Mississippi State University. His research interests include attack modeling and simulation, intrusion detection, firewall management, role-based access control, and the application of AI techniques in various security problems. He is a senior member of IEEE and a member of ACM.

Ajoy Kumar, Ph.D. is an Assistant Professor at NSU and teaches undergraduate courses such as Fundamentals of Programming, Advanced Programming, Data structures, Software Engineering and Web design and Masters courses in Database security and Digital Forensics. Prior to joining NSU, Dr. Kumar was in the IT Industry working as a Senior Software Engineer for almost 20 years. He received his Master of Science degree and Ph.D. in Computer Science from Florida Atlantic University (FAU). His research interests are Security Patterns, Analysis of Secure networks, Firewalls, Intrusion Detection Systems (IDS), Virtual Private Networks (VPN) security and Digital Forensics.