Journal of Cybersecurity Education, Research and Practice

Volume 2021 | Number 2 | Article 4

February 2022

SUBJECT MATTER EXPERTS' FEEDBACK ON EXPERIMENTAL PROCEDURES TO MEASURE USER'S JUDGMENT ERRORS IN SOCIAL ENGINEERING ATTACKS

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

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

Wei Li
Nova Southeastern University, lwei@nova.edu

Ajoy Kumar
Nova Southeastern University, akumar@nova.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/jcerp

Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

Recommended Citation

Pollock, Tommy; Levy, Yair; Li, Wei; and Kumar, Ajoy (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*: Vol. 2021 : No. 2 , Article 4.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/4

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

SUBJECT MATTER EXPERTS' FEEDBACK ON EXPERIMENTAL PROCEDURES TO MEASURE USER'S JUDGMENT ERRORS IN SOCIAL ENGINEERING ATTACKS

Abstract

Distracted users can fail to correctly distinguish the differences between legitimate and malicious emails or search engine results. Mobile phone users can 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 main goal of this research study was to design, develop, and validate a set of field experiments to assess user's 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). In this paper, we provide the results from the Delphi methodology research we conducted using an expert panel consisting of 28 cybersecurity Subject Matter Experts (SMEs) who participated, out of 60 cybersecurity experts invited. Half of the SMEs were with over 10 years of experience in cybersecurity, the rest around five years. SMEs were asked to validate two sets of experimental tasks (phishing & PMSER) as specified in RQ1. The SMEs were then asked to identify physical and Audio/Visual (A/V) environmental factors for distracting and non-distracting environments. About 50% of the SMEs found that an airport was the most distracting environment for mobile phone and computer users. About 35.7% of the SMEs also found that a home environment was the least distracting environment for users, with an office setting coming into a close second place. About 67.9% of the SMEs chose "all" for the most distracting A/V distraction level, which included continuous background noise, visual distractions, and distracting/loud music. About 46.4% of the SMEs chose "all" for the least distracting A/V level, including a quiet environment, relaxing background music, and no visual distractions. The SMEs were then asked to evaluate a randomization table. This was important for RQ2 to set up the eight experimental protocols to maintain the validity of the proposed experiment. About 89.3% indicated a strong consensus that we should keep the randomization as it is. The SMEs were also asked whether we should keep, revise, or replace the number of questions for each mini-IQ test to three questions each. About 75% of the SMEs responded that we should keep the number of mini-IQ questions to three. Finally, the SMEs were asked to evaluate the proposed procedures for the pilot testing and experimental research phases conducted in the future. About 96.4% of the SMEs selected to keep the first pilot testing procedure. For second and third pilot testing procedures, the SMEs responded with an 89.3% strong consensus to keep the procedures. For the first experimental procedure, a strong consensus of 92.9% of the SMEs recommended keeping the procedure. Finally, for the third experimental procedure, there was an 85.7% majority to keep the procedure. The expert panel was used to validate the proposed experimental procedures and recommended adjustments. The conclusions, study limitations, and recommendations for future research are discussed.

Keywords

Cybersecurity, social engineering, judgment error in cybersecurity, phishing email mitigation, distracting environments

This article is available in Journal of Cybersecurity Education, Research and Practice: https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/4

INTRODUCTION

Phishing and malware/ransomware infection from emails, along with Potentially Malicious Search Engine Results (PMSER), inflict significant financial losses to individuals and organizations (Anderson et al., 2013; Choo, 2011; Wright & Marett, 2010). Cybercriminals use increasingly ingenious schemes to take advantage of users' judgment errors when dealing with phishing emails and PMSER (Dhamija et al., 2006; 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 when "the cybercriminal sends an email 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 embedded fake links in the email (Dhamija et al., 2006; 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 the financial accounts of victims (Anderson et al., 2013; Marett & Wright, 2009; 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 (John et al., 2011; Leontiadis et al., 2014). Recently 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, are 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; Tsalis et al., 2015; Virvilis et al., 2014). Mobile phone apps such as Quick Response (QR) code readers also pose a phishing attack vector because of the difficulty differentiating an actual QR code from a hijacked one (Dabrowski et al., 2014; Focardi et al., 2018; Mavroeidis & Nicho, 2017). 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, which poses a situation for making judgment errors in distracting environments (Karakasiliotis et al., 2006). 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 having 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 logical choices in decision making, it often fails due to errors in judgment (Kahneman, 2011). Cybercriminals continue to take advantage of mobile phone or PC user's judgment errors to enrich themselves. A users' vulnerability to phishing attempts is affected by their ability to keep their information secure (Chin et al., 2012; Fette et al., 2007; Li et al., 2014). While there is plenty of 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 (Kumaraguru et al., 2007; Williams et al., 2018). Moreover, it was indicated that "environmental distractions can have an impact on 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 and music (Dalton & Behm, 2007; Larsby et al., 2008; Sanders & Baron, 1975). This distraction will lead to increased vulnerabilities to personal devices and PCs both in public and at work (Halevi et al., 2013; Kallinen, 2004). 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 (Karakasiliotis et al., 2006; Mansi, 2011; Williams et al., 2018). Thus, the main goal of this research study was to design, develop, and validate a set of experiments using an expert panel as a first step, while later in future research, empirically testing the validated 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). The two Research Questions (RQs) that this paper addressed are:

RQ1. What are the specific Subject Matter Experts (SMEs') identified two sets of validated *experimental tasks* to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER)?

RQ2. What are the specific SMEs' identified *eight experimental protocols* to assess the measures of users' judgment 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 device (mobile phone vs. computer)?

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 that they are performing causing detrimental effects on performance, also known as cyberslacking (Alharthi et al., 2019; Brooks, 2015; Hernández et al., 2016). 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; Khaddage et al., 2015; Nicholson et al., 2005). These distractions pose an attention conflict that can overload cognitive function, which reduces performance, leading to difficulty completing tasks (Groff et al., 1983; Kahneman, 1973; Sanders et al., 1978). Interruptions caused by distractions force people to focus elsewhere instead of the task they need to perform (Speier et al., 1999, 2003). The time to complete tasks can be significantly affected by interruptions in the work environment (Bailey et al., 2006; Mansi & Levy, 2013; Zijlstra et al., 1999). Distractions from environmental factors are comparable to person-based interruptions due to work time lost from the disturbance (Sanders et al., 1978; Sanders & Baron, 1975).

Phishing

Phishing scams are among the oldest and widely used social engineering methods to gain personal information and infiltrate organizational systems, mainly for financial gain (Anderson et al., 2013; Marett & Wright, 2009; 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 (Vishwanath et al., 2011; Zhao et al., 2017). PCs are not the only devices susceptible to phishing; mobile phones are also being targeted (Enck, 2011; Goel & Jain, 2018; Vidas et al., 2013). Mobile phones are rich targets for phishing attempts because users take them everywhere and often store personal and financial data (Li et al., 2014; Mylonas et al., 2013). These attempts are becoming more sophisticated using distracting features and persuasive elements (Chiew et al., 2018; Kim & Kim, 2013). 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 (Alarm & El-Khatib, 2016; Moody et al., 2017; Oliveira et al., 2017). Some demographic groups, such as children, teens, and senior citizens, are more susceptible to phishing attacks (Flores et al., 2015; Oliveira et al., 2017; Sheng et al., 2010). Users are targeted at work and private on their computers and mobile phones to gain personal information (Virvilis et al., 2014; Williams et al., 2018). Even with proper training, research provides strong evidence that users still are fall victim to phishing attacks (Albladi & Weir, 2018; Kim & Kim, 2013; Moody et al., 2017). Even corporate controls for phishing prevention often fail (Levy & Gafni, 2021; McElwee et al., 2018; Silic & Back, 2016).

Environmental Factors

Environmental factors affect how users perform tasks in the workplace, at home, and in public (Dalton & Behm, 2007; Kallinen, 2004; Vredeveldt & Perfect, 2014). Background noise negatively affects task performance because it distracts and interrupts users (Dalton & Behm, 2007; Larsby et al., 2008). However, the use of background music has mixed results (Dalton & Behm, 2007; Kallinen, 2004). Instant Messaging (IM) apps in the workplace also pose a distraction in the working environment (Garrett & Danziger, 2007; Mansi, 2011; Mansi & Levy, 2013). These distractions have a negative effect on 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, the decision-making process of users, causing judgment errors (Gómez-Chacón et al., 2014; Speier et al., 2003).

Distracting environments can have a negative effect on working and attentional memory (Awh & Jonides, 2001; Rodrigues & Pandeirada, 2015). Lapses of attention caused by external distractions interrupt task performance by inhibiting the attentive processes of working memory (Berti & Schröger, 2001; Christophel et al., 2017). Rodrigues and Pandeirada (2015) tested the working memory in 40 elderly research participants in distracting and non-distracting environments and found that they 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 (Forster & Lavie, 2008; Steinkamp, 1980; 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 et al., 2015; 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, 1998, 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 can 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 the intuitive thinking (Evans, 2003; 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, 2003, 2008; Evans et al., 2003; Fisk, 2002).

Users are subjected to various distractions when interacting with mobile phones and computers; often, these distractions cause errors in judgment (Ayton & Pascoe, 1995; Chowdhury, 2016; Funder, 1987). 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). Security tends to be a low priority for users unless a problem arises (Schneier & West, 2008). Security 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 develop coping mechanisms when dealing with potential phishing scams (Wang et al., 2017; P. Wright, 1974). 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 real consequences involved with them, depending on the context (Chowdhury, 2016; Funder, 1987).

METHODOLOGY

This study is experimental field research and documents the Expert Panel phases conducted with SMEs to validate the set of experiments. The Expert Panel Research Design Process's proposed model is based on the work of Tracey and Richey (2007), which uses the Delphi technique that uses a panel of SMEs analysis and feedback (See Figure 1). The Delphi technique is a fundamental methodology in situations where accurate information is not available, and expert judgment is needed (Ramim & Lichvar, 2014). The SME panel was used to determine if the two sets of tasks and eight experimental protocols meet understandability, answerability, and readability standards (Ramim & Lichvar, 2014).

SMEs were asked to validate two sets of experimental tasks (phishing & PMSER) as specified in RQ1. This was important to finalize the questions being developed for the mini-IQ tests for the phishing and PMSER experiments. The SMEs were then asked to identify physical and Audio Visual (A/V) environmental factors for distracting and non-distracting environments. This was important towards RQ2 for setting the environment for the questions developed for the mini-IQ tests from RQ1. The SMEs were then asked to evaluate a randomization table, as shown in Figure 1. This was important for RQ2 to set up the eight experimental protocols to maintain the validity of the proposed experiment. Finally, the SMEs were asked to evaluate the proposed procedures for the pilot testing and experimental research phases that will be conducted in the future. This was important to both RQ1 and RQ2 as it incorporates the validated questions from this research study for use in future experimental research.

Data Analysis and Results

Invitation emails to participate in the Subject Matter Expert (SME) survey was sent to about 60 cybersecurity experts along with a social media post on LinkedIn with a goal of 25 respondents. An SME panel of 28 cybersecurity experts participated in this Delphi study, and a consensus was met on the survey questions. Table 1 provides the descriptive statistics of the 28 respondents during the SME responses, which took place from March to May of 2021. The cybersecurity experts ranged from cybersecurity practitioners including network security engineers, Information

Technology (IT) security analysts, information security managers, information technology auditors, cybersecurity administrators, cybersecurity consultants, cybersecurity architects, and senior IT executives. Additionally, professors and researchers in the areas of cybersecurity were among the participants. Over 57.1% of the respondents had over 10 years of experience in cybersecurity and/or information security, followed by 25% at five to 10 years of cybersecurity or information security experience. The rest fell into the five years or less category. While most of the cybersecurity SMEs in senior positions previously worked in various positions in cybersecurity, the SMEs were limited to only entering one current profession for the survey.

Table 1

Descriptive Statistics of SMEs (N=28)

Survey Question	Frequency	Percentage
Professional role:		
Network Security or Cybersecurity Engineer	3	10.7
Cybersecurity, Information Security, or Information Technology Security Analyst	8	28.6
Information Security Manager	3	10.7
Information Technology Auditor	1	3.6
Cybersecurity Administrator	0	0
Cybersecurity Consultant	0	0
Cybersecurity Architect	0	0
Other	10	35.7
Experience in Information Security:		
10 years or more	16	57.1
At least five years, but less than 10 years	7	25
At least three years, but less than five years	2	7.1
At least one year, but less than three years	1	3.6
Less than one year	1	3.6
No Experience	1	3.6
Number of cybersecurity certifications:		
None	15	53.6
One	4	14.3
Two	4	14.3
Three	2	7.1
Four or more	3	10.7

As shown in Appendix A, the SMEs were asked to evaluate 12 sample emails for use in the mini-IQ tests for the proposed experimental research. They were asked to evaluate each email sample and answer, as shown in Table 2, if the email sample was legitimate, phishing, or unsure. The sample emails were a mixture of legitimate and various degrees of difficulty levels for the phishing emails (easy, medium, and hard). As indicated in Table 2, some of the email samples had a higher level of unsure responses as the difficulty increased.

Table 2

SME Feedback on Email Samples for Proposed IQ Testing (N=28)

Email Phishing Sample	Frequency	Percentage
Please identify the sample email above as one of the following: Legitimate, Phishing, or Unsure		
Sample 1		
Legitimate	1	3.6
Phishing	27	96.4
Unsure	0	0
Sample 2		
Legitimate	13	46.4
Phishing	12	42.9
Unsure	3	10.7
Sample 3		
Legitimate	10	35.7
Phishing	4	14.3
Unsure	14	50
Sample 4		
Legitimate	1	3.6
Phishing	24	85.7
Unsure	3	10.7
Sample 5		
Legitimate	2	7.1
Phishing	24	85.7
Unsure	2	7.1
Sample 6		
Legitimate	18	64.3
Phishing	3	10.7
Unsure	7	25
Sample 7		
Legitimate	17	60.7
Phishing	6	21.4
Unsure	5	17.9
Sample 8		
Legitimate	8	28.6
Phishing	18	64.3
Unsure	2	7.1
Sample 9		
Legitimate	9	32.1
Phishing	7	25
Unsure	12	42.9
Sample 10		
Legitimate	0	0
Phishing	28	100

Email Phishing Sample	Frequency	Percentage
Unsure	0	0
Sample 11		
Legitimate	6	21.4
Phishing	16	57.1
Unsure	6	21.4
Sample 12		
Legitimate	5	17.9
Phishing	18	64.3
Unsure	5	17.9

The SMEs were also asked to provide feedback on whether to keep, revise, or replace the sample emails they evaluated from Table 2. As shown in Table 3, most of the SMEs chose to keep all of the email samples. The SMEs were also asked to provide feedback on why they chose the revise or replace options and any additional feedback that might improve the email samples. Some vital feedback on the revisions came from the over 60 age group on adjusting the image quality on two samples to be more readable for all participants.

Table 3

SME Feedback on Email Sample Edits (N=28)

Email Phishing Sample	Frequency	Percentage
Please provide your expert opinion about the email sample above by indicating: Keep, Revise, or Replace		
Sample 1		
Keep	21	75
Revise	6	21.4
Replace	1	3.6
Sample 2		
Keep	23	82.1
Revise	2	7.1
Replace	3	10.7
Sample 3		
Keep	20	71.4
Revise	7	25
Replace	1	3.6
Sample 4		
Keep	25	89.3
Revise	1	3.6
Replace	2	7.1
Sample 5		
Keep	22	78.6
Revise	3	10.7
Replace	3	10.7
Sample 6		

Email Phishing Sample	Frequency	Percentage
Keep	25	89.3
Revise	2	7.1
Replace	1	3.6
Sample 7		
Keep	22	78.6
Revise	5	17.9
Replace	1	3.6
Sample 8		
Keep	21	75
Revise	6	21.4
Replace	1	3.6
Sample 9		
Keep	14	50
Revise	8	28.6
Replace	6	21.4
Sample 10		
Keep	26	92.9
Revise	1	3.6
Replace	1	3.6
Sample 11		
Keep	23	82.1
Revise	2	7.1
Replace	3	10.7
Sample 12		
Keep	26	92.9
Revise	1	3.6
Replace	1	3.6

The SMEs were asked to evaluate 12 PMSER samples as shown in Appendix B for future experimental research use in the mini-IQ tests. They were asked to evaluate whether each PMSER sample and answer, as shown in Table 4, if the PMSER was legitimate, potentially malicious, or if they were unsure. The PMSER samples were a mixture of legitimate and various degrees of difficulty levels for the PMSER samples (easy, medium, and hard).

Table 4

SME Feedback on PMSER Samples for Proposed IQ Testing (N=28)

PMSER Sample	Frequency	Percentage
Please identify the sample PMSER above as one of the following: Legitimate, Potentially Malicious, or Unsure		
Sample 1		
Legitimate	3	10.7
Potentially Malicious	22	78.6
Unsure	3	2.7
Sample 2		

PMSER Sample	Frequency	Percentage
Legitimate	13	36.4
Potentially Malicious	12	42.9
Unsure	3	10.7
Sample 3		
Legitimate	8	28.6
Potentially Malicious	14	50
Unsure	6	21.4
Sample 4		
Legitimate	21	75
Potentially Malicious	5	17.9
Unsure	2	7.1
Sample 5		
Legitimate	6	21.4
Potentially Malicious	16	57.1
Unsure	6	21.4
Sample 6		
Legitimate	7	25
Potentially Malicious	20	71.4
Unsure	1	3.6
Sample 7		
Legitimate	22	7.8
Potentially Malicious	4	14.3
Unsure	2	7.1
Sample 8		
Legitimate	5	17.9
Potentially Malicious	20	17.9
Unsure	3	10.7
Sample 9		
Legitimate	21	75
Potentially Malicious	6	21.4
Unsure	1	3.6
Sample 10		
Legitimate	21	75
Potentially Malicious	4	14.3
Unsure	3	10.7
Sample 11		
Legitimate	25	89.3
Potentially Malicious	2	7.1
Unsure	1	3.6
Sample 12		
Legitimate	10	35.7
Potentially Malicious	15	53.6
Unsure	3	10.7

The SMEs were also asked to provide feedback on whether to keep, revise, or replace the PMSER samples they evaluated from Table 4. As shown in Table 5, most of the SME’s chose to keep all of the PMSER samples. The SMEs were also asked to provide feedback on why they chose the revise or replace options and any additional feedback that might improve the PMSER samples. As with the sample email feedback on the revisions, we will adjust the image quality on all samples to be more readable for all participants.

Table 5

SME Feedback on PMSER Sample Edits (N=28)

PMSER Sample	Frequency	Percentage
Please provide your expert opinion about the PMSER sample above by indicating: Keep, Revise, or Replace		
Sample 1		
Keep	26	92.9
Revise	1	3.6
Replace	1	3.6
Sample 2		
Keep	23	82.1
Revise	3	10.7
Replace	2	7.1
Sample 3		
Keep	25	89.3
Revise	2	7.1
Replace	1	3.6
Sample 4		
Keep	25	89.3
Revise	1	3.6
Replace	2	7.1
Sample 5		
Keep	19	67.9
Revise	7	25
Replace	2	7.1
Sample 6		
Keep	25	89.3
Revise	2	7.1
Replace	1	3.6
Sample 7		
Keep	24	85.7
Revise	3	10.7
Replace	1	3.6
Sample 8		
Keep	25	89.3
Revise	2	7.1
Replace	1	3.6
Sample 9		
Keep	27	96.4
Revise	0	0

PMSER Sample	Frequency	Percentage
Replace	1	3.6
Sample 10		
Keep	27	96.4
Revise	0	0
Replace	1	3.6
Sample 11		
Keep	27	96.4
Revise	0	0
Replace	1	3.6
Sample 12		
Keep	25	89.3
Revise	1	3.6
Replace	2	7.1

The SMEs were asked to evaluate the topmost and least distracting environments for mobile phone and computer users. Table 6 indicates that about 50% of the SMEs found that an airport was the most distracting environment for mobile phone and computer users. About 35.7% of the SMEs also found that a home environment was the least distracting for mobile phone and computer users, with an office setting coming into a close second place.

Table 6

SME Feedback of Physical Distracting Environments (N=28)

Environment	Frequency	Percentage
Which physical environment provides the most distracting environment for Mobile Phones and Computers?		
Airport	14	50
Coffee Shop	5	17.9
Lecture Hall	0	0
Meeting	9	32.1
Which physical environment provides the least distracting environment for Mobile Phones and Computers?		
Office Setting	8	28.6
Home	10	35.7
Hotel room	6	21.4
Library/Bookstore	4	14.3

The SMEs were asked to evaluate the topmost and least Audio/Visual (A/V) distraction levels for mobile phone and computer users. Table 7 shows that about 67.9% of the SMEs chose all of the above for the most distracting A/V distraction level, including continuous background noise, visual distractions, and distracting/loud music. About 46.4% of the SMEs chose all of the above for the most distracting A/V distraction level, including a quiet environment, relaxing background music, and no visual distractions.

Table 7

SME Feedback of A/V Distraction Levels (N=28)

A/V Distraction Level	Frequency	Percentage
Which audio/visual distraction level is best for a distracting environment for Mobile Phones and Computers?		
Continuous Background Noise	3	10.7
Visual Distractions	4	14.3
Distracting/Loud Music	2	7.1
All of the above	19	67.9
Which audio/visual distraction level is best for a non-distracting environment for Mobile Phones and Computers?		
A Quiet Environment	7	25
Relaxing Background Music	5	19.9
No visual distractions	3	10.7
All of the above	13	46.4

The SMEs were asked to evaluate the randomization table in Figure 1 and provide feedback on whether to keep, revise, or replace the randomization. About 89.3% indicated that we should keep the randomization as it is. The SMEs were also asked whether we should keep, revise, or replace the number of questions for each mini-IQ test to three questions each. About 75% of the SMEs responded that we should keep the number of mini-IQ questions to three. As with the email and PMSER sample questions, the SMEs were asked to provide feedback on why they chose the revised or replace options and any additional feedback that might improve the randomization and question size.

Table 2

SME Feedback on Mini IQ Test Randomization (N=28)

Question	Frequency	Percentage
Please provide your expert opinion about the randomization table above by indicating:		
Keep	25	89.3
Revise	1	3.6
Replace	2	7.1
The proposed mini-IQ tests will consist of three questions, each using the randomization table above. Please provide your expert opinion about the randomization and size of the mini-IQ tests by indicating:		
Keep	21	75
Revise	6	21.4
Replace	1	3.6

Figure 1 indicates the proposed question randomization for the email and PMSER questions given to the pilot study participants and the main research study participants. Randomization was necessary to maintain the quality and the validity of the research study. The difficulty of the phishing and PMSER questions is evenly distributed to reduce the chance that all easy questions are asked in non-distracting environments and all hard questions being asked in distracting environments.

Figure 1

Social Engineering Attack Type Randomization Table

Social Engineering Attack Type

Phishing

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

PMSER

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

The SMEs were asked to provide feedback on the pilot and experimental testing procedures, as shown in Table 9, whether to keep, revise, or replace each procedure. For the pilot-testing procedures, 96.4% of the SMEs selected to keep the first pilot testing procedure. For the second and third pilot testing procedures, the SMEs responded with an 89.3% majority to keep the procedures. For the first experimental procedure, 92.9% of the SMEs chose to keep the procedure. The second experimental procedure had an 89.3% majority for keeping the procedure. Finally, for the third experimental procedure, there was an 85.7% majority to keep the procedure. The SMEs that chose to revise or replace asked to provide feedback on why they chose to revise or replace options on all of the procedures and any additional feedback that might improve the testing procedures.

Table 3

Pilot Testing and Experimental Testing Procedures

Experimental Testing Procedure	Frequency	Percentage
Pilot Experimental Procedure 1: Post invitation on social media such as LinkedIn		
Keep Revise Replace	27 0 1	96.4 0 3.6
Pilot Experimental Procedure 2: Email interested pilot testing participants a zoom meeting link to conduct pilot testing and assign each a participant ID.		
Keep Revise Replace	25 2 1	89.3 7.1 3.6
Pilot Experimental Procedure 3: Pilot test participants will be given links to the mini-IQ tests to complete while in a monitored simulated environment (distracting or non-distracting) via Zoom. Each participant will be asked to enter their assigned participant ID for each IQ test for data tracking purposes.		
Keep Revise Replace	25 2 1	89.3 7.1 3.6
Main Experimental Procedure 1: Post invitation on testing site organizational website and via organizational email.		
Keep Revise Replace	26 0 2	92.9 0 7.1
Main Experimental Procedure 2: Email interested experimental testing participants a zoom meeting link to conduct experimental testing and assign each a participant ID.		
Keep Revise Replace	25 2 1	89.3 7.1 3.6
Main Experimental Procedure 3: Experimental test participants will be given links to the mini-IQ tests to complete while in a monitored simulated environment (distracting or non-distracting) via Zoom. Each participant will be asked to enter their assigned participant ID for each IQ test for data tracking purposes.		
Keep Revise Replace	24 2 2	85.7 7.1 7.1

CONCLUSIONS AND DISCUSSIONS

This study presents the results of SMEs validation process of two sets of validated experimental tasks to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER), and eight experimental protocols to assess the measures of 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), used to gain access to an individual's personal or organizational accounts, mainly for monetary gain (Anderson et al., 2013; Leontiadis et al., 2014). With the widespread use of mobile phones with Internet-connected applications, phishing attempts have increased through social engineering through scams and clickbait links (Frauenstein & Flowerday, 2016; Halevi et al., 2013; Marett & Wright, 2009). 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 a person to discern between genuine and malicious links making them more susceptible to phishing attacks (Frauenstein & Flowerday, 2016; Vishwanath et al., 2011). 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 (Groff et al., 1983; Reason, 1995; Sanders & Baron, 1975). Attackers craft phishing attacks to try and distort the mental model that users form in interacting with online transactions and distract them from the visual cues they usually pick up on (Downs et al., 2006). As the number of distractions increases, cognitive cues decrease, affecting decision-making due to cognitive overload (Groff et al., 1983; Kahneman, 1973; Speier et al., 1999). We feel that the results of this study will provide significant input to the body of knowledge of users' susceptibility to social engineering attacks in distracting environments while using mobile phones and computers.

Like any research study, this study has several limitations. The main limitation of this expert panel research study is relying on the SME opinions provided during the Delphi technique. SME panel participants are often volunteers who can withdraw from the study for many reasons, negatively impacting the research (Ellis & Levy, 2010). By combining the Delphi technique with a review of the literature, we mitigated such limitations. Our recruitment of SMEs from varying industries and academia also helped mitigate this limitation.

Future research will use the validated set of experiments to collect and analyze data to find if any significant mean differences exist in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) and the two types of distracting environments while using mobile phones or desktop/laptop computers. Prior literature indicated that various demographic indicators such as age, gender, education, and level of social media usage, also play a role in phishing judgemental errors (Frauenstein & Flowerday, 2016; Sheng et al., 2010). Thus, additional assessments of the experimental data with the interaction of the different demographic indicators may help further uncover potential groups that are more susceptive to social engineering attacks.

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

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*(03), 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

Enck, W. (2011). Defending users against smartphone apps: Techniques and future directions. *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, judgment, 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

Federal Bureau of Investigation (FBI) (2020). Internet crime report 2020. *Internet Crime Complaint Center (IC3)*. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

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*(November 2018), 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 twodimensional 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? *2016 Information Security for South Africa - Proceedings of the 2016 ISSA 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

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal*, *2544742*, 1–10. https://doi.org/10.2139/ssrn.2544742

Hara, M., Yamada, A., & Miyake, Y. (2009). Visual similarity-based phishing detection without victim site information. *2009 IEEE Symposium on Computational Intelligence in Cyber Security*, 30–36. https://doi.org/10.1109/CICYBS.2009.4925087

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.

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 emails. *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. *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

Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security*, 1-13. https://doi.org/10.1108/ICS-04-2020-0054

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

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 Fifteenth AMCIS, San Francisco, California August 6th-9th 2009*, 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. *SoutheastCon 2018*, 1–6. https://doi.org/10.1109/SECON.2018.8479109

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

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*, *00*(C), 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*.

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

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 - CHI '10*, 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

Tracey, M. W., & Richey, R. C. (2007). ID model construction and validation: A multiple intelligences case. *Educational Technology Research and Development*, *55*(4), 369–390. https://doi.org/10.1007/s11423-006-9015-4

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/Doi 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.), *2014 11th International Conference on Security and Cryptography (SECRYPT)* (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

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, *17*(11), 759–783.

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

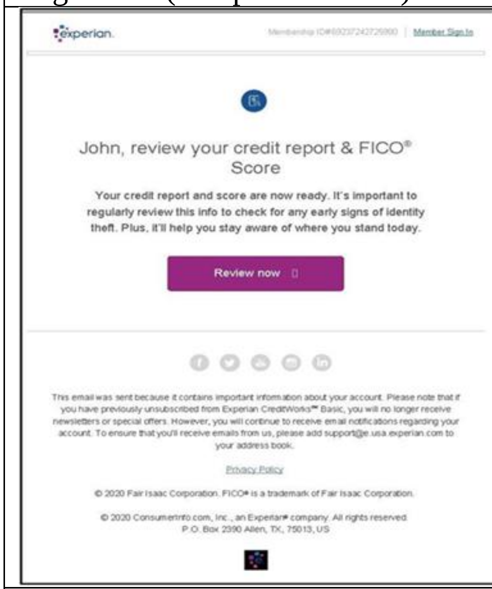
Wright, R., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273–303. https://doi.org/10.2753/MIS0742-1222270111

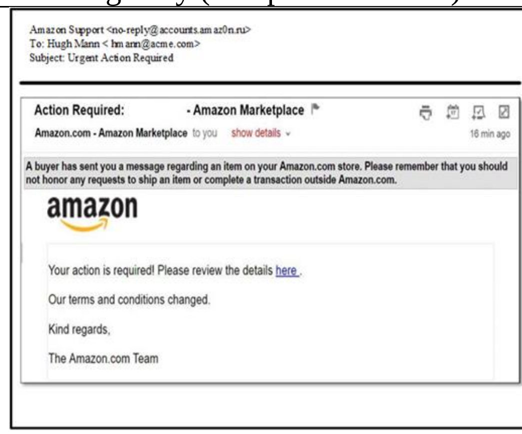
Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., Gavett, B., & Yue, C. (2017). Design and evaluation of the highly insidious extreme phishing attacks. *Computers and Security*, *70*, 634–647. https://doi.org/10.1016/j.cose.2017.08.008

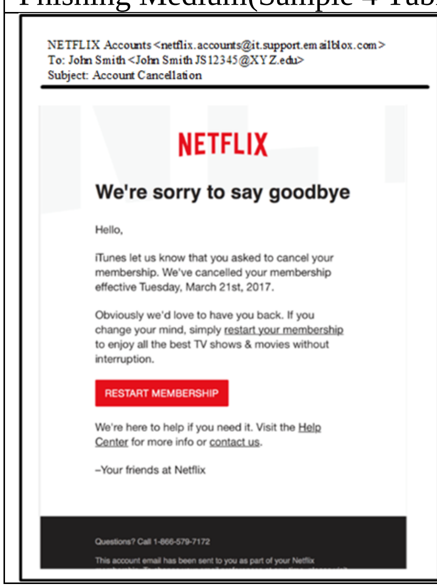
Zijlstra, F. R. H., Roe, R. A., Leonora, A. B., & Krediet, I. (1999). Temporal factors in mental work: Effects of interrupted activities. *Journal of Occupational and Organizational Psychology*, *72*(2), 163–185. https://doi.org/10.1348/096317999166581

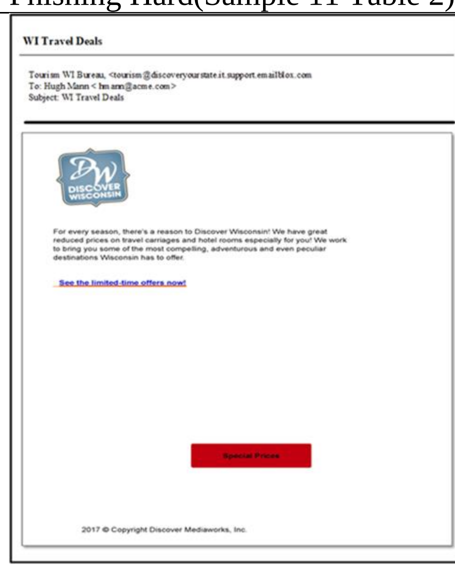
Appendix A

SME Survey Phishing Email Samples

<table>
<tr><td>Legitimate (Sample 3 Table 2)</td><td>Phishing Easy (Sample 10 Table 2)</td></tr>
<tr><td>


</td><td>


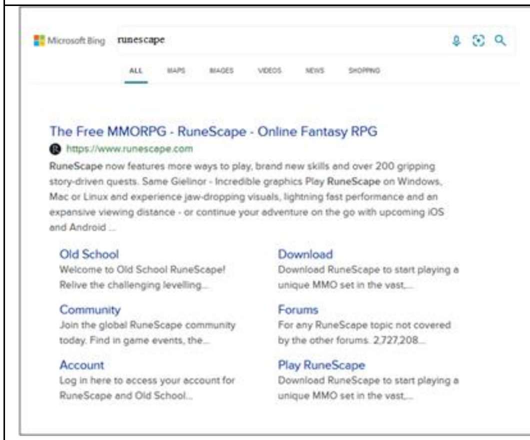
</td></tr>
<tr><td>Phishing Medium(Sample 4 Table 2)</td><td>Phishing Hard(Sample 11 Table 2)</td></tr>
<tr><td>


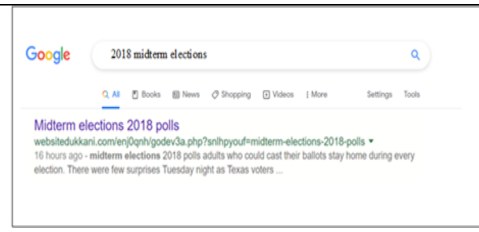
</td><td>


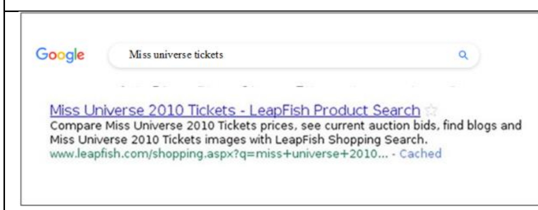
</td></tr>
</table>

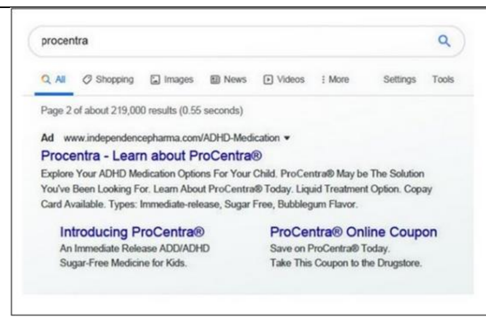
Appendix B

SME Survey PMSER Samples

<table>
<tr><td>Legitimate (Sample 10 Table 4)</td><td>PMSER Easy (Sample 8 Table 4)</td></tr>
<tr><td>


</td><td>


</td></tr>
<tr><td>PMSER Medium (Sample 2 Table 4)</td><td>PMSER Hard (Sample 12 Table 4)</td></tr>
<tr><td>


</td><td>


</td></tr>
</table>