Towards an Assessment of Judgment Errors in Social Engineering Attacks Due to Environment and Device Type

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

Yair Levy  
*Nova Southeastern University*, 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/ccerp](https://digitalcommons.kennesaw.edu/ccerp)

Part of the Information Security Commons

Pollock, Tommy; Levy, Yair; Li, Wei; and Kumar, Ajoy, "Towards an Assessment of Judgment Errors in Social Engineering Attacks Due to Environment and Device Type" (2020). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 3.  
[https://digitalcommons.kennesaw.edu/ccerp/2020/Research/3](https://digitalcommons.kennesaw.edu/ccerp/2020/Research/3)

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.
Abstract
Phishing continues to be a significant invasive threat to computer and mobile device users. Cybercriminals continuously develop new phishing schemes using email, and malicious search engine links to gather personal information of unsuspecting users. This information is used for financial gains through identity theft schemes or draining financial accounts of victims. Users are often distracted and fail to fully process the phishing attacks then unknowingly fall victim to the scam until much later. Users operating mobile phones and computers are likely to make judgment errors when making decisions in distracting environments due to cognitive overload. Distracted users can fail to correctly distinguish the differences between legitimate and malicious emails or search engine results. Mobile phone users can have even a harder 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 work-in-progress research study is to design, develop, and validate a set of field experiments to assess users judgment when exposed to two types of simulated social engineering attacks (phishing & possibly 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). In this paper, we outlines the Delphi methodology phase that this study will take using an expert panel to validate the proposed experimental procedures and recommend further steps for the empirical testing. The conclusions, study limitations and recommendations for future research are discussed.

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

Location
Zoom Session 1 (Main Papers Track)

Disciplines
Information Security
INTRODUCTION

Phishing and malware/ransomware infection from e-mails, 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 e-mails and PMSER (Dhamija et al., 2006; Leontiadis et al., 2014). Phishing is a subcategory of Social Engineering and is defined as “a type of cyber attack that sits at the intersection of social engineering and security technologies” (McElwee et al., 2018, p. 1). These phishing schemes often use official-looking logos to distract the target from the spelling inconsistencies or embedded fake links in the e-mail (Dhamija et al., 2006; Wright & Marett, 2010). Phishing continues to be an invasive threat to computer and mobile device users (McElwee et al., 2018). Cybercriminals continuously develop new phishing schemes using e-mail and malicious search engine links to gather personal information of unsuspecting users (Anderson et al., 2013). This information is used for financial gains through identity theft schemes or draining financial accounts of victims (Anderson et al., 2013; Marett & Wright, 2009; Moody et al., 2017).

Deceptive search engine results pose a problem 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). 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 in differentiating a real QR code from a hijacked one (Dabrowski et al., 2014; Focardi et al., 2018; Mavroeidis & Nicho, 2017). Mobile phones are often the primary platform utilized by users nowadays to access various web-based platforms, exposing them to phishing and clickbait schemes (Frauenstein & Flowerday, 2016). Users tend to take their mobile phones 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 e-mails and web links on their PC, being a desktop or laptop (Furnell, 2007).
Overconfidence in one’s abilities and failure to recognize the risks of phishing campaigns leads to judgmental errors (Schneier & West, 2008; Vishwanath et al., 2011; Wang et al., 2016). Judgment errors have been documented in research to cause users to fall prey to cybercriminals (Schneier & West, 2008; Vishwanath et al., 2011; Wang et al., 2016). People judge different events with a degree of uncertainty that can lead to judgmental errors (Kahneman & Tversky, 1982; Tversky & Kahneman, 1974, 1983). With the sophistication of the current phishing schemes, intuitive thinking often fails because people miss visual cues due to being distracted by various visual or audible elements in the environment (Nicholson et al., 2005; Wright, 1974).

While logical thinking provides the ability to make logical choices in decision making, it often fails as well 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 are 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 e-mails 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 as well as 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 work-in-progress research study is to design, develop, and validate a set of experiments using an expert panel as a first step, while later empirically testing the validated set of experiments with participants to assess if there are significant mean differences in users judgment, when: exposed to two types of simulated social engineering attacks (phishing & 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 will discuss include:

https://digitalcommons.kennesaw.edu/ccerp/2020/Research/3
RQ1. What are the specific Subject Matter Experts’ 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 (Halevi et al., 2013). 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 a person to focus elsewhere instead of the task that 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 the person based interruptions due to work time lost from the disturbance (Sanders et al., 1978; Sanders & Baron, 1975).

Phishing

Phishing scams are one of 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. 3).
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 with them and often store personal and financial data on them (Li et al., 2014; Mylonas et al., 2013). These attempts are becoming more sophisticated with the use of distracting features and persuasive elements (Chiew et al., 2018; Kim & Kim, 2013). The content of these messages often disguised as legitimate companies and contain rational, emotional, and motivationally appealing elements that tempt users to click on links in an attempt to gain their personal information to steal their identity or their financial assets (Kim & Kim, 2013).

QR codes pose an increased risk of falling for phishing scams on mobile phones (Dabrowski et al., 2014; Vidas et al., 2013). QR codes are subject to manipulation by cybercriminals, which can direct the mobile phone to a phishing website (Mavroeidis & Nicho, 2017; Vidas et al., 2013). These QR codes use Uniform Resource Locator (URL) shorteners to hide the URL name and their identities (Dabrowski et al., 2014; Frauenstein & Flowerday, 2016; Mavroeidis & Nicho, 2017). The cybercriminals use this method to try and gain sensitive information from users (Focardi et al., 2018).

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 also more susceptible than others to phishing attacks (Flores et al., 2015; Oliveira et al., 2017; Sheng et al., 2010). Users are targeted at work and in private on their computers and mobile phones to gain personal information (Virvilis et al., 2014; E. J. 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 put into place for phishing prevention often fail (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 tends to have a negative effect on task performance because it distracts and interrupts users (Dalton & Behm, 2007; Larsby et al., 2008). The use of background music, however, has mixed results (Dalton & Behm, 2007; Kallinen, 2004). The use of 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. They 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 e-mails as a means of distracting the recipient away from other details that may give away the true nature of the e-mail (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 the reasons that 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 only 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 that can be 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 e-mails leading to potential judgment errors (Furnell, 2007; Karakasiliotis et al., 2006). Many users make a judgment on visual and technical cues in phishing e-mails and will often not be able to detect phishing attempts (Karakasiliotis et al., 2006). Habitually reading e-mails 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 proposed study will be an experimental field research. This phase of the work-in-progress study documents the Expert Panel phases that will be conducted with SMEs to validate the set of experiments before moving to the next phases of the study. The proposed model of the Expert Panel Research Design Process 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 an essential methodology in situations where accurate information is not available, and expert judgment is needed (Ramim & Lichvar, 2014). The SME panel will be used to determine if the two sets of tasks and eight experimental protocols meet understandability, answerability, and readability standards (Ramim & Lichvar, 2014).

Phase 1 of this proposed experimental research study will utilize an SME-review process following the Delphi technique, along with prior research to design and validate the SMEs identified two sets of tasks to assess users’ judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). Phase 2 of this proposed study will also utilize the SME-review process following the Delphi technique to design and validate the SMEs’ identified eight experimental protocols to assess users’ judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER), two types of environment (distracting vs. non-distracting) and two types of device used (mobile phone vs. computer).
The validity of this experimental research builds on prior research by Dhamija et al. (2006), Halevi et al. (2015), Hara et al. (2009), Karakasiliotis et al. (2006), Sheng et al. (2010), as well as Frauenstein and Flowerday (2016). Dhamija et al. (2006) were able to fool many knowledgeable users with simple spoofing techniques. They demonstrated that even the most knowledgeable users could make judgment errors when confronted with simple phishing schemes. Halevi et al. (2015) found that users are not aware of their vulnerabilities to attacks, especially those that relied heavily on social media usage. The popularity of social media services has made it even easier for cybercriminals to post fake links to gather personal information from a wide array of demographical groups (Frauenstein & Flowerday, 2016). Heavy social media usage is a possible demographic indicator in assessing user judgment errors. Sheng et al. (2010) found that demographic factors such as gender and age play a role in a user being susceptible to falling for a phishing scheme. These factors can vary with the amount of education or perception of financial risk. Karakasiliotis et al. (2006) noted that while users often use several factors such as language, technical cues, and visual elements to judge the legitimacy of an e-mail, they often make incorrect decisions. Cybercriminals will often use visual similarities to imitate legitimate companies and websites to fool people into falling victim to their phishing schemes (Hara et al., 2009). Figure
2 illustrates this study's proposed 2X2X2 experimental design taxonomy between devices in distracting and non-distracting environments during interaction with two types of social engineering attacks (phishing & PMSER).

In order to protect the validity of the experimental study, the research participants will be informed of the significance of social engineering attacks, including phishing and PMSER. Along with the fact that they will be asked to distinguish between valid and non-valid phishing examples and PMSER, but will not be informed on the exact comparisons of the environment type and device type (Finn & Jakobsson, 2007; Parsons et al., 2015). Parsons et al. (2015) found that when participants are informed of the nature of the phishing experiment, they had a significant discrimination rate above the participants that were not told.

Figure 2

Proposed 2x2x2 Experimental Design Taxonomy of Device (Mobile Phone/Computer) vs. Environment (Distracting/Non-Distracting) vs. Social Engineering Attack Type (Phishing/PMSER)

<table>
<thead>
<tr>
<th>Social Engineering Attack Type</th>
<th>Phishing</th>
<th>PMSER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>Distracting</td>
<td>Non-Distracting</td>
</tr>
<tr>
<td>Device</td>
<td>Mobile Phone</td>
<td>Computer</td>
</tr>
<tr>
<td>Distracted via Mobile Phone</td>
<td>Not Distracted via Mobile Phone</td>
<td></td>
</tr>
<tr>
<td>Distracted via Computer</td>
<td>Not Distracted via Computer</td>
<td></td>
</tr>
</tbody>
</table>

Device Mobile Phone

Mobile Phone

Distracted via Mobile Phone

Distracted via Computer

Computer

Distracted via Computer

Not Distracted via Computer

This part of the research has two specific goals. The first specific goal is to identify and validate, using SMEs, two sets of experimental tasks for the measures of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). The second specific goal is to identify and validate, using SMEs, 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).

**Experimental Tasks and Measures**

The first draft of the experimental tasks and research protocols were developed through the exploration of current literature from empirical research databases from varying fields of study, such as IS, Cybersecurity, Psychology, and Finance. Phishing IQ and PMSER IQ tests (Table 1) were developed based on previous research to include a mixture of phishing and e-mails, along with potentially malicious and legitimate SE links.

**Table 1**

**Phishing and PMSER IQ Test Constructs and Measures used in Experimental Research Study**

<table>
<thead>
<tr>
<th>IQ Test Number</th>
<th>IQ Test Type</th>
<th>IQ Test Topic</th>
<th>IQ Test Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>PH-IQ-01</td>
<td>Phishing IQ Test</td>
<td>E-mail from the FBI about a banking transaction.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-02</td>
<td>Phishing IQ Test</td>
<td>E-mail alert from Microsoft about login activity on account.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-03</td>
<td>Phishing IQ Test</td>
<td>E-mail alert from Experian about a change to a credit report.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-04</td>
<td>Phishing IQ Test</td>
<td>E-mail alert from NETFLIX about account cancellation.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-05</td>
<td>Phishing IQ Test</td>
<td>Reminder e-mail from PayPal about security upgrades to their system.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-06</td>
<td>Phishing IQ Test</td>
<td>E-mail from Audible about a free audiobook service for kids.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-07</td>
<td>Phishing IQ Test</td>
<td>E-mail alert from Google showing a new sign in to account.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-08</td>
<td>Phishing IQ Test</td>
<td>E-mail alert from Citibank stating that the account was locked out due to three failed login attempts.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-09</td>
<td>Phishing IQ Test</td>
<td>Payment receipt from MCPROHOSTING for server space rental.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PH-IQ-10</td>
<td>Phishing IQ Test</td>
<td>E-mail alert from Amazon regarding an item selling through their website.</td>
<td>Legitimate or phishing e-mail</td>
</tr>
<tr>
<td>PM-IQ-01</td>
<td>PMSER IQ Test</td>
<td>Search results for Motillum using a search engine browser.</td>
<td>Legitimate or possibility malicious link</td>
</tr>
<tr>
<td>IQ Test Number</td>
<td>IQ Test Type</td>
<td>IQ Test Topic</td>
<td>IQ Test Measure</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>PM-IQ-02</td>
<td>PMSER IQ Test</td>
<td>Search results for tickets for the 2010 Miss Universe pageant using a search</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td>engine browser.</td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-03</td>
<td>PMSER IQ Test</td>
<td>Search results for the term blockchain using a search engine browser.</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-04</td>
<td>PMSER IQ Test</td>
<td>Search results for hotels for an upcoming trip to Berlin, Germany using a</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td>search engine browser.</td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-05</td>
<td>PMSER IQ Test</td>
<td>Search results for killer whales at SeaWorld using a search engine browser.</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-06</td>
<td>PMSER IQ Test</td>
<td>Search results for the malwaretips website using a search engine browser.</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-07</td>
<td>PMSER IQ Test</td>
<td>Search results for camping gear using a search engine browser.</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-08</td>
<td>PMSER IQ Test</td>
<td>Searched results for the 2018 midterm elections using a search engine browser</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-09</td>
<td>PMSER IQ Test</td>
<td>Search results for COVID-19 using a search engine browser.</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>link</td>
</tr>
<tr>
<td>PM-IQ-10</td>
<td>PMSER IQ Test</td>
<td>Search results for the RuneScape download website using a search engine browser.</td>
<td>Legitimate or possibility malicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>link</td>
</tr>
</tbody>
</table>

A proposed sample size of 25 cybersecurity SMEs for the Delphi rounds will be recruited via e-mail and a LinkedIn recruitment post to get a larger sample size. To reach the desired sample size, up to 40 SMEs will be recruited via e-mail and social media. The recruited SMEs will be from the cybersecurity field in industry and academia to provide a better diversity of skills and experience following the recommendation of Kennedy (2004) as well as Ramim and Lichvar (2014). The recruited SMEs will provide input for the experimental research design process, as shown in Figure 1, the two sets of experimental tasks, and eight proposed research protocols, as shown in Figure 2.

The proposed administrative approach of the experimental tasks and research protocols will be collected via e-mail using web-based Google forms based on a
scoring scale for the SMEs Delphi rounds. The SME input from each round will be recorded, and changes to the experimental tasks and protocols will be made based on the weight of the feedback based on the scale before the next round. The experimental tasks and research protocols for this proposed research study (Figure 1) will be validated using the Delphi methodology by recruiting SMEs from the field of cybersecurity. The Delphi methodology consists of a group communications process involving SMEs to provide SME feedback on a specific subject (Ramim & Lichvar, 2014). This proposed research study will conduct several rounds of SMEs elicitations to ensure consensus while developing a) SMEs identified two sets of validated experimental tasks that need to be measured, and b) SMEs identified four experimental protocols. The SMEs Delphi rounds will be used to develop two sets of experimental tasks (Figure 3) for the measures of users’ judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). These two experimental tasks will be based on SMEs’ identified eight experimental protocols to assess the measures of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER), during two types of environments (distracting vs. non-distracting), and two types of device (mobile phone vs. computer).

**Figure 3**

*Two Sets of Experimental Tasks for the Measures of Users’ Judgment When Exposed to Two Types of Simulated Social Engineering Attacks (Phishing & PMSER).*

**Validity and Reliability**

Internal validity “encompasses whether the results of the study are legitimate because of the way the groups were selected, data was recorded or analysis performed” (Lakshmi & Mohideen, 2013, p. 2752). This work-in-progress research study will utilize the Delphi methodology during the development of the testing instrument to control known sources of error that will affect the validity of the
testing (Barchard & Pace, 2011; Kimberlin & Winterstein, 2008). The Delphi technique is used in research studies because the processes involved provide the validity of the study (Kennedy, 2004; Lempinen et al., 2012; Straub & Gefen, 2004). The Delphi technique consists of several rounds of iterations to help control the design process and ensure the validity of all constructs (Hasson et al., 2000; Lempinen et al., 2012). The strength in numbers approaches offered by the Delphi technique helps to support the validity of the research methods when using knowledgeable participants in the form of SMEs (Hasson et al., 2000; Worrell et al., 2013). SMEs add valuable knowledge to the Delphi technique in the form of concurrent validity, which strengthens the research (Powell, 2003; Williams & Webb, 1994). Moreover, following the recommendation of Lakshmi and Mohideen (2013), the split-half method to ensure internal consistency will be conducted to see if one random half of the SMEs feedback is not significantly different than the other half. If it is, additional Delphi rounds will be required until final consensus is achieved. Moreover, according to Lakshmi and Mohideen (2013), “external validity, often called “generalizability”, involves whether the results given by the study are transferable to other groups (i.e., populations) of interest” (p. 2752). While this phase of the work-in-progress research study is more focused on the validity of the next phase’s experiments, external validity will be addressed in the next steps of the research, where first a pilot test will be conducted with a smaller diverse group of users, followed by a larger diverse group of users to ensure the generalizability of the results.

Reliability not only ensures consistent results are produced but also makes “a statement about measurement accuracy” (Straub & Gefen, 2004, p. 400). Eliciting the feedback from SMEs will help ensure both validity and reliability when developing measures for this proposed research (Brown et al., 2015). Reliability and validity work hand in hand with each other to ensure the accuracy of research (Creswell, 2013; Straub & Gefen, 2004). Having a large group of SME participants in a research study using the Delphi technique helps to increase the reliability of the study (Ono & Wedemeyer, 1994; Powell, 2003). A significant advantage of using the Delphi technique is that it leverages the collective wisdom of the SMEs without the confrontational pressure of a group setting. (Okoli & Pawlowski, 2004; Skinner et al., 2015).

**Proposed Sample**

A proposed sample size of 25 cybersecurity SMEs for the Delphi rounds will be recruited via e-mail and a LinkedIn recruitment post to get a larger sample size. The recruited SME’s will be from the cybersecurity field in industry and academia to provide a better diversity of skills and experience. The recruited SMEs will provide input for the experimental research design process and the proposed research protocols. This proposed research study will address RQ1 by using the Delphi.
methodology to identify and validate the specific SMEs two sets of experimental tasks to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) during two types of environments (distracting vs. non-distracting), and two types of device (mobile phone vs. computer). The Delphi methodology will also be used to address RQ2 by validating 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), during two types of environments (distracting vs. non-distracting), and two types of device (mobile phone vs. computer).

CONCLUSIONS AND DISCUSSIONS

This work-in-progress study is relevant, as it seeks to identify the vulnerabilities of Information Systems (IS) 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 the use of social engineering through scams and clickbait links (Frauenstein & Flowerday, 2016; Halevi et al., 2013; Maret & Wright, 2009). Frauenstein and Flowerday (2016) stated that users pick up bad habits through the use of link sharing applications that leave them vulnerable to phishing attacks. These bad habits make it harder for a person to discern between real 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 users 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, to distract them from the visual cues that they would 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). 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 will also face several limitations. The main limitation of this experimental research study is relying on the SME opinions provided during the Delphi technique. SME panel participants are often volunteers that can withdraw from the study for many reasons, which can have a negative
impact (Ellis & Levy, 2010). Combining the Delphi technique with a review of the literature can mitigate any limitations, and recruit SMEs from varying industries and academia will help 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 judgmental errors (Frauenstein & Flowerday, 2016; Sheng et al., 2010). As such, additional assessments of the experimental data with the interaction of the different demographic indicators may help further uncover potential groups that are more susceptible to social engineering attacks.

References


Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research


Pollock et al.: Towards an Assessment of Judgment Errors in Social Engineering At


https://digitalcommons.kennesaw.edu/ccerp/2020/Research/3
Pollock et al.: Towards an Assessment of Judgment Errors in Social Engineering At


Wright, R., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing:
