Oct 23rd, 1:13 PM - 2:00 PM

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

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:

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 (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.

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 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).

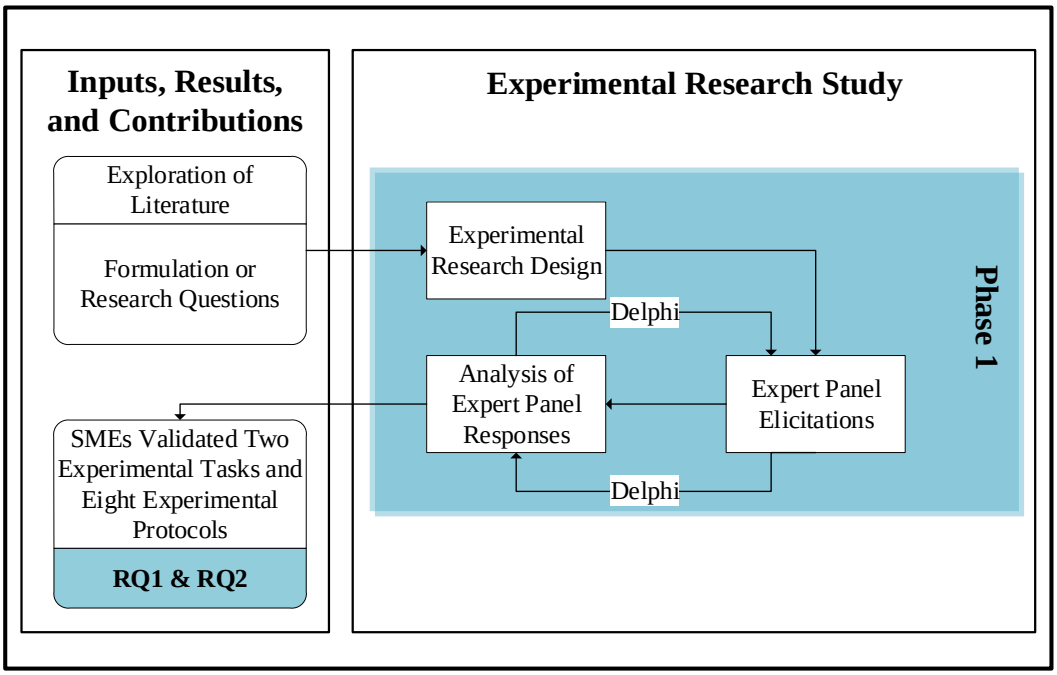
METHODOLOGY

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).

Figure 1

Proposed Overview of the Expert Panel Research Design Process



The validity of this experimental research builds on prior research by Dhamija et al. (2006), Haleviet 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 studys' 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)

Social Engineering Attack Type

Phishing

Device	**Environment**	
	Distracting	Non-Distracting
Mobile Phone	Distracted via Mobile Phone	Not Distracted via Mobile Phone
Computer	Distracted via Computer	Not Distracted via Computer

PMSER

Device	**Environment**	
	Distracting	Non-Distracting
Mobile Phone	Distracted via Mobile Phone	Not Distracted via Mobile Phone
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

IQ Test Number	IQ Test Type	IQ Test Topic	IQ Test Measure
PH-IQ-01	Phishing IQ Test	E-mail from the FBI about a banking transaction.	Legitimate or phishing e-mail
PH-IQ-02	Phishing IQ Test	E-mail alert from Microsoft about login activity on account.	Legitimate or phishing e-mail
PH-IQ-03	Phishing IQ Test	E-mail alert from Experian about a change to a credit report.	Legitimate or phishing e-mail
PH-IQ-04	Phishing IQ Test	E-mail alert from NETFLIX about account cancellation.	Legitimate or phishing e-mail
PH-IQ-05	Phishing IQ Test	Reminder e-mail from PayPal about security upgrades to their system.	Legitimate or phishing e-mail
PH-IQ-06	Phishing IQ Test	E-mail from Audible about a free audiobook service for kids.	Legitimate or phishing e-mail
PH-IQ-07	Phishing IQ Test	E-mail alert from Google showing a new sign in to account.	Legitimate or phishing e-mail
PH-IQ-08	Phishing IQ Test	E-mail alert from Citibank stating that the account was locked out due to three failed login attempts.	Legitimate or phishing e-mail
PH-IQ-09	Phishing IQ Test	Payment receipt from MCPROHOSTING for server space rental.	Legitimate or phishing e-mail
PH-IQ-10	Phishing IQ Test	E-mail alert from Amazon regarding an item selling through their website.	Legitimate or phishing e-mail
PM-IQ-01	PMSER IQ Test	Search results for Motillum using a search engine browser.	Legitimate or possibility malicious link

IQ Test Number	IQ Test Type	IQ Test Topic	IQ Test Measure
PM-IQ-02	PMSER IQ Test	Search results for tickets for the 2010 Miss Universe pageant using a search engine browser.	Legitimate or possibility malicious link
PM-IQ-03	PMSER IQ Test	Search results for the term blockchain using a search engine browser.	Legitimate or possibility malicious link
PM-IQ-04	PMSER IQ Test	Search results for hotels for an upcoming trip to Berlin, Germany using a search engine browser.	Legitimate or possibility malicious link
PM-IQ-05	PMSER IQ Test	Search results for killer whales at SeaWorld using a search engine browser.	Legitimate or possibility malicious link
PM-IQ-06	PMSER IQ Test	Search results for the malwaretips website using a search engine browser.	Legitimate or possibility malicious link
PM-IQ-07	PMSER IQ Test	Search results for camping gear using a search engine browser.	Legitimate or possibility malicious link
PM-IQ-08	PMSER IQ Test	Searched results for the 2018 midterm elections using a search engine browser	Legitimate or possibility malicious link
PM-IQ-09	PMSER IQ Test	Search results for COVID-19 using a search engine browser.	Legitimate or possibility malicious link
PM-IQ-10	PMSER IQ Test	Search results for the RuneScape download website using a search engine browser.	Legitimate or possibility malicious link

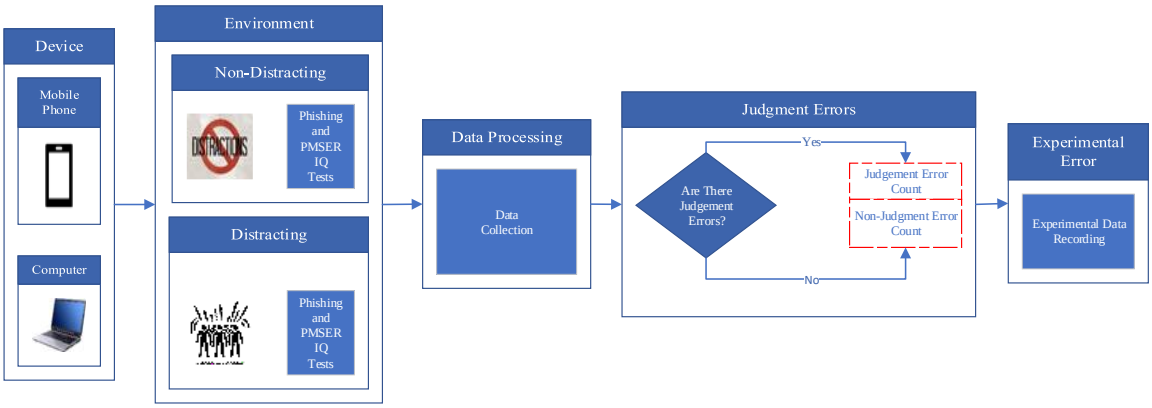
A proposed sample size of 25 cybersecurity SMEs for the Delphi rounds will be recruited via e-mail and a LinkedIn recruitment post to get a larger sample size. To reach the desired sample size, up to 40 SMEs will be recruited via e-mail and social media. The recruited SMEs will be from the cybersecurity 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; Marett & 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 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

Barchard, K., & Pace, L. (2011). Preventing human error: The impact of data entry methods on data accuracy and statistical results. In *Computers in Human Behavior* (Vol. 27). https://doi.org/10.1016/j.chb.2011.04.004

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

Brown, S. D., Levy, Y., Ramim, M. M., & Parrish, J. L. (2015). Pharmaceutical companies' documented and online privacy practices: Development of an index measure and initial test. *Online Journal of Applied Knowledge Management*, *3*(2), 68–88.

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

Creswell, J. (2013). *Qualitative inquiry & research design: Choosing among five approaches.* (Third). Sage Publications Inc.

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

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security*, *15213*, 79. https://doi.org/10.1145/1143120.1143131

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

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

methods. *Proceedings of Informing Science & IT Education Conference (InSITE)*, *10*, 107–118. http://proceedings.informingscience.org/InSITE2010/InSITE10p107-118Ellis725.pdf

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, judgement, and social cognition. *Annual Review of Psychology*, *59*, 255–278. https://doi.org/10.1146/annurev.psych.59.103006.093629

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

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

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing e-mails 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 e-mails. *Proceedings of the 16th International Conference on World Wide Web*, 649–656. https://doi.org/10.1145/1242572.1242660

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

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

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

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

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

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

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

Fox, C. R., & Tversky, A. (1998). A belief-based account of decision under uncertainty. *Management Science*, *44*(7), 879–895. https://doi.org/10.1287/mnsc.44.7.879

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

Frauenstein, E. D., & Flowerday, S. V. (2016). Social network phishing: Becoming habituated to clicks and ignorant to threats? *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

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, *32*(4), 1008–1015. https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x

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

Kennedy, H. P. (2004). Enhancing Delphi research: Methods and results. *Journal of Advanced Nursing*, *45*(5), 504–511. https://doi.org/10.1046/j.1365-2648.2003.02933.x

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

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

Kimberlin, C. L., & Winterstein, A. G. (2008). Validity and reliability of measurement instruments used in research. *American Journal of Health-System Pharmacy*, *65*(23), 2276–2284. https://doi.org/10.2146/ajhp070364

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

Lakshmi, S., & Mohideen, M. (2013). Issues in reliability and validity of research. *International Journal of Management Research and Review*, *3*(4), 2752–2758.

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

Lempinen, H., Rossi, M., & Tuunainen, V. K. (2012). Design principles for inter-organizational systems development - Case Hansel. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 7286 LNCS*. https://doi.org/10.1007/978-3-642-29863-9_5

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

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

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

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, *42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

Oliveira, D., Ebner, N., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., & Lin, T. (2017). Dissecting spear phishing e-mails 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

Ono, R., & Wedemeyer, D. J. (1994). Assessing the validity of the Delphi technique. *Futures*, *26*(3), 289–304. https://doi.org/10.1016/0016-3287(94)90016-7

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers and Security*, *52*, 194–206. https://doi.org/10.1016/j.cose.2015.02.008

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

Powell, C. (2003). The Delphi technique: Myths and realities. *Journal of Advanced Nursing*, *41*(4), 376–382. https://doi.org/10.1046/j.1365-2648.2003.02537.x

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.

Reason, James T. (1995). Understanding adverse events: human factors. *Qual Saf Health Care*, *4*(2), 80–89. https://doi.org/10.1136/qshc.4.2.80

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

Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems*, *37*, 31–63. https://doi.org/10.17705/1cais.03702

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

Straub, D., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(13), 380–427. https://doi.org/10.17705/1CAIS.01324

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 e-mail 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

Williams, P. L., & Webb, C. (1994). The Delphi technique: A methodological discussion. *Journal of Advanced Nursing*, *19*(1), 180–186. https://doi.org/10.1111/j.1365-2648.1994.tb01066.x

Worrell, J. L., Di Gangi, P. M., & Bush, A. A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems*, *14*(3), 193–208. https://doi.org/10.1016/j.accinf.2012.03.003

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