

2022

Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors

Tommy Pollock

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Experimental Study to Assess the Role of Environment and Device Type on
the Success of Social Engineering Attacks: The Case of Judgment Errors

by

Tommy Pollock

A dissertation report submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Assurance

College of Computing and Engineering
Nova Southeastern University

2022

We hereby certify that this dissertation, submitted by Tommy Pollock conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

5/11/22
Date



Ajoy Kumar, Ph.D.
Dissertation Committee Member


5/11/22
Date



Wei Li, Ph.D.
Dissertation Committee Member

5/11/21
Date

Approved:



Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

5/11/21
Date

College of Computing and Engineering Nova
Southeastern University

2022

An Abstract of a Dissertation Proposal Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Experimental Study to Assess the Role of Environment and Device Type on
the Success of Social Engineering Attacks: The Case of Judgment Errors

by
Tommy Pollock
May 2022

Phishing continues to be an invasive threat to computer and mobile device users. Cybercriminals continuously develop new phishing schemes using e-mail and malicious search engine links to gather the personal information of unsuspecting users. This information is used for financial gains through identity theft schemes or draining victims' financial accounts. Many users of varying demographic backgrounds fall victim to phishing schemes at one time or another. Users are often distracted and fail to process the phishing attempts fully, 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 cannot distinguish between legitimate and malicious emails or search engine results correctly. Mobile phone users can have a harder time distinguishing malicious content due to the smaller screen size and the limited security features in mobile phone applications.

The main goal of this research study was to design, develop, and validate experimental settings to empirically test if there are significant mean differences in users' judgment when: exposed to two types of simulated social engineering attacks (phishing & Potentially Malicious Search Engine Results (PMSER)), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile vs. computer). This research used field experiments to test whether users are more likely to fall for phishing schemes in a distracting environment while using mobile phones or desktop/laptop computers. The second phase included a pilot test with 10 participants testing the Subject Matter Experts (SME) validated tasks and measures. The third phase included the delivery of the validated tasks and measures that were revised through the pilot testing phase with 68 participants.

The results of the first phase have SME validated two sets of experimental tasks and 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 devices (mobile phone vs. computer). The second phase results, the phishing mini-IQ test results, do not follow what was initially indicated in prior literature. Specifically, it was surprising to learn that the non-distracting environment results for the Phishing IQ tests were overall lower than those of distracting environment, which is counter to what was envisioned. These Phishing IQ test results may be assumed to be because, during the distracting sound environment, the participants were monitored over zoom to enable the distracting sound file. In contrast, in the non-distracting environment, they have marked the selections independently and may have rushed to identify the phishing samples.

In contrast, PMSER detection on a computer outperformed mobile devices. It is suspected that these results are more accurate as individuals' familiarity with PMSER is much lower. Their habituation to such messages is more deficient, causing them to pay closer attention and be more precise in their detections. A two-way Analysis of Variance (ANOVA) was conducted on the results. While it appears that some variations do exist, none of the comparisons were significant for Phishing IQ tests by environment ($F=3.714$, $p=0.061$) or device type ($F=0.380$, $p=0.541$), and PMSER IQ tests by environment ($F=1.383$, $p=0.247$) or device type ($F=0.228$, $p=0.636$). The results for the final phase showed there were no significant differences among both groups for Phishing and PMSER ($F=0.985$, $p=0.322$) and PMSER ($F=3.692$, $p=0.056$) using a two-way ANOVA. The two-way ANOVA results also showed significant differences among both groups for Phishing and PMSER vs. Device Type and Environment, Phishing ($F=3.685$, $p=0.013$), PMSER ($F=1.629$, $p=0.183$). A two-way ANOVA was evaluated for significant differences between groups. The results of the two-way ANOVA showed there were significant differences among both groups for Phishing and PMSER vs. Device Type and Environment. Phishing ($F=3.685$, $p=0.013$), PMSER ($F=1.629$, $p=0.183$). The p -values of the F -test for the Phishing IQ vs. Device Type and Environment were lower than the .05 level of significance. The two-way Analysis of Covariance (ANCOVA) results showed significant differences between Phishing vs. Environment and Device Type plus PMSER vs. Environment and Device Type. Specifically, the Education covariate for Table 32($F=3.930$, $p=0.048$), Table 33($F=3.951$, $p=0.048$), Table 34($F=10.429$, $p=0.001$), and Table 35($F=10.329$, $p=0.001$) was lower than the .05 level of significance.

Acknowledgments

I am incredibly grateful to receive such support throughout this remarkable journey. I want to thank several people, especially my Mom and Dad, who continually inspire me. To my wife Sandra and children Hunter and Madison for supporting me every step of the way. To my submarine force brethren, the crew of the USS Flying Fish SSN- 673, and Admiral Richard Mies, who always encouraged me to improve and never settle for second best constantly. Submarines once, Submarines twice.

To my peers at Tidewater Community College, especially Kyndra Brown, Lisa Peterson, and the LAC and Workforce Development crews. Thank you for your help and support.

To my late-night statistics friend Patricia Baker - thank you for your creative energy and help in recruiting.

Thank you to everyone at NSU for working through this process together. Especially: Bob Jones, Molly Cooper, Jim Furstenberg, John McConnell, Mel Tomeo, Javier Coto, Kimberly Smith, Tyler Pieron, Vazzi, David Zeichick, Andrea Di Fabio, Amy Antonucci, Emily Brown, Darrell Eilts, Ariel Luna, Reid Cooper, and the rest of the NSU AIS group. You all have been a great support group.

Thank you to all the SME Survey, Pilot Testing, and Main Research Study participants. I appreciate your valuable input!

To Dr. Li and Dr. Kumar, I was incredibly fortunate to have such amazing and talented committee members. Thank you for your time, expertise, and guidance through the process.

To Dr. Levy, you have been an inspiration to me from the very beginning. Thank you for pushing me to be the best I can be. Thank you for taking me on and investing so much of yourself into this journey. I appreciate your vision and guidance more than words can say. It has been such an honor to collaborate with you.

Table of Contents
Abstract iii
Acknowledgments v
List of Tables ix
List of Figures xii

Chapters

1. Introduction 1

Background 1
Problem Statement 4
Research Goals 7
Research Questions 11
Relevance and Significance 12
Barriers and Issues 13
Limitations 14
Definition of Terms 14
Summary 16

2. Review of the Literature 17

Introduction 17
Phishing 17
Environment 24
Judgment Errors 27
Summary of What is Known and Unknown 33

3. Methodology 35

Experimental Tasks and Measures 36
Validity and Reliability 41
SME Data and Analysis 43
Sample 49
Pre-Analysis Data Screening 50
Data Analysis 51
Resources 54
Summary 54

4. Results 56

Overview 56
Phase I – SME Survey Feedback and Findings 56
Phase II – Pilot Testing 68
Phase III - Main Research Study 73
Phase III – Pre-Analysis Data Screening 74

Phase III - Participant Demographics Characteristics 74

Phase III – Data Scoring 76

Phase III Findings 78

Phase III RQ3 80

Phase III RQ4 83

Phase III RQ5 86

Phase III RQ6 90

5. Conclusions, Implications, Recommendations, and Summary 98

Conclusions 98

Implications 99

Reccomendations 101

Summary 101

Appendices

A. Institutional Review Board Approval Letter 104

B. Site Approval Letter 105

C. Expert Recruitment E-mail 106

D. Example of SME Participant Demographics Survey 107

E. Research Study Recruitment Flyer 111

F. Research Study Informed Consent Form 112

G. Demographics Questions 117

H. Phishing E-mail Questions 119

I. PMSER Questions 131

J. Participant Research Recruiting Letter 139

References 142

List of Tables

Tables

1. Summary of Phishing 19
2. Summary of Environment 26
3. Summary of Judgment Errors 29
4. Phishing and PMSER Mini IQ Test Randomization Table 42
5. Research Questions and Methodology 44
6. Descriptive Statistics of SMEs (N=28) 56
7. SME Feedback on Email Samples for IQ Testing (N=28) 57
8. SME Feedback on Email Sample Edits (N=28) 62
9. SME Feedback on PMSER Samples for IQ Testing (N=28) 63
10. SME Feedback on PMSER Sample Edits (N=28) 64
11. SME Feedback of Physical Distracting Environments (N=28) 65
12. SME Feedback of A/V Distraction Levels (N=28) 66
13. SME Feedback on Mini IQ Test Randomization (N=28) 66
14. Pilot Testing and Experimental Testing Procedures 66
15. Descriptive Statistics of Pilot Test Participants (N=10) 68
16. Scoring of Mini-IQ Responses for Phishing and PMSER Selections 69
17. Descriptive Statistics of Main Study Participants (N=68) 73
18. Mini IQ Test-Revised Survey Answers 75
19. Scoring of Mini-IQ Responses for Phishing and PMSER Selections 76
20. ANOVA Results of Phishing IQ vs. Environment (N=68) 79
21. ANOVA Results of PMSER IQ vs. Environment (N=68) 79
22. Descriptive Statistics of Phishing IQ vs. Environment (N=68) 80

23. Descriptive Statistics of PMSER IQ vs. Environment (N=68) 81
24. ANOVA Results of Phishing IQ vs. Device Type (N=68) 82
25. ANOVA Results of PMSER IQ vs. Device Type (N=68) 82
26. Descriptive Statistics of Phishing IQ vs. Device Type (N=68) 83
27. Descriptive Statistics of PMSER IQ vs. Device Type (N=68) 84
28. ANOVA Results of Phishing IQ vs. Device Type and Environment (N=68) 86
29. ANOVA Results of PMSER IQ vs. Device Type and Environment (N=68) 86
30. Descriptive Statistics of Phishing IQ vs. Device Type (Mobile (1) and Computer (2)) and Environment (N=68) 87
31. Descriptive Statistics of PMSER IQ vs. Device Type (Mobile (1) and Computer (2)) and Environment (N=68) 88
32. ANCOVA Results of Phishing IQ vs. Environment with Demographic Covariates(N=68) 90
33. ANCOVA Results of Phishing IQ vs. Device Type with Demographic Covariates(N=68) 90
34. ANCOVA Results of PMSER IQ vs. Environment with Demographic Covariates(N=68) 91
35. ANCOVA Results of PMSER IQ vs. Device Type with Demographic Covariates(N=68) 91
36. Descriptive Statistics of Phishing IQ vs. Environment with Demographic Covariates (N=68) 92
37. Descriptive Statistics of Phishing IQ vs. Device Type with Demographic Covariates (N=68) 93
38. Descriptive Statistics of PMSER IQ vs. Environment with Demographic Covariates (N=68) 94
39. Descriptive Statistics of PMSER IQ vs. Device Type with Demographic Covariates (N=68) 95

List of Figures

Figures

1. 2x2x2 Experimental Design Taxonomy of Device (Mobile/Computer) vs. Environment (Distracting/Non-Distracting) vs. Social Engineering Attack Type (Phishing/PMSER) 9
2. Overview of the Research Design Process 36
3. 2x2x2 Experimental Design Taxonomy of Device (Mobile Phone/Computer) vs. Environment (Distracting/Non-Distracting) vs. Social Engineering Attack Type (Phishing/PMSER) with Experimental Tasks and Protocols 38
4. Two Sets of Experimental Tasks for the Measures of Users' Judgment When Exposed to Two Types of Simulated Social Engineering Attacks (Phishing & PMSER). 39
5. Sample SME Survey of the Physical Environment Distractions 40
6. Sample SME Survey of the Audio/Visual Distraction Levels 41
7. Physical Environment and AV Distraction Levels for SME Survey 47
8. Sample Email Question for the SMEs Survey 48
9. Research Questions and Methodology. 52
10. Pilot Test Summary of Participants Results (N=10) 70
11. Results of the Pilot Mini-IQ Tests for Phishing IQ (a) and PMSER (b) 72
12. Main Study Summary of Participants Results (N=68) 78
13. Results of the Main Study Mini-IQ Tests for Phishing IQ (a) and PMSER (b) 79
14. Mean Score for Phishing IQ vs. Environment (N=68) 81
15. Mean Score for PMSER IQ vs. Environment (N=68) 82
16. Mean Score for Phishing IQ vs. Device Type (N=68) 84
17. Mean Score for PMSER IQ vs. Device Type (N=68) 85
18. Mean Score for Phishing IQ vs. Device Type (Mobile (1) and Computer (2)) and Environment (N=68) 88
19. Mean Score for PMSER IQ vs. Device Type (Mobile (1) and Computer (2)) and Environment (N=68) 89

20. Mean Score for Phishing IQ vs. Environment with Demographic Covariates (N=68)
93
21. Mean Score for Phishing IQ vs. Device Type with Demographic Covariates (N=68)
94
22. Mean Score for PMSER IQ vs. Environment with Demographic Covariates (N=68)
95
23. Mean Score for PMSER IQ vs. Device Type with Demographic Covariates (N=68)
96

Chapter 1

Introduction

Background

Phishing and malware/ransomware infection from emails, along with Potentially Malicious Search Engine Results (PMSE), inflict significant financial losses to individuals and organizations (Anderson et al., 2013; Choo, 2011; Wright & Marett, 2010). Cybercriminals use increasingly ingenious schemes to take advantage of users' judgment errors when dealing with phishing emails and PMSE (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 the personal information of unsuspecting users (Anderson et al., 2013). This information is used for financial gains through identity theft schemes or draining victims' financial accounts (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 differentiating an actual QR code from a hijacked one (Dabrowski et al., 2014; Focardi et al., 2018; Mavroeidis & Nicho, 2017). Mobile phones are often the primary platform users utilize 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 have a hard time judging the legitimacy of emails and web links on their PC, being a desktop or laptop (Furnell, 2007).

Overconfidence in one's abilities and failure to recognize phishing campaigns' risks 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 users' judgment errors to enrich themselves. A user's 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 emails or web links due to security not being their primary concern (Kumaraguru et al., 2007; Williams et al., 2018). Moreover, it was indicated that “environmental distractions can impact cognitive performance, whether this concerns solving a mathematical problem, maintaining a conversation, or retrieving an experienced event from memory” (Vredevelde & 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 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).

Problem Statement

The research problem that this study addressed is financial losses to individuals and organizations due to phishing and malware/ransomware infection from emails and Potentially Malicious Search Engine Results (PMSER) (Anderson et al., 2013; Choo, 2011; Wright & Marett, 2010). Cybercriminals use increasingly ingenious schemes to take advantage of users' judgment errors when dealing with phishing emails and PMSER (Dhamija et al., 2006; Leontiadis et al., 2014). Phishing is a subcategory of Social Engineering and is 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). Deceptive Search Engine Results (SER) pose a problem because cybercriminals often manipulate the SER algorithms through search poisoning techniques, which promote malicious links to the first page of the SER (John et al., 2011; Leontiadis et al., 2014). In particular, mobile phones are more vulnerable to phishing

attacks than PCs due to poor fraudulent website detection of some mobile browsers such as Chrome Mobile and Opera Mini (Mavroeidis & Nicho, 2017; Tsalis et al., 2015; Virvilis et al., 2014). Mobile phone apps such as Quick Response (QR) code readers also pose a phishing attack vector because of the difficulty differentiating an actual QR code from a hijacked one (Dabrowski et al., 2014; Focardi et al., 2018; Mavroeidis & Nicho, 2017). Mobile phones are often the primary platform users utilize 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 dictionary meaning of “error of judgment” is “making a bad or wrong decision,” it usually involves calculated risks, evaluating options, and executive decision making” (Chowdhury, 2016, p. 42). Even in nondistracting environments such as an office setting, it is well known in research that users still have difficulty judging the legitimacy of emails 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. 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). Various demographic indicators such as (a) age, (b) gender, (c) education, and (d) level of social media usage also play a role in phishing judgmental errors (Frauenstein & Flowerday, 2016; Sheng et al., 2010). 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 users' judgment errors to enrich themselves. A user's 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, users tend to be unmotivated or ignore the visual cues in emails or web links due to security not being their primary concern (Kumaraguru et al., 2007; Williams et al., 2018). "Environmental distractions can impact cognitive performance, whether this concerns solving a mathematical problem, maintaining a conversation, or retrieving an experienced event from memory" (Vredeveldt & Perfect, 2014, p. 1). A distracting environment can occur in any setting with constant interruptions from background noise 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).

Research Goals

The main goal of this research study is to design, develop, and validate experimental settings to empirically test 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 phone vs. computer). The need for this work was demonstrated by Anderson et al. (2013), Furnell (2007), Karakasiliotis et al. (2006), Sheng et al. (2010), as well as Nicholson et al. (2005). Anderson et al. (2013) found that there is a combination of direct costs, indirect costs, and defense costs that add up to society's cost for cybercriminals' activities such as phishing attacks. These costs do not just include monetary losses from the victims but also their loss of confidence in the security mechanisms involved (Anderson et al., 2013). Furnell (2007) found that some users are unable to correctly judge that a phishing e-mail is illegitimate based just on the content. Demographic factors such as education level, age, gender, and not fully understanding phishing play a role in users' inability to make the correct judgments (Cain et al., 2018; Gratian et al., 2018; Oliveira et al., 2017).

This research builds on prior literature by assessing if there are any 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), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile phone vs. computer). Users who habitually share web links on their devices tend to have low-security awareness, potentially opening them 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 users ability to perform assigned tasks (Drew & Forbes, 2017; Khaddage et al., 2015; Nicholson et al., 2005). These distractions pose an attention conflict that can overload cognitive function, which reduces performance, leading to difficulty completing tasks (Groff et al., 1983; Kahneman, 1973; Sanders et al., 1978). Interruptions caused by distractions force people to focus elsewhere instead of the task they need to perform (Speier et al., 1999, 2003). The time to complete tasks can be significantly affected by interruptions in the work environment (Bailey et al., 2006; Mansi & Levy, 2013; Zijlstra et al., 1999). Distractions from environmental factors are comparable to person-based interruptions due to work time lost from the disturbance (Sanders et al., 1978; Sanders & Baron, 1975).

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. Dhamija et al. (2006) 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 unaware of their vulnerabilities to attacks, especially those that rely heavily on social

media usage. Social media services' popularity 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).

Figure 1

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

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's susceptibility 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 1 illustrates this study's 2X2X2 experimental design taxonomy between devices in distracting and non-distracting environments during interaction with two types of social engineering attacks (phishing & PMSER).

The six specific goals of this research study are as follows. This research study's first specific goal is to identify and validate, using Subject Matter Experts (SMEs), *two sets of experimental tasks* for the measure of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). The second specific goal of this research study 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). This research study's third specific goal is to find if there are any statistically significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) based on the kind of environment (distracting vs. non-distracting) the users are experiencing. This research study's fourth specific goal is to find if there are any statistically significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) based on the type of device used (mobile phone vs. computer). The fifth specific goal of this research study is to find if there are any statistically significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) based on the interaction of the types of environments (distracting vs. non-distracting) and type of device used (mobile phone vs. computer). The sixth specific goal

of this research study is to find if there are any statistically significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when controlled for the users: (a) gender, (b) age, (c) education, and (d) level of social media usage.

Research Questions

The main research question that this research study addressed is: Are there any statistically 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 phone vs. computer)?

RQ1. What are the specific 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 devices (mobile phone vs. computer)?

RQ3. Are there significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) in distracting vs. non-distracting environments?

- RQ4. Are there significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when using a mobile phone vs. a computer?
- RQ5: Are there statistically 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 phone vs. computer)?
- RQ6: Are there any significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when controlled for the users': (a) age, (b) gender, (c) education, and (d) level of social media usage?

Relevance and Significance

This 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 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 link-sharing applications that leave them vulnerable to phishing attacks. These bad habits make it harder for people

to discern between genuine and malicious links making them more susceptible to phishing attacks (Frauenstein & Flowerday, 2016; Vishwanath et al., 2011).

This research is significant as it will advance 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, 1995a; Sanders & Baron, 1975). Attackers craft phishing attacks to distort the mental model that users form in interacting with online transactions to distract them from the visual cues 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 provided significant input to the body of knowledge of users' susceptibility to social engineering attacks in distracting environments while using mobile phones and computers. The results were added to the body of knowledge on which demographic groups are more susceptible to social engineering attacks in distracting environments.

Barriers and Issues

One potential barrier to this experimental research study is obtaining permission to evaluate users exposed to two types of simulated social engineering attacks (phishing & PMSER). Institutional Review Board (IRB) approval is needed from multiple institutions to conduct research on human subjects. Moreover, using the Delphi technique also poses a potential barrier. Selecting the correct SME participants who will cooperate

with the process while avoiding induced bias in this experimental research study can be complicated (Botterill & Platenkamp, 2014; Gordon, 2009). Collecting an adequate number of useable responses from SMEs can also be an issue if the experiments ask ambiguous questions (Gordon, 2009).

Limitations

This experimental research study's main limitation relies on the SME opinions provided during the Delphi technique. SME panel participants are often volunteers who 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.

An additional limitation is correctly recording and analyzing participant responses without error. All data must be manually and visually reviewed to address this validity and reliability issue and identify any errors. Missing data must be evaluated before the final analysis to ensure consistency, validity, and reliability (Levy, 2006; Onwuegbuzie et al., 2010).

Definition of Terms

Information System (IS) –

A discrete set of information resources [i.e., personnel, equipment, funds, and information technology] organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Also includes specialized systems such as industrial/process control systems, telephone

switching and private branch exchange (PBX) systems, and environmental control systems. (Kissel, 2013, p. 101)

Information Technology (IT) – “The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources” (Kissel, 2013, p. 101).

Instrument – “Observational instruments or rating scales are developed to evaluate the behaviors of subjects who are being directly observed” (Kimberlin & Winterstein, 2008, p. 2278).

Judgment Error – “Making a bad or wrong decision, usually involving calculated risks, evaluating options, and executive decision making” (Chowdhury, 2016, p. 42).

Phishing – Phishing is a type of cyber attack that sits at the intersection of social engineering and security technologies (McElwee et al., 2018).

Phishing IQ. test – A test where “participants are informed that they are participating in a phishing study, are presented with images of phishing and legitimate emails and are asked to make judgments concerning the authenticity of the images” (Parsons et al., 2015)

PMSE – Potentially Malicious Search Engine Results.

Social engineering – “Techniques used to manipulate people into performing actions or divulging confidential information” (Mitnick & Simon, 2002; Workman, 2008).

User – “An individual or a process (subject) acting on behalf of the individual authorized to access an information system” (Kissel, 2013, p. 209).

Validity – “The extent to which an instrument measures what it purports to measure.

Validity requires that an instrument is reliable, but an instrument can be reliable without being valid” (Kimberlin & Winterstein, 2008, p. 2278).

Summary

This experimental research addressed financial losses due to users’ judgment errors when dealing with phishing emails and PMSER. Anderson et al. (2013) found that there is a combination of direct costs, indirect costs, and defense costs that add up to society's cost for cybercriminals' activities such as phishing attacks. These costs do not just include monetary losses from the victims but also their loss of confidence in the security mechanisms involved (Anderson et al., 2013). Cybercriminals use increasingly ingenious schemes to take advantage of users’ judgment errors when dealing with phishing emails and PMSER (Dhamija et al., 2006; Leontiadis et al., 2014). The main goal of this research study is to design, develop, and validate experimental settings to empirically test 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 phone vs. computer).

Chapter 2

Review of the Literature

Introduction

In this chapter, a literature review is used to provide a theoretical foundation for this experimental research study. The literature offers a synopsis of relevant literature related to phishing, environmental factors, and judgment errors. According to Hart (2003), literature reviews are needed so that the researcher can gain a better understanding of prior research on a topic to find out what has been done, what the issues are, and how the analysis was performed. Using a concept–centric approach and quality resources, researchers can build a solid foundation for their research (Levy & Ellis, 2006; Webster & Watson, 2002). This literature review searched for quality peer-reviewed journals and past research to find relevant data and findings for this research.

Phishing

Phishing scams are among the oldest and most widely used social engineering methods to gain personal information and infiltrate organizational systems, mainly for financial gain (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 e-mail-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 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 by using distracting features and persuasive elements (Chiew et al., 2018; Kim & Kim, 2013). The content of these messages is often disguised as legitimate companies. It contains rational, emotional, and motivationally appealing elements that tempt users to click on links to gain their personal information to steal their identity or financial assets (Kim & Kim, 2013).

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, directing the mobile phone to a phishing website (Mavroeidis & Nicho, 2017; Vidas et al., 2013). These QR codes use a method called Uniform Resource Locator (URL) shorteners to hide the URL name and their identities (Dabrowski et al., 2014; Frauenstein & Flowerday, 2016; Mavroeidis & Nicho, 2017). 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 more susceptible to phishing attacks (Flores et al., 2015; Oliveira et al., 2017; Sheng et al., 2010). Users are targeted at work and private on their computers and mobile phones to gain personal information (Virvilis et al., 2014; Williams et al., 2018). Even with proper training, research provides

strong evidence that users still 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).

Table 1

Summary of Phishing Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Dhamija et al., 2006	Empirical study	22 participants were shown 20 websites	Phishing websites	Even in the best-case scenario, when users expect spoofs to be present and are motivated to discover them, many cannot distinguish a legitimate website from a spoofed one.
Fette et al., 2007	Theoretical	860 phishing emails and 6950 non-phishing emails	Phishing emails	It is possible to detect phishing emails with high accuracy by using a specialized filter.
Moody et al., 2007	Experimental research	42 participants who had been randomly assigned to one of three conditions	Phishing education	Participants with high CRT scores are more likely to click on phishing emails when they are from an unknown source.
Marett & Wright, 2009	Experimental research	224 undergraduate students	Phishing	There was no systematic difference between the mail servers and the unrecoverable emails ($p=.89$).

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Wright & Marett, 2010	Empirical	446 undergraduate students	Phishing	Four behavioral factors were influential as to whether the phishing emails were answered with sensitive information.
Choo, 2011	Survey of Australian businesses	A random sample of 4000 respondents	Cybercrime	The financial industry was the most targeted industry sector in phishing attacks in the 2009 calendar year
Enck, 2011	Theoretical	Current mobile phone research	Mobile phone security	Advantages and limitations of existing mobile phone protection research.
John et al., 2011	Theoretical	5,000 Web domains that attract 81000 users	Search Engine poisoning attacks	36% of searches yield links to malicious pages among their top results.
Vishwanath et al., 2011	Theoretical	161 intended phishing victims	Phishing	The present research is the first to integrate these different streams of research
Chin et al., 2012	Experimental research	60 mobile phone users	Mobile phone security	Participants are apprehensive about running privacy-and financially sensitive tasks on their phones

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Anderson et al., 2013	Systemic Study	Previous research	Cybercrime	Cybercrime carries higher indirect costs than traditional crimes.
Kim & Kim, 2013	Theoretical	2,068 phishing emails	Phishing	When messages include quality and supportive arguments, they will positively influence attitude change.
Vidas et al., 2013	Theoretical	225 users scanned QR codes in 139 locations.	Mobile phone security	Of the 139 posted flyers, 85 (61%) were utilized by participants to visit the study website at least once, totaling 225 hits across all conditions.
Dabrowski et al., 2014	Experimental research	Ten different 2D barcode applications for iPhone and Android.	Mobile phone security	Users with different apps or devices return different data when the same barcode is scanned.
Leontiadis et al., 2014	Theoretical	Five million search results were collected over four years	Search Engine poisoning attacks	Despite the best efforts of search engines to demote low-quality content, miscreants have readily adapted.
Li et al., 2014	Theoretical	1033 Chinese youth.	Mobile phone security	There are more than 500 third-party app stores containing malicious apps.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Virvilis et al., 2014	Theoretical	10 mobile phone and desktop browsers	Mobile phone security	Android and iOS users are not adequately or sometimes not at all protected from phishing attacks.
Ferreira et al., 2015	Theoretical	52 emails in the data theft, malware, and fraud categories.	Social engineering	A reviewed list of principles of persuasion that works in social engineering
Flores et al., 2015	Survey	2,099 employees of nine organizations in Sweden, the USA, and India	Phishing	Intention to resist social engineering, general information security awareness, formal IS training, and computer experience was identified to correlate to phishing resilience positively.
Tsalis et al., 2015	Experimental research	Mobile phone and desktop browsers accessing 5000 manually verified phishing URLs	Mobile phone security	Only a subset of the mobile browsers supported anti-phishing protection.
Alarm & El Katib, 2016	Theoretical	none	Phishing	There is an abundance of identifiable information about individuals that is easily accessible by the public.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Frauenstein & Flowerday, 2016	Theoretical	Multiple websites and social networking sites	Social engineering	Phishers are using URL shorteners not only to reduce space but also to hide their identity.
Silic & Back, 2016	Field experiment and a qualitative study	Employees of a Fortune 500 company (Financial Services)	Phishing	Existing organizational SNS policies and procedures are inadequate and should be adapted to SNS realities.
Mavroeidis & Nicho, 2017	Experimental research	Simulated phishing attack using a QR code with shortened URL	Mobile phone security	Hackers are increasingly leveraging QR codes as attack vectors putting companies and users at risk.
Moody et al., 2017	Empirical Research	632 undergraduate psychology and IS students	Phishing	41.3% of subjects clicked on the enclosed links in unsolicited emails.
Zhao et al., 2017	Theoretical	194 participants	Phishing	Extreme phishing attacks are highly effective and insidious as over 90% of the participants became the “victims”.
Chiew et al., 2018	Survey of phishing mediums and vectors	Three mediums and eight vectors	Phishing	A holistic approach is needed to develop phishing countermeasures.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Focardi et al., 2018	Theoretical	Previous research	Mobile phone security	We have found that some of the studies and applications developed to protect 2D barcodes lack essential detailed information.
Goel & Jain, 2018	Theoretical	Current attack techniques and solutions for phishing in research	Mobile phone security	User education or training is necessary for reducing susceptibility to phishing attacks.
McElwee et al., 2018	Theoretical	Summary data from four years of simulated phishing from a US company with approximately 1,000 e-mail end-users	Phishing	Outcome-based controls were not effective in changing end-user susceptibility to phishing attacks.
Williams et al., 2018	Theoretical	Study 1- 62000 employees, Study 2 – six focus groups	Phishing	The presence of authority cues increased the likelihood that a user would click a suspicious link in an e-mail.

Environment

Environmental factors affect how users perform tasks in the workplace, at home, and in public (Dalton & Behm, 2007; Kallinen, 2004; Vredeveldt & Perfect, 2014).

Background noise negatively affects task performance because it distracts and interrupts users (Dalton & Behm, 2007; Larsby et al., 2008). However, the use of background music has mixed results (Dalton & Behm, 2007; Kallinen, 2004). 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, users' decision-making process causes 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 working memory's attentive processes (Berti & Schröger, 2001; Christophel et al., 2017). Rodrigues and Pandeirada (2015) evaluated the working memory of 40 elderly research participants in distracting and non-distracting environments. They found that they performed the tasks better in a non-distracting environment. The use of irrelevant stimuli has been found to distract someone from focusing on a task by disrupting attentional awareness (Forster & Lavie, 2008; Steinkamp, 1980; Unsworth & Robison, 2016). Many of these irrelevant stimuli are used in phishing emails to distract the recipient 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).

Table 2

Summary of Environment Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Wright, 1974	Theoretical	210 male undergraduates	Distraction	People tend to accentuate negative evidence when the environment discourages leisurely processing may be indicated.
Sanders & Baron, 1975	Theoretical	40 undergraduate students	Distraction	Distraction does not necessarily impair task performance.
Folk & Remington, 1999	Experimental research	10 test participants	Distraction	Distractors produced significant location effects consistent with attentional capture.
Kallinen, 2004	Theoretical	30 subjects with varying educational backgrounds	Background music	Background music listening elicited a more immersed user experience (with fewer distractions to attention and longer user time) than using PDA without listening to music.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Dalton & Behm, 2007	Theoretical	Prior research	Background noise	Acute and continuous noise adversely affects vigilance and comprehension.
Larsby et al., 2008	Theoretical	24 subjects, aged 56-83 years, with a bilateral sensorineural hearing impairment, participated.	Background noise	Noise characteristics affect speech recognition differently depending on the response criteria
Vredeveltdt & Perfect, 2014	Theoretical	Prior research	Environmental distraction.	Understanding the mechanisms involved in the effects of distractions on cognitive performance.
Rodrigues & Pandeirada, 2015	Experimental research	40 elderly participants	Environmental distraction	The results revealed better performance in the attentional tasks when these were done in the non-distracting environment

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 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 their research, they developed System 1 (intuitive) and 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 with human judgment, with analytical thinking confirming or overriding intuitive thinking (Evans, 2003; Frankish, 2010). Judgments are often made from multiple cues provided by the information being processed. However, these judgments can be affected by subconscious cognitive biases (Evans, 2003, 2008; Evans et al., 2003; Fisk, 2002).

Reason (1990) viewed human error as failures of execution broken down into slips and lapses. Slips are attention-based, whereas lapses are memory-based failures often occurring when performing routine tasks (Flehmig et al., 2007; Norman, 1981; Reason, 1995a; Reason, 1984). Slips in judgment can be caused by external environmental factors or distractions (Flehmig et al., 2007). Lapses in attention can reduce reaction times and inhibit the completion of tasks (Weissman et al., 2006). Lapses also can impair one's ability to minimize distractions in the environment (Weissman et al., 2006).

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

users' working memory (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 coping mechanisms when dealing with potential phishing scams (Wang et al., 2017; Wright, 1974). Distracted users often have a hard time detecting the elements of phishing emails leading to potential judgment errors (Furnell, 2007; Karakasiliotis et al., 2006). Many users judge visual and technical cues in phishing emails and will often not be able to detect phishing attempts (Karakasiliotis et al., 2006). Habitually reading emails while distracted by various environmental factors can increase users' susceptibility to phishing scams (Vishwanath et al., 2011). Errors of judgment often have real consequences involved, depending on the context (Chowdhury, 2016; Funder, 1987).

Table 3

Summary of Judgment Errors Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Wright, 1974	Theoretical	210 male undergraduates	Distraction	People tend to accentuate negative evidence when the environment discourages leisurely processing may be indicated.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Norman, 1981	Theoretical	None	Slip categorization	Categorized slips into three major categories and many subcategories.
Tverski & Kahneman, 1983	Theoretical	Two groups of students, N= 105 and 102	Probability Judgment	The numerous conjunction errors illustrate people's affinity for nonextensional reasoning.
Funder, 1987	Theoretical	Two samples N= 37 and 69	Judgment errors	Although errors can be highly informative about judgment, they are not necessarily relevant to the content.
Kahneman & Tverski, 1996	Theoretical	Three groups of students N= 36,33, and 31.	Cognitive awareness	Subjects use representativeness to estimate outcome frequencies and edit their responses to obey class inclusion in the presence of solid extensional cues.
Lampel & Shapira, 2001	Theoretical	None	Judgment errors	Context influences judgment. Judgmental errors cause misinterpretation of evidence and a consequent sense of false security.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Nicholson et al., 2005	Theoretical	48 subjects	Distraction - Conflict theory	Tasks requiring a higher amount of cognitive effort in environments with moderate to elevated levels of distractions may impair an individual's performance.
Karakasiliotis et al., 2006	Experimental research	179 participants	Social engineering	179 participants were 36% successful in identifying legitimate emails versus 45% illegitimate ones.
Weissman et al., 2006	Experimental research	16 participants	Region of Interest (ROI) analyses	Lapses impair goal-directed behavior.
Flehmig et al., 2007	Survey	222 participants	Neuroticism and cognitive failure liability	Positive correlations between N and general cognitive failure liability.
Furnell, 2007	Theoretical	179 participants	Phishing	People have significant problems in discriminating between messages based on the content alone.
Schneier & West, 2008	Theoretical	Prior research	Decision making	Security only becomes a priority for many when they have problems with it.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Vishwanath et al., 2011	Theoretical	161 e-mail users at a major university in the northeast USA	Phishing	Habitual media use patterns combined with high e-mail load levels significantly influence individuals' likelihood of being phished.
Chowdhury, 2016	Theoretical	20 mid and top-level managers from 10 large apparel manufacturing factories	Judgment errors	The respondents also have different interpretations of the term "error of Judgment" and "white-collar crime" are associated with OHS negligence and evasion.
Tay et al., 2016	Experimental research	128 medical students	Decision Making	Up to half of the medical students demonstrated complete or partial reliance on System 1 (intuitive) thinking
Wang et al., 2016	Survey	547 US consumers	Phishing	Coping adaptiveness was driven by a perceived threat, efficacy, and phishing anxiety, determining detection effort and accuracy.

Summary of What is Known and Unknown

With the presence of increasingly ingenious phishing schemes looking to steal identities and information for financial gain, it has become essential for organizations and government agencies to increase their users' awareness. Social engineering has become increasingly easier for cybercriminals with the added distraction of mobile phones in users' hands. Cyberslacking and environmental distractions such as conversations or background noise affect users' cognitive performance, sometimes negatively (Alharthi et al., 2019; Hernández et al., 2016). User distraction can negatively affect their ability to judge phishing schemes' validity in emails or malicious search engine links. Distracted users will often miss the phishing scheme's cues leading to stolen identities or financial losses for them and their organizations (Williams et al., 2018). Demographic factors such as age, gender, education, and social media usage level determine the likelihood of a user making a judgment error when dealing with phishing schemes (Gratian et al., 2018; Oliveira et al., 2017; Sheng et al., 2010). Security awareness training plays a decisive role in defending from phishing attacks; however, it is not entirely successful (Goode, 2018; Musuva et al., 2019; Rocha Flores & Ekstedt, 2016).

Judgment errors can occur in many different ways when distractions overload a person's cognitive processes. An overloaded cognitive process is a slow reaction and negatively affects spatial awareness when performing tasks. Slips or Lapses in attention can inhibit task performance and lead to errors in judgment when users are in distracting environments (Reason, 1984). System 1 and System 2 thinking helps users with cue processing in the performance of tasks. These processes can get interrupted by

environmental distractions leading to errors in judgment (Kahneman & Tversky, 1983; Tversky & Kahneman, 1981). Irrelevant stimuli can distract users from the visual cues that are used to detect phishing emails or PMSER links. This stimulus can affect a user's spatial awareness, leading to a successful phishing attempt.

Chapter 3

Methodology

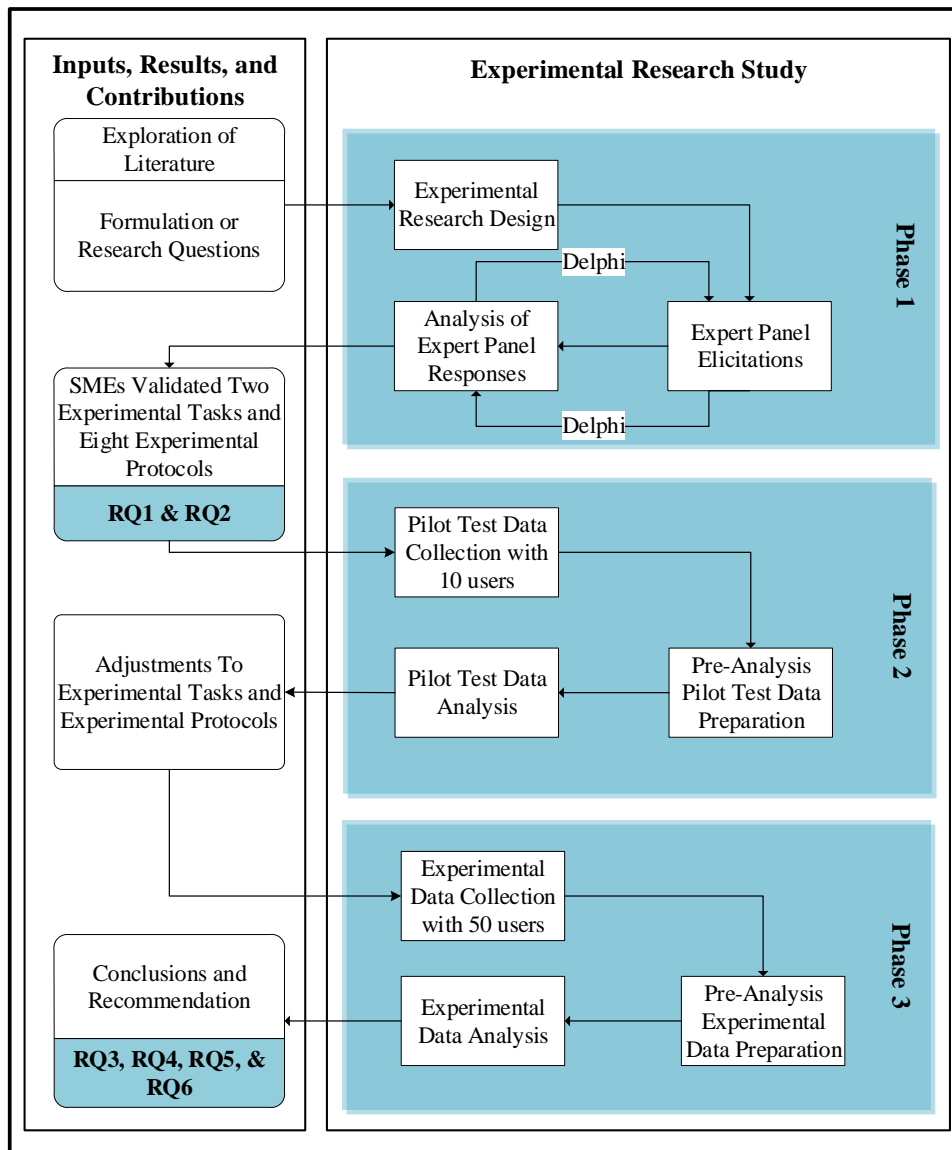
Overview of Research Design

This study is an experimental field research. This phase of the study documents the expert panel phases conducted with SMEs to validate the set of experiments before moving to the subsequent phases of the study. The expert panel research design process's model is based on the work of Tracey and Richey (2007), which uses the Delphi technique that uses a panel of SME 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).

To protect the validity of the experimental study, the research participants were informed of the significance of social engineering attacks, including phishing and PMSER. Along with the fact that they were 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 were informed of the phishing experiment's nature, they had a significant discrimination rate over the participants that were not told. 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 determine if the *two sets of tasks* and *eight experimental protocols* meet understandability, answerability, and readability standards (Ramim & Lichvar, 2014). Figure 2 illustrates the research design that this study will follow.

Figure 2

Overview of the Research Design Process



Phase 1 of this 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 and eight experimental protocols to assess users’ judgment when exposed to two types of simulated social engineering attacks (phishing &

PMSER). Phase 2 of this study will employ pilot testing of the SMEs' identified two sets of experimental tasks and eight experimental protocols to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER), two types of environments (distracting vs. non-distracting) and two types of devices used (mobile phone vs. computer). About 10 users were recruited for the pilot test of the SME validated two sets of experimental tasks and eight experimental protocols to make any needed adjustments. Finally, Phase 3 of this study was used to collect and analyze the experimental data from 50 users to find if any significant mean differences exist in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER).

Experimental Tasks and Measures

The first draft of the two sets of experimental tasks and eight experimental protocols were developed by exploring current literature from empirical research databases from varying fields of study such as IS, Cybersecurity, Psychology, and Finance. Phishing IQ and PMSER IQ tests, as shown in Table 5, were developed based on previous research to include a mixture of phishing emails and potentially malicious and legitimate SE links.

The administrative approach of the two sets of experimental tasks and eight experimental protocols were collected via e-mail using web-based Google forms based on a scoring scale for the SME's Delphi rounds. The SME input from each round was recorded, and changes to the experimental tasks and protocols were made based on the weight of the feedback based on the scale before the next round. The two sets of

experimental tasks and eight experimental protocols for this research study (Figure 3) were validated using the Delphi methodology by recruiting SMEs from the field of cybersecurity.

Figure 3

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

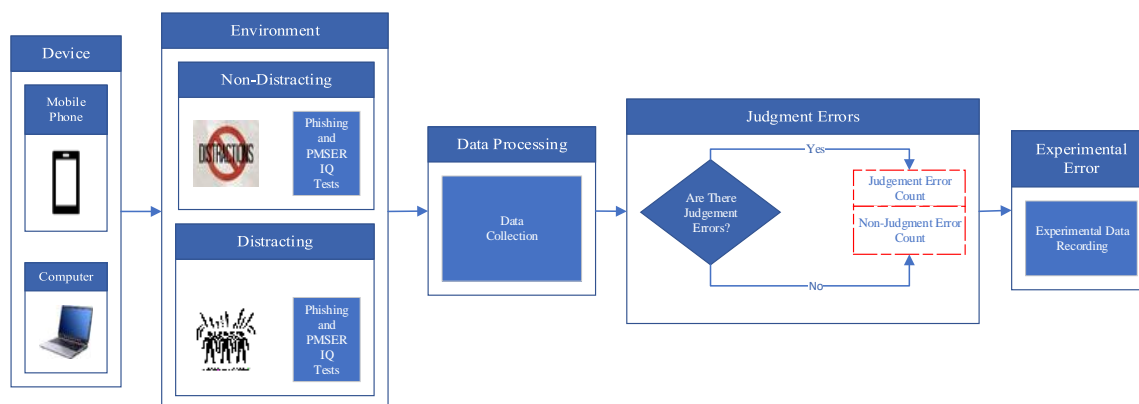
		Social Engineering Attack Type			
		Phishing		PMSER	
		Environment		Environment	
		Distracting	Non-Distracting	Distracting	Non-Distracting
Device	Mobile Phone	Distracted via Mobile Phone <ul style="list-style-type: none"> • Phishing Hard • Legitimate Easy • Phishing Easy 	Not Distracted via Mobile Phone <ul style="list-style-type: none"> • Legitimate Easy • Phishing Medium 	Distracted via Mobile Phone <ul style="list-style-type: none"> • Legitimate Easy • PMSER Easy • PMSER Medium • PMSER Hard 	Not Distracted via Mobile Phone <ul style="list-style-type: none"> • PMSER Easy • PMSER Medium • PMSER Hard
	Computer	Distracted via Computer <ul style="list-style-type: none"> • Phishing Easy • Phishing Medium • Phishing Hard 	Not Distracted via Computer <ul style="list-style-type: none"> • Phishing Medium • Phishing Hard • Legitimate Easy 	Distracted via Computer <ul style="list-style-type: none"> • PMSER Medium • PMSER Hard • Legitimate Easy 	Not Distracted via Computer <ul style="list-style-type: none"> • PMSER Hard • Legitimate Easy

The Delphi methodology involves a group communications process involving SMEs to provide SME feedback on a specific subject (Ramim & Lichvar, 2014). This research study conducted rounds of SME elicitations to ensure consensus while developing a) SMEs identified two sets of validated experimental tasks that need to be measured, and b) SMEs identified eight experimental protocols. The SME Delphi rounds

were used to develop two sets of experimental tasks (Figure 4) to measure users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). These two experimental tasks were 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 devices (mobile phone vs. computer).

Figure 4

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



Figures 5 and 6 detail a sample of the two experimental tasks and the eight experimental protocols presented to the SMEs for validation. The SMEs provided feedback on each question, and the highest weighted question among the feedback was chosen. An additional round may be necessary if the scores are tied for some questions or better suggestions are made that need to be voted on. RQ1 and RQ2 will collect the SME validation for the two experimental tasks and the eight experimental protocols. RQ3 and RQ4 will analyze the phishing and PMSER Pilot testing and experimental testing data

using a two-way Analysis of Variance (ANOVA). RQ5 and RQ6 will analyze the phishing and PMSER pilot and experimental testing data using a two-way Analysis of Covariance (ANCOVA).

Figure 5

Sample SME Survey of the Physical Environment Distractions

Which physical environment provides the **most distracting environment** for Mobile Phones and Computers?

- A. Airport
- B. Coffee Shop
- C. Lecture Hall
- D. Meeting

Which physical environment provides the **least distracting environment** for Mobile Phones and Computers?

- A. Office Setting
 - B. Home
 - C. Hotel room
 - D. Library/Bookstore
-

Figure 6

Sample SME Survey of the Audio/Visual Distraction Levels

Which audio/visual ***distraction level is best for a distracting environment*** for Mobile Phones and Computers?

- A. Continuous Background Noise
- B. Visual Distractions
- C. Distracting/Loud Music
- D. All of the above

Which audio/visual ***distraction level is best for a non-distracting environment*** for Mobile Phones and Computers?

- A. A Quiet Environment
- B. Relaxing Background Music
- C. No visual distractions
- D. All of the above

Validity and Reliability

Internal validity “encompasses whether the study results are legitimate because of the way the groups were selected, data was recorded or analysis performed” (Lakshmi & Mohideen, 2013, p. 2752). This research study utilized 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 study’s validity (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).

Reliability ensures consistent results are produced and makes “a statement about measurement accuracy” (Straub & Gefen, 2004, p. 400). Eliciting SMEs’ feedback will help ensure validity and reliability when developing measures for this research (Brown et al., 2015). Reliability and validity work hand in hand to ensure research accuracy (Creswell, 2013; Straub & Gefen, 2004). To ensure the validity and reliability of the SMEs’ validated two experimental tasks and eight experimental protocols, the questions for each mini phishing and PMSER IQ test were randomized into groups of three questions based on SME feedback. As shown in Table 4 and Figure 3, these groupings are broken down into legitimate, easy, medium, and hard questions for phishing and PMSER. Each group is separated into distracting and non-distracting testing environments for mobile phones and computers. The SMEs were asked to evaluate the randomization table and provide feedback on how to properly randomize each group’s questions to maintain the reliability of the two experimental tasks and eight experimental protocols.

Table 4*Phishing and PMSER Mini IQ Test Randomization Table*

Test Type	Group 1 Mobile Phone/ Non-Distracting	Group 2 Mobile Phone/ Distracting	Group 3 Computer/ Non- Distracting	Group 4 Computer/ Distracting
Phishing Mini IQ	Legitimate	Phishing Hard	Phishing Medium	Phishing Easy
Phishing Mini IQ	Phishing Easy	Legitimate	Phishing Hard	Phishing Medium
Phishing Mini IQ	Phishing Medium	Phishing Easy	Legitimate	Phishing Hard
PMSER Mini IQ	PMSER Easy	Legitimate	PMSER Hard	PMSER Medium
PMSER Mini IQ	PMSER Medium	PMSER Easy	Legitimate	PMSER Hard
PMSER Mini IQ	PMSER Hard	PMSER Medium	PMSER Easy	Legitimate

Having a large group of SMEs in a research study using the Delphi technique helps increase the study's reliability (Ono & Wedemeyer, 1994; Powell, 2003). A significant advantage of using the Delphi technique is that it leverages the SMEs' collective wisdom without the group setting's confrontational pressure. (Okoli & Pawlowski, 2004; Skinner et al., 2015). Therefore, this study will collect data from at least 25 SMEs and incorporate their input into the mini phishing and PMSER IQ tests to ensure the validity of the two sets of experimental tasks and eight experimental protocols.

SME Data and Analysis

A sample size of 25 cybersecurity SMEs for the Delphi rounds was 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 were recruited. SMEs were from the cybersecurity field in

industry and academia to provide a better diversity of skills and experience following the recommendation of Kennedy (2004) and Ramim and Lichvar (2014). The recruited SMEs provided input for the experimental research design process, as shown in Figure 2, the physical environment distractions in Figure 5, and audio/visual distraction levels in Figure 6.

This research study addressed 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 devices (mobile phone vs. computer). The Delphi methodology was also 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 devices (mobile phone vs. computer).

Table 5

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

IQ Test Number	IQ Test Type	IQ Test Topic	Simulation Type	IQ Test Scale
PH-IQ-01	Phishing	E-mail from the FBI about a banking transaction.	Phishing Easy	Legitimate, Phishing, or Ask IT Department
PH-IQ-02	Phishing	E-mail alert from Microsoft about login activity on account.	Phishing Medium	Legitimate, Phishing, or Ask IT Department

IQ Test Number	IQ Test Type	IQ Test Topic	Simulation Type	IQ Test Scale
PH-IQ-03	Phishing	E-mail alert from Experian about a change to a credit report.	Legitimate	Legitimate, Phishing, or Ask IT Department
PH-IQ-04	Phishing	E-mail alert from NETFLIX about account cancellation.	Phishing Medium	Legitimate, Phishing, or Ask IT Department
PH-IQ-05	Phishing	Reminder e-mail from PayPal about security upgrades to their system.	Phishing Hard	Legitimate, Phishing, or Ask IT Department
PH-IQ-06	Phishing	E-mail from Audible about a free audiobook service for kids.	Legitimate	Legitimate, Phishing, or Ask IT Department
PH-IQ-07	Phishing	E-mail alert from Google showing a new sign-in to account.	Phishing Medium	Legitimate, Phishing, or Ask IT Department
PH-IQ-08	Phishing	E-mail alert from Citibank stating that the account was locked out due to three failed login attempts.	Phishing Easy	Legitimate, Phishing, or Ask IT Department
PH-IQ-09	Phishing	Payment receipt from MCPROHOSTING for server space rental.	Legitimate	Legitimate, Phishing, or Ask IT Department
PH-IQ-10	Phishing	E-mail alert from Amazon regarding an item selling through their website.	Phishing Easy	Legitimate e-mail, Phishing e-mail, or Ask IT Department
PH-IQ-11	Phishing	E-mail advertisement asking the user to view travel offers for the state of Wisconsin.	Phishing Hard	Legitimate e-mail, Phishing e-mail, or Ask IT Department
PH-IQ-12	Phishing	E-mail alert from Cisco WebEx asking the user to update to an updated version of WebEx.	Phishing Hard	Legitimate, Phishing, or Ask IT Department
PM-IQ-01	PMSER	Search for Motillum using a search engine browser.	PMSER Easy	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-02	PMSER	Search for tickets for the 2010 Miss Universe pageant	PMSER Medium	Legitimate, Possibility

IQ Test Number	IQ Test Type	IQ Test Topic	Simulation Type	IQ Test Scale
		using a search engine browser.		Malicious, or Ask IT Department
PM-IQ-03	PMSER	Search for the term blockchain using a search engine browser.	PMSER Hard	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-04	PMSER	Search for hotels for an upcoming trip to Berlin, Germany using a search engine browser.	PMSER Hard	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-05	PMSER	Search for killer whales at SeaWorld using a search engine browser.	PMSER Easy	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-06	PMSER	Search for the malwaretips website using a search engine browser.	PMSER Medium	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-07	PMSER	Search for camping gear using a search engine browser.	PMSER Medium	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-08	PMSER	Searched for the 2018 midterm elections using a search engine browser	PMSER Easy	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-09	PMSER	Search for COVID-19 using a search engine browser.	Legitimate	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-10	PMSER	Search for the RuneScape download website using a search engine browser.	Legitimate	Legitimate, Possibility Malicious, or Ask IT Department
PM-IQ-11	PMSER	Search for the NFL tickets using a search engine browser.	Legitimate	Legitimate, Possibility Malicious, or Ask IT Department

IQ Test Number	IQ Test Type	IQ Test Topic	Simulation Type	IQ Test Scale
PM-IQ-12	PMSER	Search for information about the drug Procentra using a search engine browser.	PMSER Hard	Legitimate, Possibility Malicious, or Ask IT Department

The SMEs were given a four-part survey to provide feedback during the Delphi rounds. The first part provided a brief demographic background to ensure that they are cybersecurity professionals, as shown in Appendix D. The second part will consist of questions based on Figure 5 and Figure 6, based on the physical environment and AV distraction levels in Figure 7. Part three of the SME survey will contain a 12-question sample phishing e-mail IQ test, based on Table 5 and Appendix I. SMEs were asked their opinion of the sample of the emails, as shown in Figure 8, on whether to (a) *keep*; (b) *revise*; (c) *replace* each sample. Options B and C will have a section for SME comments on why they chose to revise or replace each sample. Part four of the survey will contain a 12-question sample PMSER IQ test, based on Table 5 and Appendix I. SMEs were asked their opinion of the sample of the SERs on whether to (a) keep; (b) revise; (c) replace each sample. As noted earlier, the revise and replace options will have an option for SME feedback to improve the process.

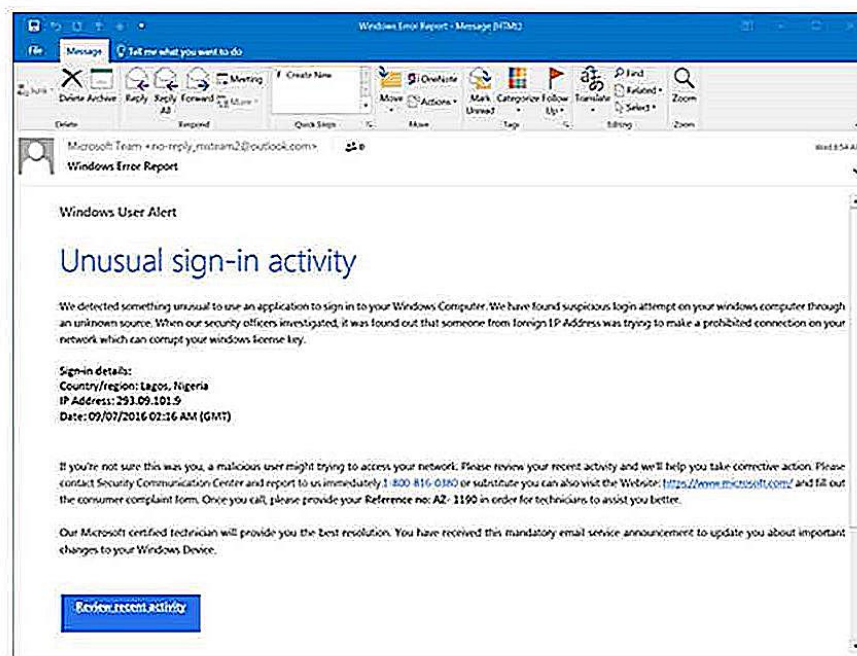
Figure 7*Environment Possibilities for Location and AV Distraction Levels for SMEs Survey*

Physical Environment	AV Distraction Levels
Airport	Continuous Background Noise
Coffee Shop	Visual Distractions
Lecture Hall	Distracting/Loud Music
Meeting	Quiet Environment
Office Setting	Relaxing Background Music
Home	No Visual Distractions
Hotel Room	
Library/Bookstore	

The data collected from the SME surveys were used to create eight mini-IQ tests based on the: environment and device type. These IQ tests are based on prior literature and industry tests. After the SME survey, an application delivery system was developed to collect quantitative and qualitative data from the research participants. Once the mini-IQ test was developed based on the SME's feedback in Phase 1, a pilot test was conducted with 10 participants to determine if any adjustments needed to be made to this research study's testing, data collection, and data analysis.

Figure 8

Sample Email Question for the SMEs Survey.



- A. Keep B. Revise C. Replace

Sample

The sample size for the pilot testing phase of this experimental research study was ten users recruited from a regional Virginia Community College staff and student population. These users were chosen based on age, gender, education, and computer experience levels to check for errors in the pilot testing process.

The sample size for this experimental research study included 68 users from varying demographic backgrounds (Boudreau et al., 2001, p. 5). The participants of this research study were recruited from all the regional Virginia Community College

campuses through flyers posted on bulletin boards in the communal areas and through campus e-mail. The student population has a diverse enrollment in terms of age, gender, education, and computer experience levels. Faculty and staff members were also included to help even out the numbers for age groups and add more diversity to the education levels. The likely ages of participants were also between 18 and 70 years of age, with the age groups broken down into generational groups according to sample size.

Pre-Analysis Data Screening

Pre-analysis data screening is used to “detect irregularities or problems with the collected data” (Levy, 2006, p. 150). Missing data must be evaluated before the final analysis to ensure consistency, validity, and reliability (Levy, 2006; Onwuegbuzie et al., 2010). For reporting accuracy, it is essential to correct any data entry errors. The visual checking or double entry methods can ensure no discrepancies between the testing data and what is entered into the statistical software (Barchard & Pace, 2011). The visual checking method involves a single-entry method in which each entry is verified visually from the test results as it is being entered. The double-entry method involves entering the test results twice and having software detect any discrepancies.

In order to correct any potential data entry errors, statistical methods such as correlation, frequency distributions, and simple and cross variable checking can be used to detect possible outliers that can skew the data (Barchard & Pace, 2011; Mavridis & Moustaki, 2008; Wilcox, 1998; Yuan & Zhong, 2008). Any out-of-range values can then be identified and corrected by statistical means such as histograms, frequency tables, and a Bonferroni correction (Barchard & Pace, 2011; Li et al., 2015). Any incomplete or

missing data is generally discarded by a majority of multivariate statistics algorithms, which can lead to skewed results due to overlooked data (Raymond & Roberts, 1987). Other methods that use mathematical comparisons or machine learning techniques are also available options when dealing with incomplete data (Aste et al., 2014; Van Der Palm et al., 2012). For this research study, every effort was made to ensure that the data entered was correct by double-checking every entry and not including any incomplete or missing data entries to prevent skewing the results by adding outliers.

Data Analysis

Figure 2 outlines the three phases of the data collection process for this research study. Phase 1 of this experimental research study collected data from 25 SME surveys from the Google forms spreadsheet. This SME data was sorted based on the SME demographics data, shown in Appendix D, and the scores provided on their responses, as shown in Figure 5 and Figure 6. The highest score was used to select the two experimental tasks and eight experimental protocols used for data collection for Phase 2 and Phase 3 testing for the experimental research participants.

Phase 2 of this experimental research study collected data from a ten experimental user pilot test of the SMEs validated two experimental tasks and eight experimental protocols following the methods, as shown in Figure 2. Figure 4 outlines the flow of the data collection methods of the two experimental tasks and eight experimental protocols for Phase 2 and Phase 3 of this experimental research. The data collected in Phase 2 was used to adjust the two SMEs-validated experimental tasks and the eight validated

experimental protocols. These adjustments were based on errors produced in the administration and data analysis procedures.

Phase 3 of this experimental research study will collect data from the adjusted experimental tasks and protocols shown in Figure 2. This data was processed using the methods shown in Figure 2, Figure 4, and Figure 9. Figures 2 and 4 show the data flow methods for administering, collecting, and analyzing the experimental data for the two experimental tasks and eight experimental protocols. Figure 4 shows the data analysis methods used in all three phases of this experimental research study.

Three types of analysis were conducted to assess the six research questions, as shown in Figure 10: The Delphi methodology, two-way ANOVA, and two-way ANCOVA. An initial proposal of two sets of experimental tasks and eight experimental protocols were developed from the literature exploration and submitted to the SMEs for validation. Appendices H, I, and J contain sample questions used to collect data from the research participants. Appendix G contains basic demographic questions, Appendix H contains Phishing IQ questions, and Appendix I contains PMSER IQ questions. The demographic data from Appendix G separated the IQ questions from Appendices H and I into distinct categories for statistical analysis.

This research study addressed 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 devices (mobile phone vs. computer). The Delphi methodology was also 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 devices (mobile phone vs. computer).

Figure 9

Research Questions and Methodology

RQ	Description	Methodology
RQ1	SMEs identified two sets of validated <i>experimental tasks</i> to assess users' judgment	Delphi
RQ2	What are the specific SMEs identified <i>eight experimental protocols</i> to assess the measures of users' judgment	Delphi
RQ3	Significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) in distracting vs. non-distracting environments.	Two-way ANOVA
RQ4	Significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when using a mobile phone vs. a computer.	Two-way ANOVA
RQ5	Statistically, 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 phone vs. computer).	Two-way ANOVA
RQ6	Significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when controlled for the users': (a) age, (b) gender, (c) education, and (d) level of social media usage	Two-way ANCOVA

To address RQ3, a two-way ANOVA was conducted to see any statistically significant mean differences in users' judgment when: exposed to two types of simulated social engineering attacks (phishing & PMSER). A two-way ANOVA also addressed RQ4 to determine if there are any significant mean differences in users' judgment when

exposed to two types of simulated social engineering attacks (phishing & PMSER) when using a mobile phone vs. a computer. A two-way ANOVA was also used to address RQ5 to determine if there were any significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER), based on the interaction of the types of environment (distracting vs. non-distracting) and type of device used (mobile phone vs. computer. A two-way ANCOVA was used to answer RQ6 to determine if there are any significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when controlled for the users': (a) age, (b) gender, (c) education, and (d) level of social media usage.

Resources

IRB approval was needed to collaborate with human subjects. Access to cybersecurity SMEs for following the Delphi technique SME panel process and research SMEs for developing the four experimental protocols. A Windows laptop or MacBook was provided for two protocols to access the four experimental protocols. A mobile device was provided for the other two protocols. The experimental protocols were administered in random order through a Google forms page for each protocol in the form of a phishing IQ test. A statistical tool was utilized following data collection to analyze the results.

Summary

Chapter Three included a description of the research design and methodology for this research study. This experimental research will use a combination of a Delphi

methodology and ANOVA and ANCOVA statistics. Phase 1 of this 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 and eight experimental protocols that need to be measured to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). Phase 2 will employ pilot testing of the SMEs' identified two sets of experimental tasks and eight experimental protocols to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER), two types of environments (distracting vs. non-distracting), and two types of devices used (mobile phone vs. computer). 10 users were recruited for the pilot test of the SME validated two experimental tasks and eight experimental protocols to make any needed adjustments. Finally, Phase 3 of this study was used to collect and analyze the experimental data from 50 users to find if any significant mean differences exist in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). Phase 3 included the research study conclusion and recommendations.

Chapter 4

Results

Overview

This chapter presents the data collection and analysis results from this research study. The main goal was to design, develop, and validate experimental settings to empirically test 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 phone vs. computer).

Phase I – SME Survey Feedback and Findings

RQ1 and RQ2 were answered through a survey instrument during the first phase of this research study. Invitation emails to participate in the Subject Matter Expert (SME) survey was sent to about 60 cybersecurity experts and a social media post on LinkedIn with a goal of 25 respondents. An SME panel of 28 cybersecurity experts participated in this Delphi study, and a consensus was met on the survey questions. Table 6 provides the descriptive statistics of the 28 respondents during the SME responses from March to May of 2021. The cybersecurity experts ranged from cybersecurity practitioners including network security engineers, Information Technology (IT) security analysts, information security managers, information technology auditors, cybersecurity administrators, cybersecurity consultants, cybersecurity architects, and senior IT executives.

Additionally, professors and researchers in cybersecurity were among the participants. Over 57.1% of the respondents had over 10 years of experience in cybersecurity or information

security, followed by 25% with five to 10 years of cybersecurity or information security experience. The rest fell into the five years or less category. While most of the cybersecurity SMEs in senior positions previously worked in various positions in cybersecurity, the SMEs were limited to only entering one current profession for the survey.

Table 6

Descriptive Statistics of SMEs (N=28)

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

As shown in Appendix H, the SMEs were asked to evaluate 12 sample emails for use in the mini-IQ tests for the experimental research. They were asked to evaluate each email sample and answer, as shown in Table 7, if the email sample was legitimate, phishing, or unsure. The

sample emails were a mixture of legitimate and various difficulty levels for the phishing emails (easy, medium, and hard). As indicated in Table 7, some email samples had a higher level of unsure responses as the difficulty increased.

Table 7

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

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

Email Phishing Sample	Frequency	Percentage
Unsure	2	7.1%
Sample 9		
Legitimate	9	32.1%
Phishing	7	25%
Unsure	12	42.9%
Sample 10		
Legitimate	0	0%
Phishing	28	100%
Unsure	0	0%
Sample 11		
Legitimate	6	21.4%
Phishing	16	57.1%
Unsure	6	21.4%
Sample 12		
Legitimate	5	17.9%
Phishing	18	64.3%
Unsure	5	17.9%

The SMEs were also asked to provide feedback on whether to keep, revise, or replace the sample emails they evaluated from Table 7. As shown in Table 8, most SMEs chose to keep all the email samples. The SMEs were also asked to provide feedback on why they chose the revise or replace options and any additional feedback that might improve the email samples. Some vital feedback on the revisions came from the over 60 age group on adjusting the image quality on two samples to be more readable for all participants.

Table 8

SME Feedback on Email Sample Edits (N=28)

Email Phishing Sample	Frequency	Percentage
<i>Please provide your expert opinion about the email sample above by indicating: Keep, Revise, or Replace</i>		
Sample 1		
Keep	21	75%
Revise	6	21.4%
Replace	1	3.6%

Email Phishing Sample	Frequency	Percentage
Sample 2		
Keep	23	82.1%
Revise	2	7.1%
Replace	3	10.7%
Sample 3		
Keep	20	71.4%
Revise	7	25%
Replace	1	3.6%
Sample 4		
Keep	25	89.3%
Revise	1	3.6%
Replace	2	7.1%
Sample 5		
Keep	22	78.6%
Revise	3	10.7%
Replace	3	10.7%
Sample 6		
Keep	25	89.3%
Revise	2	7.1%
Replace	1	3.6%
Sample 7		
Keep	22	78.6%
Revise	5	17.9%
Replace	1	3.6%
Sample 8		
Keep	21	75%
Revise	6	21.4%
Replace	1	3.6%
Sample 9		
Keep	14	50%
Revise	8	28.6%
Replace	6	21.4%
Sample 10		
Keep	26	92.9%
Revise	1	3.6%
Replace	1	3.6%
Sample 11		
Keep	23	82.1%
Revise	2	7.1%
Replace	3	10.7%

Email Phishing Sample	Frequency	Percentage
Sample 12		
Keep	26	92.9%
Revise	1	3.6%
Replace	1	3.6%

The SMEs were asked to evaluate 12 PMSER samples as shown in Appendix I for future experimental research use in the mini-IQ tests. They were asked to evaluate whether each email sample and answer, as shown in Table 9, was whether the PMSER was legitimate, potentially malicious, or unsure. The PMSER samples were a mixture of legitimate and various difficulty levels for the PMSER samples (easy, medium, and hard).

Table 9

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

PMSER Sample	Frequency	Percentage
<i>Please identify the sample PMSER above as one of the following: Legitimate, Potentially Malicious, or Unsure</i>		
Sample 1		
Legitimate	3	10.7%
Potentially Malicious	22	78.6%
Unsure	3	2.7%
Sample 2		
Legitimate	13	36.4%
Potentially Malicious	12	42.9%
Unsure	3	10.7%
Sample 3		
Legitimate	8	28.6%
Potentially Malicious	14	50%
Unsure	6	21.4%
Sample 4		
Legitimate	21	75%
Potentially Malicious	5	17.9%
Unsure	2	7.1%
Sample 5		
Legitimate	6	21.4%
Potentially Malicious	16	57.1%

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

The SMEs were also asked to provide feedback on whether to keep, revise, or replace the PMSER samples they evaluated from Table 9. As shown in Table 10, most SMEs chose to keep all the PMSER samples. The SMEs were also asked to provide feedback on why they chose the revise or replace options and any additional feedback that might improve the PMSER samples.

As with the sample email feedback on the revisions, the image quality will be adjusted on all samples to be more readable for all participants.

Table 10

SME Feedback on PMSER Sample Edits (N=28)

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

PMSER Sample	Frequency	Percentage
Replace	1	3.6%
Sample 9		
Keep	27	96.4%
Revise	0	0%
Replace	1	3.6%
Sample 10		
Keep	27	96.4%
Revise	0	0%
Replace	1	3.6%
Sample 11		
Keep	27	96.4%
Revise	0	0%
Replace	1	3.6%
Sample 12		
Keep	25	89.3%
Revise	1	3.6%
Replace	2	7.1%

The SMEs were asked to evaluate the mobile phone and computer users' topmost and least distracting environments. Table 11 indicates that 50% of the SMEs found that an airport was the most distracting environment for mobile phone and computer users. 35.7% of the SMEs also found that a home environment was the least distracting for mobile phone and computer users, with an office setting coming into a close second place.

Table 11

SME Feedback of Physical Distracting Environments (N=28)

Environment	Frequency	Percentage
<i>Which physical environment provides the most distracting environment for Mobile Phones and Computers?</i>		
Airport	14	50%
Coffee Shop	5	17.9%
Lecture Hall	0	0%
Meeting	9	32.1%
<i>Which physical environment provides the least distracting environment for Mobile Phones and Computers?</i>		

Environment	Frequency	Percentage
Office Setting	8	28.6%
Home	10	35.7%
Hotel room	6	21.4%
Library/Bookstore	4	14.3%

The SMEs were asked to evaluate the topmost and least Audio/Visual (A/V) distraction levels for mobile phone and computer users. Table 12 shows that 67.9% of the SMEs chose all the above for the most distracting A/V distraction level, including continuous background noise, visual distractions, and distracting/loud music. 46.4% of the SMEs chose all the above for the most distracting A/V distraction level, including a quiet environment, relaxing background music, and no visual distractions.

Table 12

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

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

The SMEs were asked to evaluate the randomization table in Figure 3 and provide feedback on whether to keep, revise, or replace the randomization. About 89.3% indicated that the randomization table should be kept. The SMEs were also asked whether to keep, revise, or replace the number of questions for each mini-IQ test with three questions each. About 75% of

the SMEs responded that the number of mini-IQ questions should be kept to three. As with the email and PMSER sample questions, the SMEs were asked to provide feedback on why they chose the revised or replace options and any additional feedback that might improve the randomization and question size.

Table 13

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

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

Figure 3 indicates the question randomization for the email and PMSER questions given to the pilot study participants and the main research study participants. Randomization was necessary to maintain the research study's quality and validity. The difficulty of the phishing and PMSER questions is evenly distributed to reduce the chance that all easy questions are asked in non-distracting environments, and all hard questions are asked in distracting environments.

The SMEs were asked to provide feedback on the pilot and experimental testing procedures, as shown in Table 14, on whether to keep, revise, or replace each procedure. For the pilot-testing procedures, 96.4% of the SMEs selected to keep the pilot testing procedure 1. For pilot testing procedures 2 and 3, the SMEs responded with an 89.3% majority to keep the

procedures. For experimental procedure 1, 92.9% of the SMEs chose to keep the procedure. Experimental procedure 2 had an 89.3% majority for keeping the procedure. Finally, for experimental procedure 3, there was an 85.7% majority to keep the procedure. The SMEs that chose to revise or replace were asked to provide feedback on why they chose to revise or replace options on all the procedures and any additional feedback that might improve the testing procedures.

Table 14

Pilot Testing and Experimental Testing Procedures

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

Experimental Testing Procedure	Frequency	Percentage
<i>Main Experimental Procedure 2: Email interested experimental testing participants a zoom meeting link to conduct experimental testing and assign a participant ID.</i>		
Keep	25	89.3%
Revise	2	7.1%
Replace	1	3.6%
<i>Main Experimental Procedure 3: Experimental test participants were given links to the mini-IQ tests to complete while in a monitored simulated environment (distracting or non-distracting) via Zoom. Each participant was asked to enter their assigned participant ID for each IQ test for data tracking purposes.</i>		
Keep	24	85.7%
Revise	2	7.1%
Replace	2	7.1%

Phase II – Pilot Testing

This study is experimental field research and documents the pilot testing phase conducted with research volunteers to validate the set of experiments validated by the SMEs during the Delphi round. The Expert Panel Research Design Process's model is based on the work of Tracey and Richey (2007), which uses the Delphi technique that uses a panel of SME analysis and feedback (See Figure 3). The Delphi technique is a fundamental methodology in situations where accurate information is not available, and expert judgment is needed (Ramim & Lichvar, 2014). The SME panel determined if the two sets of tasks and eight experimental protocols meet understandability, answerability, and readability standards (Ramim & Lichvar, 2014).

Participants were asked to take four short Mini-IQ surveys using their mobile phones and computers in non-distracting and distracting environments. This was important to finalize the delivery method and data analysis for the mini-IQ tests for the phishing and PMSER experiments. The participants were given instructions that included links for the non-distracting environment phase and a zoom link for the distracting environment phase to be observed. This

was important to ensure that the distracting sound file was played while taking the surveys. The participants were then asked to identify the one sound in the sound file that distracted them the most to ensure that they were distracted by the audio. The sound file was developed based on the SME's feedback in the Delphi rounds. Six soundtracks were combined into the sound file consisting of crowd noise from an office and two airports, a crying baby, circus music, and a random distracting sound found on YouTube.

Invitation emails to participate in the pilot testing surveys were sent to about 20 potential participants to reach a 50% response rate or 10 respondents. 10 respondents participated in this pilot test, answering questions based on the SME-validated tasks and procedures. Table 15 provides the descriptive statistics of the 10 participants during the pilot test, which took place in December of 2021. The participants were both males and females, ages 30 to 59.

Table 15.

Descriptive Statistics of Pilot Test Participants (N=10)

Demographics Indicator	Frequency	Percentage
Age		
18-19	4	5.9%
20-29	31	45.6%
30-39	18	26.5%
40-49	4	5.9%
50-59	9	13.2%
Over 60	2+	2.9%
Gender		
Female	36	52.9%
Male	32	47.1%
Education		
High School Diploma	29	42.6%
2-year College (Associates Degree)	17	25%
4-year College (Bachelor's degree)	20	8.8%
Graduate degree	25	14.7%
Doctorate/Professional	3	8.8%

Demographics Indicator	Frequency	Percentage
Social Media Usage		
Never	2	2.9%
Occasionally	18	26.5%
Sometimes	20	29.4%
Often	25	36.8%

The participants' educational backgrounds included highly educated pilot participants, with 60% with Doctoral/Professional degrees and 40% with Graduate degrees. The participants' social media usage had 50% Often, 30% Sometimes, 10% Occasionally, and 10% Never.

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

Phishing email and PMSER samples were then created following the three levels of detection (easy, medium, & hard) for each social engineering type and were validated using SMEs. Each response was coded based on the severity of the identified email or link, as indicated in Table 16. Moreover, for each mini-IQ test, three samples were provided, and scoring across all three was summed, indicating a scoring from three (3x1) to 18 (3x6).

Table 16.*Scoring of Mini-IQ Responses for Phishing and PMSER Selections*

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

Figure 10 summarizes the participant results from the aggregated testing data across all eight mini-IQ tests on the two devices, two environments, and two types of social engineering simulated attacks. The phishing mini-IQ test results do not follow what was initially indicated in prior literature. Specifically, it was surprising to learn that the non-distracting environment results for the Phishing IQ tests were overall lower than those of distracting environment, which is counter to what was envisioned (See Figure 10 & Figure 11a).

Figure 10.*Pilot Test Summary of Participants' Results (N=10)*

Phishing IQ					PMSER IQ					
	Distracting		Non-Distracting			Distracting		Non-Distracting		
	Mean	St.Dev	Mean	St.Dev		Mean	St.Dev	Mean	St.Dev	
Mobile	14.80	2.10	13.70	1.95	14.00	2.05	14.50	3.14	Mobile	
Computer	14.90	3.96	12.40	3.47	14.00	2.11	15.20	1.81	Computer	

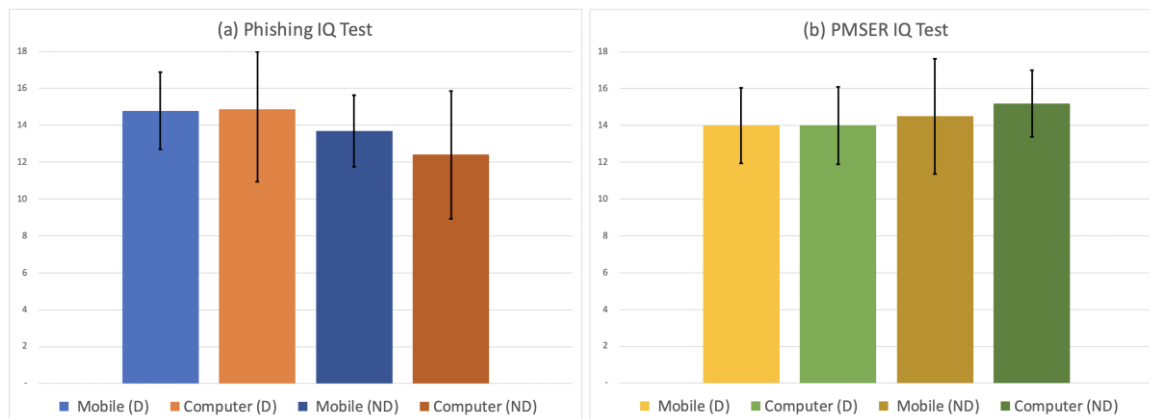
These Phishing IQ test results may be assumed to be because, during the distracting environment, the participants were monitored over zoom to enable the distracting sound file. In

contrast, in the non-distracting environment, they have marked the selections independently and may have rushed to identify the phishing samples. Additionally, counter to the initial expectation from literature, it was found that computer users from our pilot results in a non-distracting environment resulted in the lowest scoring. In contrast, computer users in distracting environments appeared to have scored the highest, again counterintuitive results. They may require further investigation during this study's full data collection results (See Figure 10 & Figure 11b). However, the PMSER IQ test results were as expected, with overall scores on both mobile and computer in a distracting environment being lower than those in a non-distracting environment.

In contrast, PMSER detection on a computer outperformed mobile devices. It is suspected that these results are more accurate as individuals' familiarity with PMSER is much lower. Their habituation to such messages is more deficient, causing them to pay closer attention and be more precise in their detections. A two-way ANOVA was conducted on the results. While it appears that some variations do exist, as presented in Table 17 and Figure 10, none of the comparisons were significant for Phishing IQ tests by environment ($F=3.714$, $p=0.061$) or device type ($F=0.380$, $p=0.541$), and PMSER IQ tests by environment ($F=1.383$, $p=0.247$) or device type ($F=0.228$, $p=0.636$).

Figure 11.

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



A two-way ANCOVA was also conducted on the overall scores of all eight mini-IQ tests based on the demographics indicators and found that, at least from the results of this pilot study, no demographics indicator evaluated provided any significant differences among the pilot study participants.

Phase III - Main Research Study

This study is experimental field research and documents the main research testing phase conducted with research volunteers to validate the set of experiments validated by the pilot testing phase and the SMEs during the Delphi round. The Expert Panel Research Design Process's model is based on the work of Tracey and Richey (2007), which uses the Delphi technique that uses a panel of SME analysis and feedback (See Figure 3). The Delphi technique is a fundamental methodology in situations where accurate information is not available, and expert judgment is needed (Ramim & Lichvar, 2014). The SME panel determined if the two sets of tasks and eight experimental protocols meet understandability, answerability, and readability standards (Ramim & Lichvar, 2014).

Participants were asked to take four short Mini-IQ surveys using their mobile phones and computers in non-distracting and distracting environments. The participants were given revised instructions in Appendix J that included links for the non-distracting environment phase and a zoom link for the distracting environment phase to be observed. This was important to ensure that the distracting sound file was played while taking the surveys. The instructions had to be revised from the pilot study because participants had difficulty following the current instructions as written. The participants were then asked to identify the one sound in the sound file that distracted them the most to ensure that they were distracted by the audio. The sound file was developed based on the SME's feedback in the Delphi rounds. Six soundtracks were combined into the sound file consisting of crowd noise from an office and two airports, a crying baby, circus music, and a random distracting sound found on YouTube.

Phase III – Pre-Analysis Data Screening

There were 68 total participants in this study. Invitation emails to participate in the main testing surveys were sent to about 500 potential participants from Tidewater Community College to reach a 10% response rate of 50 respondents. A group of 68 respondents participated in this main research testing, answering questions based on the adjustments made after the pilot testing phase. IBM SPSS Statistics version 27 was used to analyze the scored answers of the main research study participants.

Phase III - Participant Demographics Characteristics

Table 17 provides the descriptive statistics of the 68 participants during the main, from January to March of 2022. The participants were both males and females, ages 18 to over 60. Gender was evenly distributed with 36 female participants and 32 male participants.

Table 17*Descriptive Statistics of Main Study Participants (N=68)*

Demographics Indicator	Frequency	Percentage
Age		
18-19	4	5.9%
20-29	31	45.6%
30-39	18	26.5%
40-49	4	5.9%
50-59	9	13.2%
Over 60	2	2.9%
Gender		
Female	36	52.9%
Male	32	47.1%
Education		
High School Diploma	29	42.6%
2-year College (Associates Degree)	17	25%
4-year College (Bachelor's degree)	20	8.8%
Graduate degree	25	14.7%
Doctorate/Professional	3	8.8%
Social Media Usage		
Never	2	2.9%
Occasionally	18	26.5%
Sometimes	20	29.4%
Often	25	36.8%
Always	3	4.4%

The participants' educational backgrounds included participants from the whole education spectrum, with 8.8% with Doctoral/Professional degrees, 14.7% with Graduate degrees, 8.8% with 4-year College (Bachelor's degrees), 25% with 2-year College (Associates Degrees), and 42.6% with High School Diplomas. The participants' social media usage had 3% always, 36.8% Often, 29.4% Sometimes, 26.5% Occasionally, and 2.9% Never.

Phase III – Data Scoring

The mini-IQ tests were developed based on previous research to include a mixture of phishing emails and potentially malicious and legitimate search engine links. Participants were asked to identify if the image of an email or a search engine link was legitimate and given a seven-answer scale 1) Strongly Disagree, 2) Disagree, 3) Somewhat Disagree, 4) Neither Agree nor Disagree, 5) Somewhat Agree, 6) Agree, 7) Strongly Agree, as shown in Table 18, to score their level of agreement. After viewing the pilot study results, these answer choices were revised from a three-answer scale 1) Legitimate, 2) Phishing/potentially Malicious, 3) Ask IT Department to improve the statistical measures and level of agreement. This change was supported by reviewing the SME feedback, in which some of the respondents suggested that having three answer choices was not adequate. There were three legitimate emails, three legitimate links, nine non-legitimate emails, and nine non-legitimate links. For the emails and PMSER links, to avoid user fatigue and have the user remember the social engineering samples provided, a randomized list was generated to include easy, medium, and hard to detect samples to ensure the level of detection is not constant as it is in confirmed cases of social engineering.

Table 18

Mini IQ Test-Revised Survey Answers

Answer Choice	Level of Agreement
1	Strongly Disagree
2	Disagree
3	Somewhat Disagree
4	Neither Agree or Disagree
5	Somewhat Agree

Answer Choice	Level of Agreement
6	Agree
7	Strongly Agree

Phishing email and PMSER samples were then created following the three levels of detection (easy, medium, & hard) for each social engineering type and were validated using SMEs. Each response was coded based on the severity of the identified email or link, as indicated in Table 19. Moreover, seven samples were provided for each mini-IQ test, and scoring across all seven was summed, indicating a scoring from seven (7x1) to 10. Some of the scores were given equal weights to assign the same score to opposite sides of the spectrum for correct or incorrect answers from the participants.

Table 19.

Scoring of Mini-IQ Responses for Phishing and PMSER Selections

<i>Actual</i>	<i>Participant's Selection</i>	<i>Score</i>
Non-Legitimate	Strongly disagree	10
Legitimate	Strongly agree	10
Non- Legitimate	Disagree	9
Legitimate	Agree	8
Legitimate	Somewhat agree	7
Non- Legitimate	Somewhat disagree	6
Legitimate	Neither agree or disagree	6
Non- Legitimate	Neither agree or disagree	5
Legitimate	Somewhat disagree	5
Non- Legitimate	Somewhat agree	4
Non- Legitimate	Agree	3
Legitimate	Disagree	2
Legitimate	Strongly disagree	1
Non- Legitimate	Strongly agree	1

Phase III Findings

Figure 12 summarizes the participant results from the aggregated testing data across all eight mini-IQ tests on the two devices, two environments, and two types of social engineering simulated attacks. The phishing mini-IQ test results now follow what was initially indicated in prior literature for mobile devices with lower mean scores than computers due to smaller screen sizes. However, the score for the computer is slightly higher than the non-distracting environment. Specifically, results for the Phishing IQ and PMSER tests were overall lower for the mobile devices than those of the computers in a distracting environment, which is what was envisioned (See Figure 12 & Figure 13a).

The anomalous scores for the computer in a distracting environment and a mobile phone in a non-distracting environment could be from survey fatigue. The 29 and under demographic group appears to be habituated to using the smaller display size on mobile devices. It is assumed that these Phishing and PMSER IQ test results may be because, during the distracting environment, the participants were monitored over zoom to enable the distracting sound file. In contrast, in the non-distracting environment, they have marked the selections independently and may have rushed to identify the phishing samples.

Figure 10

Main Study Summary of Participants' Results (N=68)

Phishing IQ Test					PMSER IQ Test					
	Distracting		Non-Distracting			Distracting		Non-Distracting		
	Mean	St.Dev	Mean	St.Dev		Mean	St.Dev	Mean	St.Dev	
Mobile	17.01	5.53	19.26	4.26	Mobile	17.26	4.46	18.32	4.90	Mobile
Computer	19.60	5.19	18.56	4.68	Computer	17.88	3.76	18.88	4.49	Computer

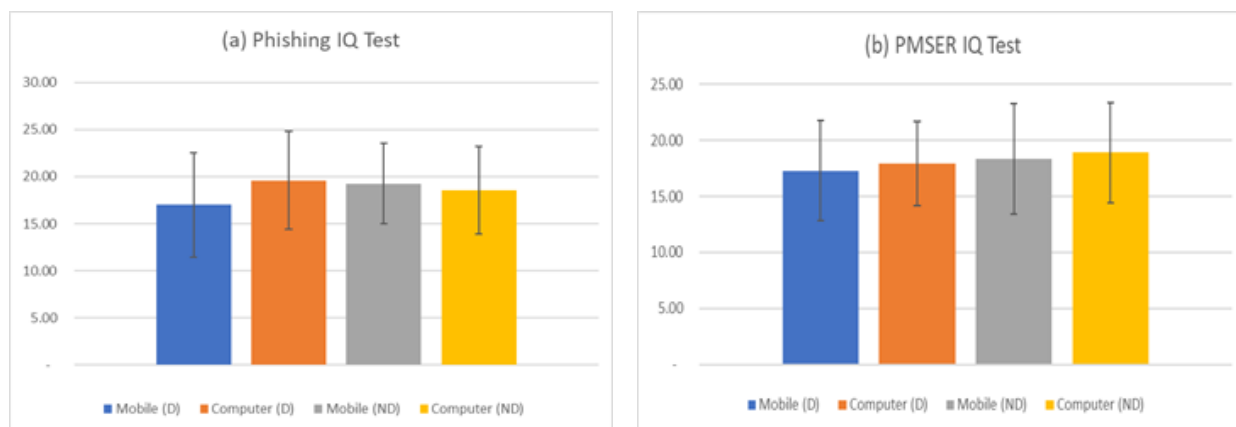
Additionally, it was found that mobile users from our main research resulted in a distracting environment with the lowest scoring, which is in line with prior literature. In contrast, computer users in distracting environments appeared to have scored the highest, which are counterintuitive results. They may require further investigation with this study's full data collection results (See Figure 12 & Figure 13b). However, the PMSER IQ test results were as expected, with overall scores on both mobile and computer in a distracting environment being lower than those in a non-distracting environment.

In contrast, PMSER detection on a computer outperformed mobile devices. It is suspected that these results are more accurate as individuals' familiarity with PMSER is much lower. Their habituation to such messages is more deficient, causing them to pay closer attention and be more precise in their detections. A two-way ANOVA was conducted on the results. While it appears that some variations do exist, as presented in Figure 12 and Figure 13, none of the comparisons were significant for Phishing IQ tests by environment ($F=0.985$, $p=0.322$) or device

type ($F=2.413$, $p=0.122$) and PMSER IQ tests by environment ($F=3.692$, $p=0.056$) or device type ($F=1.195$, $p=0.275$).

Figure 13.

Results of the Main Study Mini-IQ Tests for Phishing IQ (a) and PMSER (b)



A two-way ANCOVA was also conducted on the overall scores of all eight mini-IQ tests based on the demographics indicators and found that, at least from the results of this main research study, the Education demographics indicator showed significant differences among the main research study participants.

Phase III RQ3

Are there significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) in distracting vs. non-distracting environments? A two-way ANOVA was evaluated for significant differences between groups. The results of the two-way ANOVA showed there were no significant differences among both groups for Phishing and PMSER. Phishing ($F=0.985$, $p=0.322$), PMSER ($F=3.692$, $p=0.056$).

The p -values of the F -test were greater than the .05 level of significance. Results are shown in Table 20 and Table 21.

Table 20

ANOVA Results of Phishing IQ vs. Environment (N=68)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	24.721 ^a	1	24.721	.985	.322
Intercept	94205.309	1	94205.309	3753.770	.000
Environment	24.721	1	24.721	.985	.322
Error	6775.971	270	25.096		
Total	101006.000	272			
Corrected Total	6800.691	271			

Table 21

ANOVA Results of PMSER IQ vs. Environment (N=68)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	72.059 ^a	1	72.059	3.692	.056
Intercept	88994.118	1	88994.118	4559.624	.000
Environment	72.059	1	72.059	3.692	.056
Error	5269.824	270	19.518		
Total	94336.000	272			
Corrected Total	5341.882	271			

This section represents the results of descriptive statistics between groups for Phishing IQ and PMSER IQ vs. Environment among all 68 participants. Descriptive statistics for RQ3 are shown in Table 22 and Table 23. The results show that the research participants performed worse in distracting environments based on the mean comparisons in Table 23 and Table 24, including graphical representation in Figures 14 and Figure 15 for estimated marginal means.

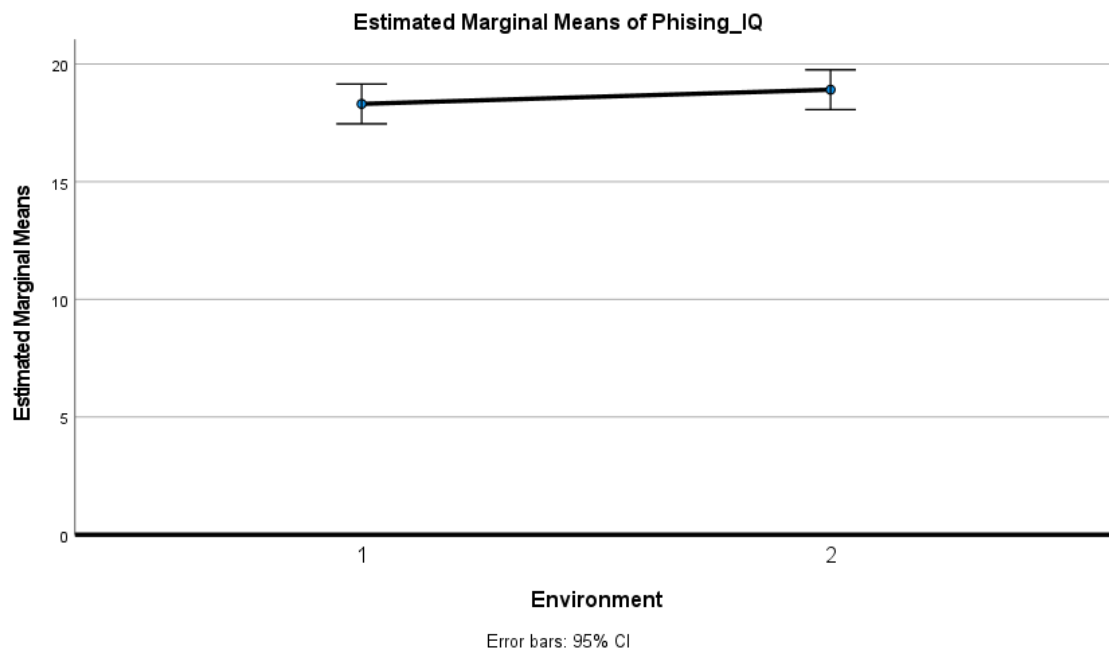
Table 22

Descriptive Statistics of Phishing IQ vs. Environment (N=68)

Environment	Mean	Std. Deviation	N
Distracting (1)	18.31	5.498	136
Non-Distracting (2)	18.91	4.468	136
Total	18.61	5.009	272

Figure 14

Mean Score for Phishing IQ vs. Environment (N=68)

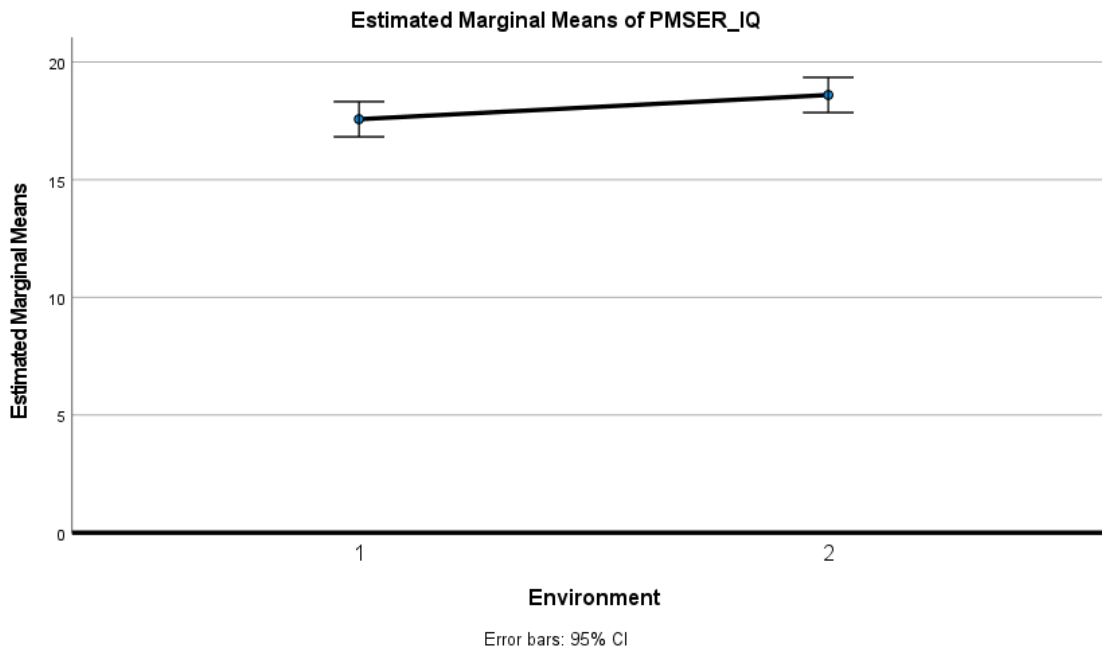
**Table 23**

Descriptive Statistics of PMSER IQ vs. Environment (N=68)

Environment	Mean	Std. Deviation	N
Distracting (1)	17.57	4.123	136
Non-Distracting (2)	18.60	4.694	136
Total	18.09	4.440	272

Figure 15

Mean Score for PMSER IQ vs. Environment (N=68)



Phase III RQ4

Are there significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when using a mobile phone vs. a computer? A two-way ANOVA was evaluated for significant differences between groups. The results of the two-way ANOVA showed there were no significant differences among both groups for Phishing and PMSER. Phishing ($F=2.413$, $p=0.122$), PMSER ($F=1.195$, $p=0.275$). The p -values of the F -test were greater than the .05 level of significance. Results are shown in Table 24 and Table 25.

Table 24*ANOVA Results of Phishing IQ vs. Device Type (N=68)*

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	60.235 ^a	1	60.235	2.413	.122
Intercept	94205.309	1	94205.309	3773.548	.000
Device Type	60.235	1	60.235	2.413	.122
Error	6740.456	270	24.965		
Total	101006.000	272			
Corrected Total	6800.691	271			

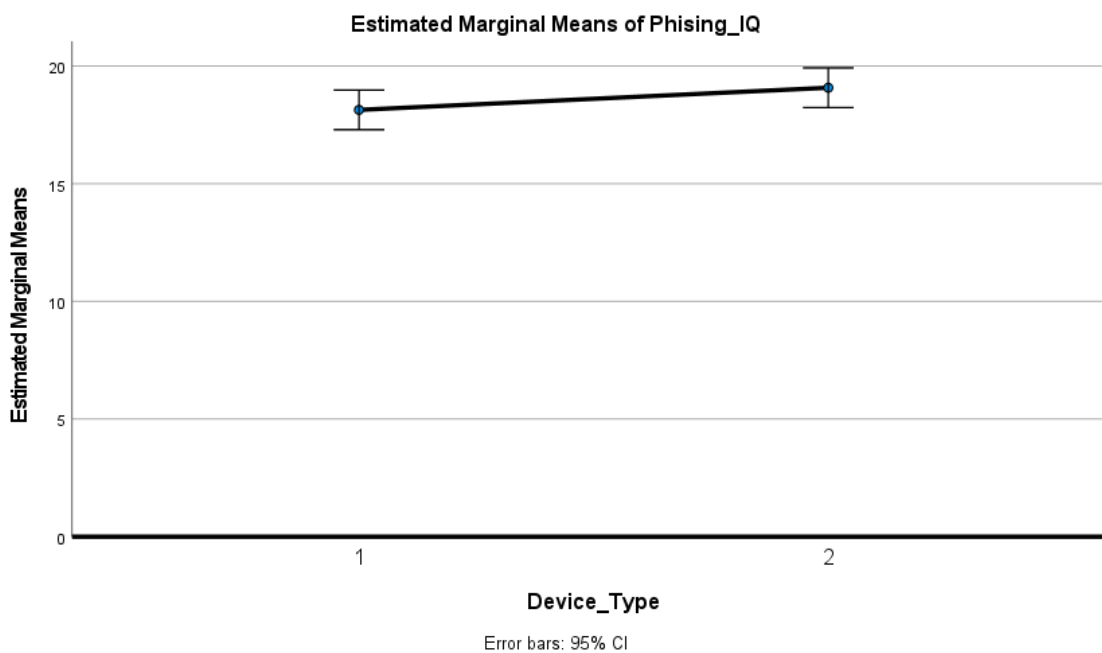
Table 25*ANOVA Results of PMSER IQ vs. Device Type (N=68)*

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	23.529 ^a	1	23.529	1.195	.275
Intercept	88994.118	1	88994.118	4518.018	.000
Device Type	23.529	1	23.529	1.195	.275
Error	5318.353	270	19.698		
Total	94336.000	272			
Corrected Total	5341.882	271			

This section represents the results of descriptive statistics between groups for Phishing IQ and PMSER IQ vs. Device Type among all 68 participants. Descriptive statistics for RQ4 are shown in Table 28 and Table 29. Based on mean comparisons in Table 26 and Table 27, including graphical representation in Figure 16 and Figure 17 for estimated marginal means, the computers outperformed the mobile devices.

Table 26*Descriptive Statistics of Phishing IQ vs. Device Type (N=68)*

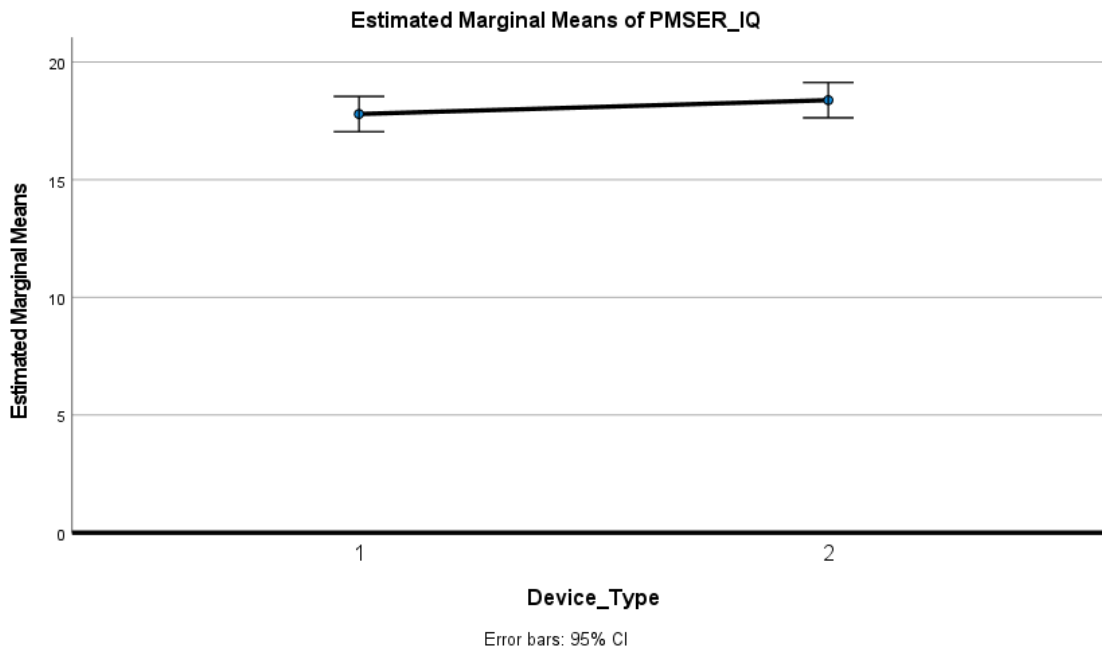
Device Type	Mean	Std. Deviation	N
Mobile (1)	18.14	5.045	136
Computer (2)	19.08	4.947	136
Total	18.61	5.009	272

Figure 16*Mean Score for Phishing IQ vs. Device Type (n=68)***Table 27***Descriptive Statistics of PMSER IQ vs. Device Type (N=68)*

Device Type	Mean	Std. Deviation	N
Mobile (1)	17.79	4.702	136
Computer (2)	18.38	4.158	136
Total	18.09	4.440	272

Figure 17

Mean Score for PMSER IQ vs. Device Type (n=68)



Phase III RQ5

Are there statistically 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 phone vs. computer)? A two-way ANOVA was evaluated for significant differences between groups. The results of the two-way ANOVA showed there were significant differences among both groups for Phishing and PMSER vs. Device Type and Environment. Phishing ($F=3.685$, $p=0.013$), PMSER ($F=1.629$, $p=0.183$). The p -values of the F -test for the Phishing IQ vs. Device Type and Environment were lower than the .05 level of significance. Results are shown in Table 28 and Table 29.

Table 28*ANOVA Results of Phishing IQ vs. Device Type and Environment (N=68)*

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	269.426 ^a	3	89.809	3.685	.013
Intercept	94205.309	1	94205.309	3865.564	.000
Environment	24.721	1	24.721	1.014	.315
Device Type	60.235	1	60.235	2.472	.117
Environment * Device Type	184.471	1	184.471	7.569	.006
Error	6531.265	268	24.370		
Total	101006.000	272			
Corrected Total	6800.691	271			

Table 29*ANOVA Results of PMSER IQ vs. Device Type and Environment (N=68)*

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	95.647 ^a	3	31.882	1.629	.183
Intercept	88994.118	1	88994.118	4546.198	.000
Environment	72.059	1	72.059	3.681	.056
Device Type	23.529	1	23.529	1.202	.274
Environment * Device Type	.059	1	.059	.003	.956
Error	5246.235	268	19.576		
Total	94336.000	272			
Corrected Total	5341.882	271			

This section represents the results of descriptive statistics between groups for Phishing IQ and PMSER IQ vs. Device Type and Environment among all 68 participants. Descriptive statistics for RQ5 are shown in Table 30 and Table 31. Based on mean comparisons shown in Table 31 and

Table 32, including graphical representation in Figure 18 and Figure 19 for estimated marginal means, the computer outperformed the mobile device for all PMSER measures. However, for the Phishing IQ, the mobile device outperformed the computer slightly in a non-distracting environment.

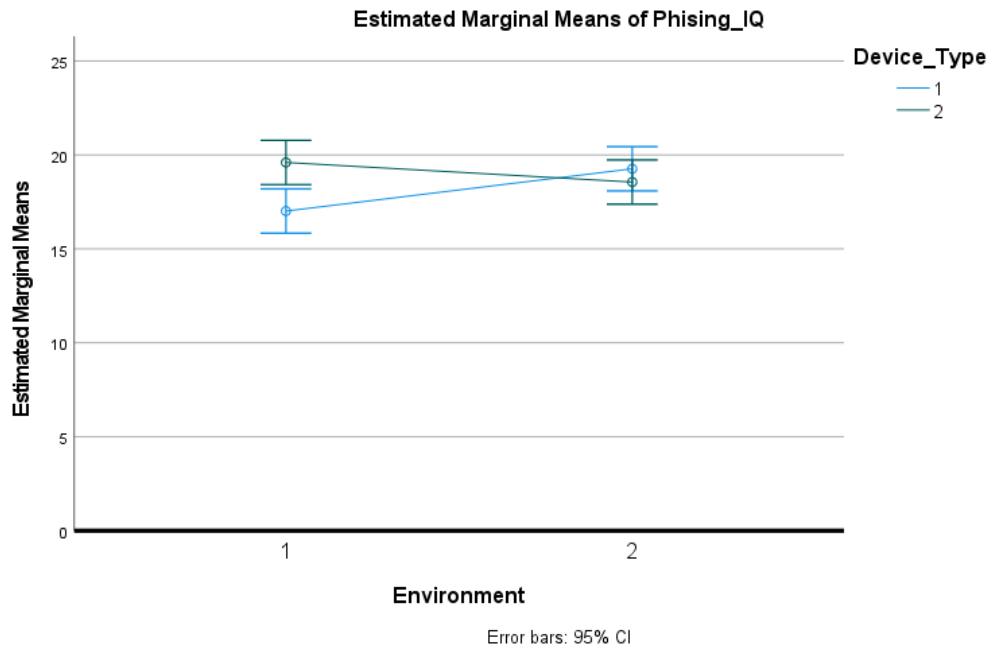
Table 30

Descriptive Statistics of Phishing IQ vs. Device Type (Mobile (1) and Computer (2)) and Environment (N=68)

Environment	Device Type	Mean	Std. Deviation	N
Distracting (1)	Mobile (1)	17.01	5.533	68
	Computer (2)	19.60	5.186	68
	Total	18.31	5.498	136
Non-Distracting (2)	Mobile (1)	19.26	4.255	68
	Computer (2)	18.56	4.676	68
	Total	18.91	4.468	136
Total	Mobile (1)	18.14	5.045	136
	Computer (2)	19.08	4.947	136
	Total	18.61	5.009	272

Figure 18

Mean Score for Phishing IQ vs. Device Type (Mobile (1) and Computer (2)) and Environment (N=68)

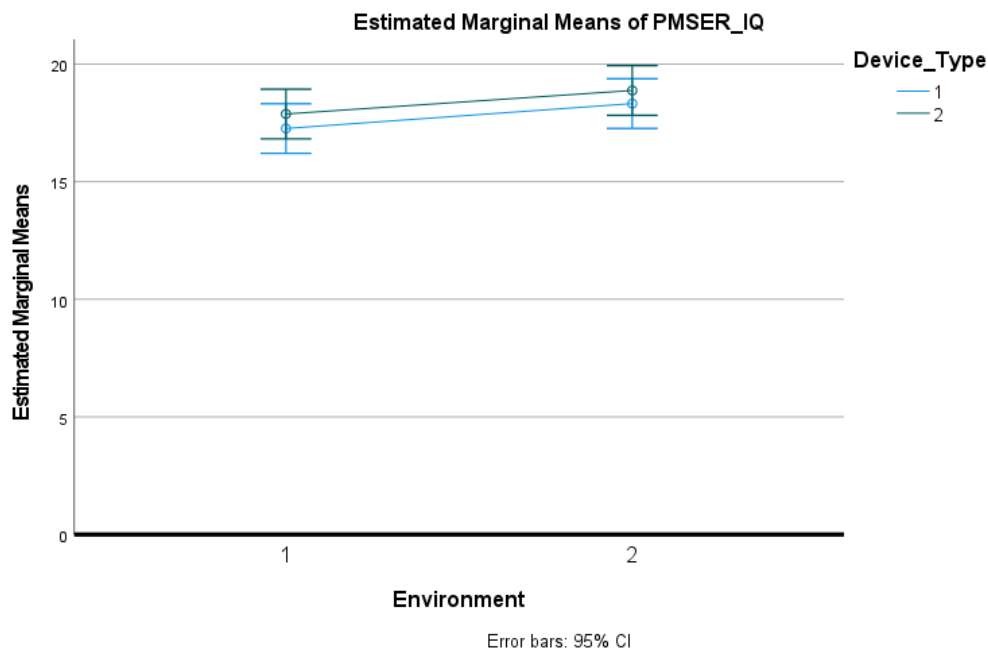
**Table 31**

Descriptive Statistics of PMSER IQ vs. Type (Mobile (1) and Computer (2)) and Environment (N=68)

Environment	Device Type	Mean	Std. Deviation	N
Distracting (1)	Mobile (1)	17.26	4.464	68
	Computer (2)	17.88	3.760	68
	Total	17.57	4.123	136
Non-Distracting (2)	Mobile (1)	18.32	4.903	68
	Computer (2)	18.88	4.494	68
	Total	18.60	4.694	136
Total	Mobile (1)	17.79	4.702	136
	Computer (2)	18.38	4.158	136
	Total	18.09	4.440	272

Figure 19

Mean Score for PMSER IQ vs. Type (Mobile (1) and Computer (2)) and Environment (N=68)



Phase III RQ6

Are there any significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when controlled for the users': (a) age, (b) gender, (c) education, and (d) level of social media usage? A two-way ANCOVA was used to evaluate for significant differences between groups. The results of the two-way ANCOVA showed there were significant differences among both groups for Phishing vs. Environment and Device Type plus PMSER vs. Environment and Device Type. Phishing vs. Environment ($F=1.521$, $p=0.183$), Phishing vs. Device Type ($F=1.817$, $p=0.110$) PMSER vs. Environment ($F=3.779$, $p=0.003$), and PMSER vs. Device Type ($F=3.230$, $p=0.008$). The p -values of the F -test for the PMSER IQ vs. Environment and Device Type were lower than the

.05 level of significance. Also, the Education covariate for Table 32($F=3.930$, $p=0.048$), Table 33($F=3.951$, $p=0.048$), Table 34($F=10.429$, $p=0.001$), and Table 35($F=10.329$, $p=0.001$) was lower than the .05 level of significance. Results are shown in Table 32 and Table 33 for the Phishing IQ and Table 34 and Table 35 for the PMSER IQ.

Table 32

ANCOVA Results of Phishing IQ vs. Environment with Demographic Covariates(N=68)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	189.087 ^a	5	37.817	1.521	.183
Intercept	2755.166	1	2755.166	110.847	.000
Age	1.150	1	1.150	.046	.830
Gender	28.410	1	28.410	1.143	.286
Education	97.682	1	97.682	3.930	.048
Social Media	6.553	1	6.553	.264	.608
Environment	24.721	1	24.721	.995	.320
Error	6611.605	266	24.856		
Total	101006.000	272			
Corrected Total	6800.691	271			

Table 33

ANCOVA Results of Phishing IQ vs. Device Type with Demographic Covariates(N=68)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	224.601 ^a	5	44.920	1.817	.110
Intercept	2755.166	1	2755.166	111.445	.000
Age	1.150	1	1.150	.047	.829
Gender	28.410	1	28.410	1.149	.285
Education	97.682	1	97.682	3.951	.048
Social Media	6.553	1	6.553	.265	.607
Device Type	60.235	1	60.235	2.436	.120
Error	6576.090	266	24.722		
Total	101006.000	272			

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Total	6800.691	271			

Table 34

ANCOVA Results of PMSER IQ vs. Environment with Demographic Covariates(N=68)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	354.318 ^a	5	70.864	3.779	.003
Intercept	2461.733	1	2461.733	131.291	.000
Age	12.577	1	12.577	.671	.414
Gender	17.825	1	17.825	.951	.330
Education	195.548	1	195.548	10.429	.001
Social Media	6.582	1	6.582	.351	.554
Environment	72.059	1	72.059	3.843	.051
Error	4987.564	266	18.750		
Total	94336.000	272			
Corrected Total	5341.882	271			

Table 35

ANCOVA Results of PMSER IQ vs. Device Type with Demographic Covariates(N=68)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	305.789 ^a	5	61.158	3.230	.008
Intercept	2461.733	1	2461.733	130.026	.000
Age	12.577	1	12.577	.664	.416
Gender	17.825	1	17.825	.941	.333
Education	195.548	1	195.548	10.329	.001
Social Media	6.582	1	6.582	.348	.556
Device Type	23.529	1	23.529	1.243	.266
Error	5036.093	266	18.933		
Total	94336.000	272			
Corrected Total	5341.882	271			

This section represents the results of descriptive statistics between groups for Phishing IQ and PMSER IQ vs. Device Type and Environment, including the four demographic covariates among all 68 participants. Descriptive statistics for RQ6 are shown in Table 36, Table 37, Table 38, and Table 39. Based on mean comparisons shown in Table 36, Table 37, Table 38, and Table 39, including graphical representation in Figure 20, Figure 21, Figure 22, and Figure 23 for estimated marginal means, the computer outperformed the mobile device for all measures and the distracting environment performed better than the non-distracting environment as expected.

Table 36

Descriptive Statistics of Phishing IQ vs. Environment with Demographic Covariates (N=68)

Environment	Mean	Std. Deviation	N
Distracting (1)	18.31	5.498	136
Non-Distracting (2)	18.91	4.468	136
Total	18.61	5.009	272

Figure 20

Mean Score for Phishing IQ vs. Environment with Demographic Covariates (N=68)

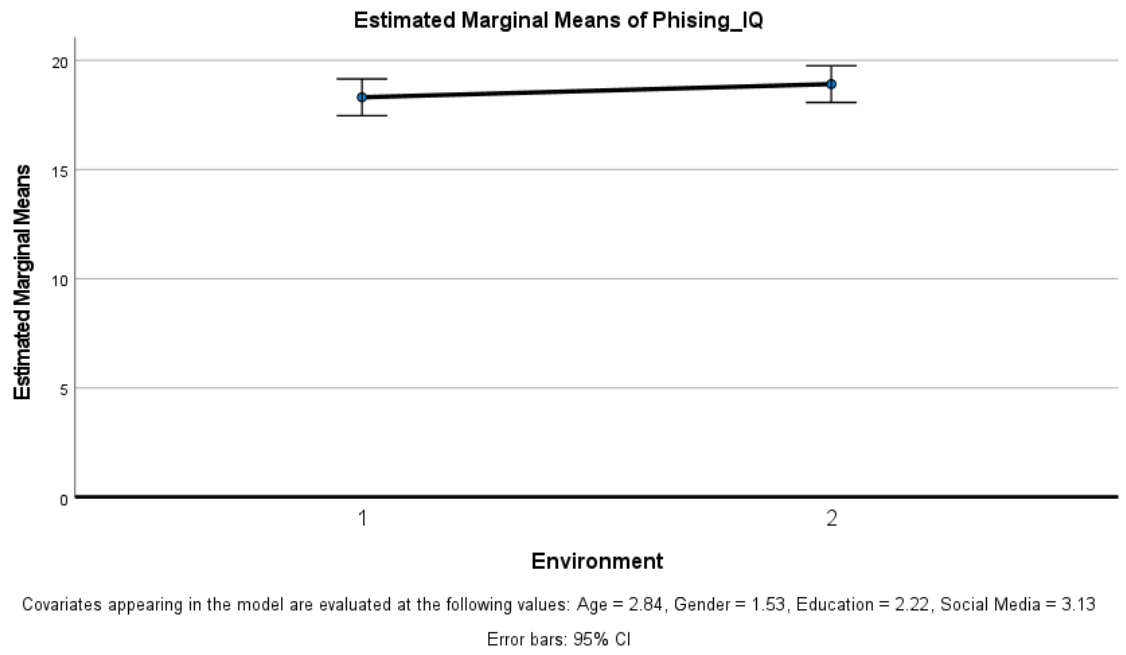


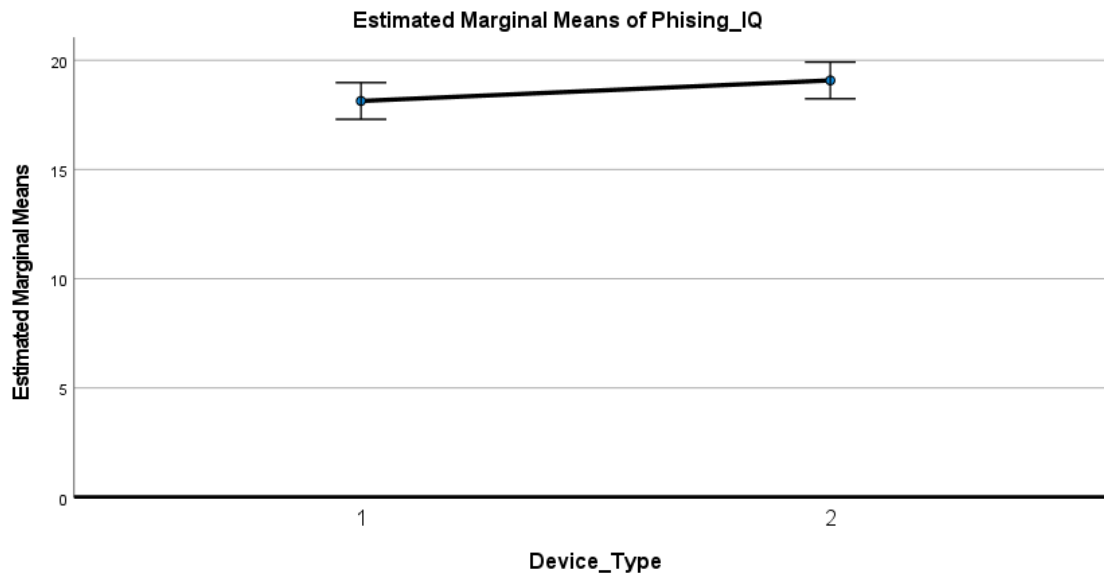
Table 37

Descriptive Statistics of Phishing IQ vs. Device Type with Demographic Covariates (N=68)

Device Type	Mean	Std. Deviation	N
Mobile (1)	18.14	5.045	136
Computer (2)	19.08	4.947	136
Total	18.61	5.009	272

Figure 21

Mean Score for Phishing IQ vs. Device Type with Demographic Covariates (N=68)

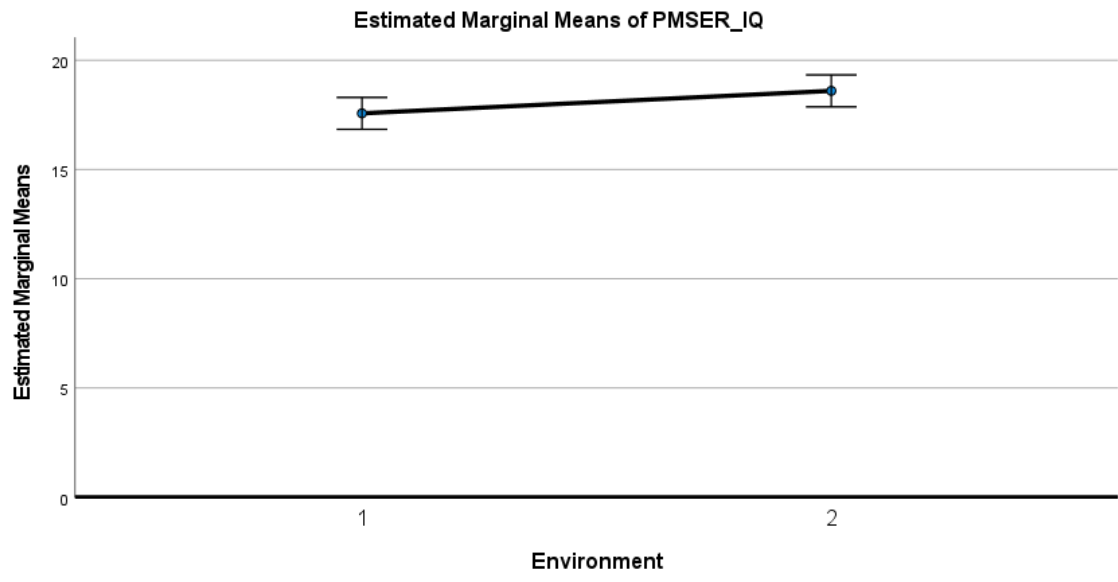
**Table 38**

Descriptive Statistics of PMSER IQ vs. Environment with Demographic Covariates (N=68)

Environment	Mean	Std. Deviation	N
Distracting (1)	17.57	4.123	136
Non-Distracting (2)	18.60	4.694	136
Total	18.09	4.440	272

Figure 22

Mean Score for PMSER IQ vs. Environment with Demographic Covariates (N=68)



Covariates appearing in the model are evaluated at the following values: Age = 2.84, Gender = 1.53, Education = 2.22, Social Media = 3.13
 Error bars: 95% CI

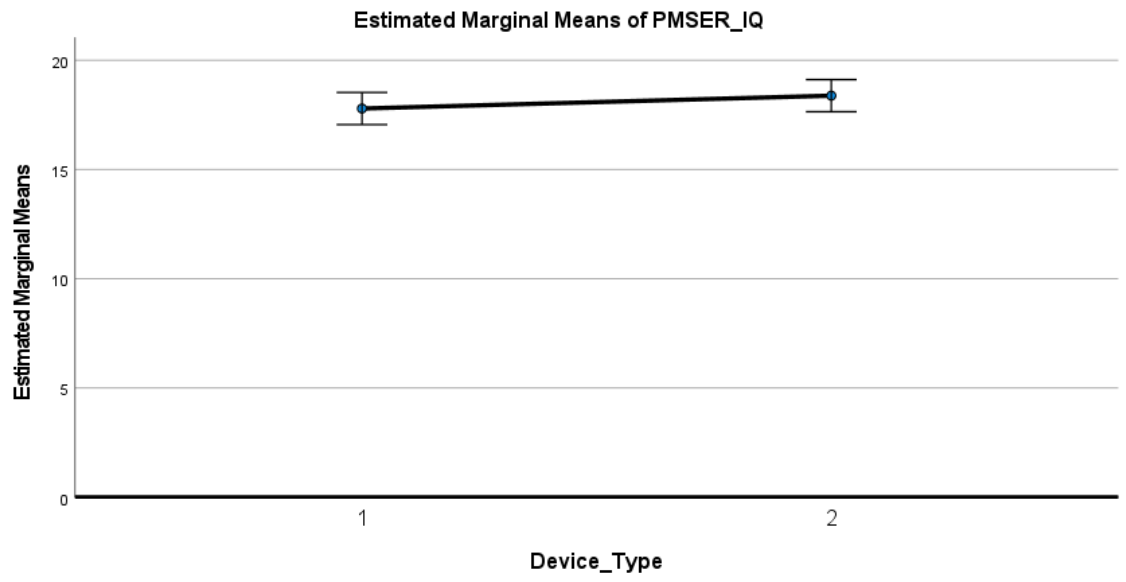
Table 39

Descriptive Statistics of PMSER IQ vs. Device Type with Demographic Covariates (N=68)

Device Type	Mean	Std. Deviation	N
Mobile (1)	17.79	4.702	136
Computer (2)	18.38	4.158	136
Total	18.09	4.440	272

Figure 23

Mean Score for PMSER IQ vs. Device Type with Demographic Covariates (N=68)



Covariates appearing in the model are evaluated at the following values: Age = 2.84, Gender = 1.53, Education = 2.22, Social Media = 3.13
Error bars: 95% CI

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

This study presents the results of the experimental testing process previously validated by the SMEs to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) during two kinds of environments (distracting vs. non-distracting) and two types of devices (mobile phone vs. computer). This study is relevant as it seeks to identify the vulnerabilities of information systems users exposed to two types of simulated social engineering attacks (phishing & PMSER), which adversaries commonly use to gain access to an individual's personal or organizational accounts for monetary gain. With the widespread use of mobile phones with Internet-connected applications, phishing attempts have increased through social engineering through scams and clickbait links. Frauenstein and Flowerday (2016) stated that users pick up bad habits by using link-sharing applications that leave them vulnerable to phishing attacks. These bad habits make it harder for people to discern between genuine and malicious links making them more susceptible to phishing attacks. Moreover, the significance of this research is in its potential to advance the current research in cybersecurity by increasing the body of knowledge regarding users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER). Distracting environments at work and in public make it easier for a user to have errors in judgment when performing tasks. Attackers craft phishing attacks to try and distort the mental model users form in interacting with online transactions and distract them from the visual cues they usually notice. As the number of distractions increases, cognitive cues decrease, affecting decision-making due to cognitive overload (Kahneman, 1973).

The results of this study provide initial input to the body of knowledge of users' susceptibility to social engineering attacks in distracting environments while using mobile phones and computers.

Discussion

Like any research study, this study has several limitations. The main limitation of this pilot testing procedure is that all interactions with the participants were conducted remotely due to COVID-19 restrictions. All measures have been taken to ensure that the distracting and non-distracting environments mimic reality. Still, it is understandably valid that users may be preconditioned during an experiment versus the full impact of such environments in natural settings. Another limitation was that the participants were limited to identifying phishing and PMSER samples to graphical images only due to limitations of survey distributions. This limitation can be mitigated by having an application created to hover over links to see if they lead to where they indicate. Another limitation was that the instructions for the testing procedures had to be changed a few times to ensure that our message was clear to the study participants on what they were asked to do. Our recruitment of research participants that had experience in pilot testing procedures helped mitigate this limitation. This change did help with the overall completion of the main study. One last limitation is that the survey instruments did not allow research participants to hover over links to determine whether a phishing email or SER was valid. All care was taken in the design process to try and mitigate this limitation, but this limitation could not be mitigated altogether.

Implications

There are several implications for cybersecurity, social awareness, and phishing susceptibility reduction. This study implicates that reducing distracting environments in the

workplace, at home, and in public may significantly reduce social engineering susceptibility.

This study also implicates that education level may play a significant role in social engineering susceptibility. Having a robust training program for the workforce may significantly reduce social engineering susceptibility in the workplace.

Implications for Practice

Organizations could potentially reduce the severity of social engineering for both organizational and personal data loss by implementing training programs that help increase user awareness of the potential dangers of distracting environments and help identify social engineering attempts to gain access to organizational data and systems.

Implications for Research

Implications for research indicate additional discovery on what phishing and PMSER IQ combinations could be created to increase further ability to notice social engineering attempts through phishing emails and malicious SERs. A more controlled environment during testing phases may also help improve the testing scores in distracting and non-distracting environments to see if there are significant mean differences between device type and environment. This research had a high level of high school graduates under the education demographic (40%) compared to the rest of the education levels. This potential limitation can be mitigated by recruiting from a more diverse pool that is more representative of the current population outside of an educational institution. Having a more balanced demographic pool based on age, gender, education level, and social media usage may help identify if more demographic covariate factors have a significant mean difference 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). Having the ability to add visual distractions into the experiment would also likely improve the quality of research. Also, adding distractions such as pop-up windows, notifications, and text notifications would add a layer of realism to the testing of mobile phones and computers.

Recommendations and Future Research

Another round of testing in a more controlled environment during testing should be performed. This change may help improve the testing scores in distracting and non-distracting environments to see if there are significant mean differences between device type and environment. Some surprising results occurred during the pilot testing phase. Unexpected results such as this may need to be investigated further to see if any new facts are discovered that can contribute to the body of knowledge or identify potential flaws in the research. 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). Thus, additional assessments of the experimental data with the interaction of different demographic indicators may help further uncover potential groups that are more susceptible to social engineering attacks.

Summary

In summary, this research assessed users' susceptibility to social engineering attacks in distracting and non-distracting environments while using mobile phones and computers.

The main research question (RQ) that this study addressed was: Are there any statistically 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 phone vs. computer) and included RQ1, RQ2, RQ3, RQ4, RQ5, and RQ6:

- RQ1. What are the specific 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 devices (mobile phone vs. computer)?
- RQ3. Are there significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) in distracting vs. non-distracting environments?
- RQ4. Are there significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when using a mobile phone vs. a computer?
- RQ5: Are there statistically 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 phone vs. computer)?

RQ6: Are there any significant mean differences in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) when controlled for the users': (a) age, (b) gender, (c) education, and (d) level of social media usage?

Phase I answered RQ1 through the SMEs, validating the 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 phone vs. computer)? RQ2 was answered by the SMEs, validating *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 devices (mobile phone vs. computer)? The phishing and PMSER IQ tests were paired with SME-validated physical and AV environmental factors for testing in a remote environment.

Phase II included building the surveys and pilot testing the SME validated tasks and measures from RQ1 and RQ2. The participants' instructions for accessing the surveys for the non-distracting environmental testing also included some FAQs and the email address to contact us to set up testing appointments for the distracting environment testing. A Zoom link was also provided to monitor the participants during the distracting environment testing phase.

Phase III included recruitment and the delivery of the testing instructions and the testing participation of the respondents who answered the following research questions RQ3, RQ4, RQ5, and RQ6.

RQ3 and RQ4 were answered by evaluating the research data with a two-way ANOVA. The results of the two-way ANOVA showed there were no significant differences among both groups for Phishing and PMSER.

RQ5 was answered by evaluating the research data with a two-way ANOVA. The results of the two-way ANOVA showed there were significant differences among both groups for Phishing and PMSER vs. Device Type and Environment.

RQ6 was answered by evaluating the research data with a two-way ANCOVA. The results of the two-way ANCOVA showed there were significant differences among both groups for Phishing vs. Environment and Device Type plus PMSER vs. Environment and Device Type. Specifically, the Education covariate for Table 32($F=3.930$, $p=0.048$), Table 33($F=3.951$, $p=0.048$), Table 34($F=10.429$, $p=0.001$), and Table 35($F=10.329$, $p=0.001$) was lower than the .05 level of significance.

Overall, this study developed and evaluated an experimental testing process previously validated by SMEs to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) during two kinds of environments (distracting vs. non-distracting) and two types of devices (mobile phone vs. computer).

Appendix A

Institutional Review Board Approval Letter

MEMORANDUM

To: **Tommy Pollock**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **April 7, 2020**

Re: **IRB #: 2020-167; Title, "Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

Appendix B

Site Approval Letter



TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

DISTRICT ADMINISTRATION

August 6, 2020

Nova Southeastern University
3301 College Avenue
Fort Lauderdale, FL 33314-7796

Subject: Site Approval Letter

To whom it may concern:

This letter acknowledges that I have received and reviewed a request by Tommy Pollock to conduct a research project entitled "Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors" at Tidewater Community College and I approve of this research to be conducted at our facility.

When the researcher receives approval for his/her research project from the Nova Southeastern University's Institutional Review Board/NSU IRB, I agree to provide access for the approved research project. If we have any concerns or need additional information, we will contact the Nova Southeastern University's IRB at (954) 262-5369 or irb@nova.edu.

Sincerely,

Curtis K. Aasen
Vice President for Information Systems and Institutional Effectiveness
Phone: (757) 822-1010
Email: caasen@tcc.edu

CHESAPEAKE NORFOLK PORTSMOUTH SUFFOLK VIRGINIA BEACH

P.O. Box 9000 Norfolk Virginia 23509-9000 • Telephone: 757-822-1122 • www.tcc.edu

Appendix C

Example of SME Recruitment E-mail

Dear Cybersecurity Experts,

I need your help in providing feedback on developing two sets of validated experimental tasks and eight experimental protocols for my upcoming doctoral research study. I am a Ph.D. Candidate in Information Assurance at the College of Computing and Engineering, Nova Southeastern University (NSU), working under Dr. Yair Levy's supervision and a member of his [Levy CyLab](#).

My research seeks to assess users' judgment when exposed to two types of simulated social engineering attacks (phishing & Potentially Malicious Search Engine Results (PMSE)). I am also seeking to develop eight experimental protocols to assess the measures of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSE), in two kinds of environments (distracting vs. non-distracting), and two types of devices (mobile phone vs. computer).

In this part of the research, I need your assistance in the validation of two sets of experimental tasks for device vs. environment. The sets are as follows:

Set 1: Phishing

1. Mobile phone usage in distracting and non-distracting environments.
2. Computer usage in distracting and non-distracting environments.

Set 2: PMSE

1. Mobile phone usage in distracting and non-distracting environments.
2. Computer usage in distracting and non-distracting environments.

I also need your assistance in validating the eight experimental protocols measuring user judgment errors in device vs. environment simulations. The eight protocols are:

1. Distracted via Mobile Phone (phishing).
2. Not Distracted via Mobile Phone (phishing).
3. Distracted via computer (phishing).
4. Not Distracted via Computer (phishing).
5. Distracted via Mobile Phone (PMSE).
6. Not Distracted via Mobile Phone (PMSE).
7. Distracted via Computer (PMSE).
8. Not Distracted via Computer (PMSE).

The information provided was used for this research study and in an aggregated form. No Personally Identifiable Information (PII) was collected. As a participant, you agree to keep all information regarding this research confidential and refrain from disclosing any details related to this survey or its material. If you are willing to participate in developing these research protocols, please respond to this e-mail. Upon receiving your reply, a follow-up e-mail was sent to you with the research protocols for the device vs. environment and the measurement of judgment errors.

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. Should you wish to receive the study's findings, please indicate them with your reply to this e-mail. I was happy to provide you with information about the academic research publication(s) resulting from this study.

Respectfully,
Tommy Pollock
Doctoral Candidate in Information Assurance
College of Computing and Engineering
Nova Southeastern University
tp809@mynsu.nova.edu

Appendix D

Example of SME Participant Demographics Survey

SME Demographics Survey

Please answer the following demographic questions that best fits your situation.

*** Required**

1. SME-DO1: What is your gender? *

Mark only one oval.

- Male
 Female
 Other

2. SME-DO2: What is your age? *

Mark only one oval.

- 18-19
 20-29
 30-39
 40-49
 50-59
 Over 60

3. SME-D03: What is your highest level of education completed? *

Mark only one oval.

- High School Diploma
- 2-year college (Associates degree)
- 4-year college (Bachelors degree)
- Graduate degree
- Doctorate/Professional
- Other: _____

4. SME-D04: Which of the following best describes your professional role? *

Mark only one oval.

- Network Security or Cybersecurity Engineer
- Cybersecurity, Information Security, or Information Technology Security Analyst
- Information Security Manager
- Information Technology Auditor
- Cybersecurity Administrator
- Cybersecurity Consultant
- Cybersecurity Architect
- Other: _____

5. SME-D05: How many years of experience do you have in information security? *

Mark only one oval.

- 10 years or more
- At least 5 years, but less than 10 years
- At least three years, but less than 5 years
- At least one year, but less than 3 years
- Less than one year
- No Experience

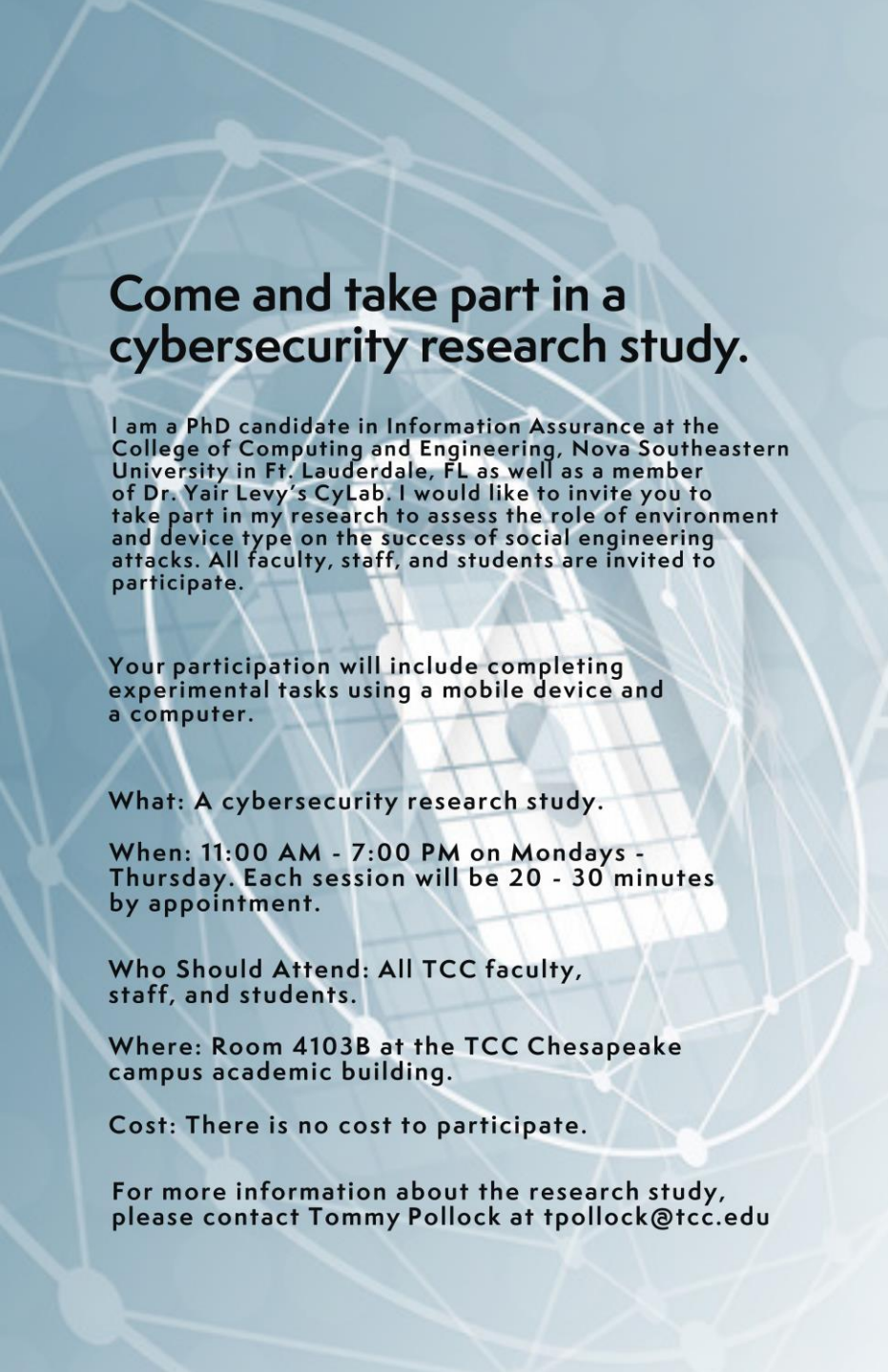
6. SME-D06: How many cybersecurity certifications do you have? *

Mark only one oval.

- None
- One
- Two
- Three
- Four or more

Appendix E

Example of Experiment Participant Research Study Recruitment Flyer



Come and take part in a cybersecurity research study.

I am a PhD candidate in Information Assurance at the College of Computing and Engineering, Nova Southeastern University in Ft. Lauderdale, FL as well as a member of Dr. Yair Levy's CyLab. I would like to invite you to take part in my research to assess the role of environment and device type on the success of social engineering attacks. All faculty, staff, and students are invited to participate.

Your participation will include completing experimental tasks using a mobile device and a computer.

What: A cybersecurity research study.

When: 11:00 AM - 7:00 PM on Mondays - Thursday. Each session will be 20 - 30 minutes by appointment.

Who Should Attend: All TCC faculty, staff, and students.

Where: Room 4103B at the TCC Chesapeake campus academic building.

Cost: There is no cost to participate.

For more information about the research study, please contact Tommy Pollock at tpollock@tcc.edu

Appendix F

Example of Experiment Participant General Informed Consent Form



**General Informed Consent Form
NSU Consent to be in a Research Study Entitled**

Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors

Who is doing this research study?

College: College of Computing and Engineering Nova Southeastern University

Principal Investigator: Tommy Pollock, MS, MBA

Faculty Advisor/Dissertation Chair: Yair Levy, Ph. D

Co-Investigator(s): Yair Levy, Ph. D

Site Information: Tidewater Community College
1428 Cedar RD
Chesapeake, VA 23322
Academic Building Room 4103B

Funding: Unfunded

What is this study about?

This is a research study, designed to test and create new ideas that other people can use. The purpose of this research study is to design, develop, and validate experimental settings to empirically test if there are significant mean differences in users judgment, when: exposed to two types of simulated social engineering attacks (phishing & possibly malicious search engine results (PMSE)), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile vs. computer). This research will test whether users are more likely to fall for phishing schemes in a distracting environment while using mobile phones or desktop/laptop computers. The experimental research questions will be presented as sample emails and sample search engine results asking the participants to determine if each sample is valid or phishing/possibly malicious.

Why are you asking me to be in this research study?

You are being asked to be in this research study because we need a sample of people from various demographic backgrounds such as age, gender, education, and level of social media

Page 1 of 5

usage to measure the mean differences in users judgment, when: exposed to two types of simulated social engineering attacks (phishing & possibly malicious search engine results (PMSE)), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile vs. computer).

This study will include about 60 people.

What will I be doing if I agree to be in this research study?

While you are taking part in this research study, Participants would be asked to take part in up to eight sessions of 20 to 30 minutes each. Each session will consist of using a mobile phone or a computer in various environments, answering questions provided during the research study.

You may have to come back to the Room 4103B every week for 8 weeks.

Research Study Procedures - as a participant, this is what you will be doing:

Using a mobile phone or a computer you will be asked to access the testing application for each of the eight different experimental procedures. The application will collect some demographic information from you, but no personal identifiable information (PII). You will be presented a series of questions to answer in a normal and a distracting environment on each device during the course of this experimental research study. We ask that you provide your own mobile device for this research study so that you are using a device that you are familiar with. If you do not have access to a mobile phone a secondary device may be provided to you.

Are there possible risks and discomforts to me?

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

What happens if I do not want to be in this research study?

You have the right to leave this research study at any time, or not be in it. If you do decide to leave or you decide not to be in the study anymore, you will not get any penalty or lose any services you have a right to get. If you choose to stop being in the study, any information collected about you before the date you leave the study will be kept in the research records for 36 months from the end of the study but you may request that it not be used.

Page 2 of 5

What if there is new information learned during the study that may affect my decision to remain in the study?

If significant new information relating to the study becomes available, which may relate to whether you want to remain in this study, this information will be given to you by the investigators. You may be asked to sign a new Informed Consent Form, if the information is given to you after you have joined the study.

Are there any benefits for taking part in this research study?

There are no direct benefits from being in this research study. We hope the information learned from this study will provide you a positive educational experience when dealing with phishing and social engineering.

Will I be paid or be given compensation for being in the study?

You will not be given any payments or compensation for being in this research study.

Will it cost me anything?

There are no costs to you for being in this research study.

Ask the researchers if you have any questions about what it will cost you to take part in this research study (for example bills, fees, or other costs related to the research).

How will you keep my information private?

Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law and will be limited to people who have a need to review this information. All responses will be collected on an online form and stored offline on a USB drive at the conclusion of the collection period. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies (if applicable). If we publish the results of the study in a scientific journal or book, we will not identify you. All confidential data will be kept securely. The USB drive will be stored in a locked filing cabinet. All data will be kept for 36 months from the end of the study and destroyed after that time by wiping the data on the drive.



Whom can I contact if I have questions, concerns, comments, or complaints?

If you have questions now, feel free to ask us. If you have more questions about the research, your research rights, or have a research-related injury, please contact:

Primary contact:
Tommy Pollock, MS, MBA can be reached at 757-793-5430

If primary is not available, contact:
Yair Levy, Ph. D can be reached at 954-262-2006

Research Participants Rights

For questions/concerns regarding your research rights, please contact:

Institutional Review Board
Nova Southeastern University
(954) 262-5369 / Toll Free: 1-866-499-0790
IRB@nova.edu

You may also visit the NSU IRB website at www.nova.edu/irb/information-for-research-participants for further information regarding your rights as a research participant.

All space below was intentionally left blank.

Page 4 of 5

Research Consent & Authorization Signature Section

Voluntary Participation - You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you leave this research study before it is completed, there will be no penalty to you, and you will not lose any benefits to which you are entitled.

If you agree to participate in this research study, sign this section. You will be given a signed copy of this form to keep. You do not waive any of your legal rights by signing this form.

SIGN THIS FORM ONLY IF THE STATEMENTS LISTED BELOW ARE TRUE:

- You have read the above information.
- Your questions have been answered to your satisfaction about the research.

<u>Adult Signature Section</u>		
I have voluntarily decided to take part in this research study.		
_____	_____	_____
Printed Name of Participant	Signature of Participant	Date
_____	_____	_____
Printed Name of Person Obtaining Consent and Authorization	Signature of Person Obtaining Consent & Authorization	Date

Page 5 of 5

Appendix G

Example of Experiment Participant Demographic Questions

Demographic Data

Please answer the following demographic questions that best fits your situation.

*** Required**

1. What is your age? *

Mark only one oval.

- 18-19
 20-29
 30-39
 40-49
 50-59
 Over 60

2. What is your gender? *

Mark only one oval.

- Male
 Female
 Other: _____

3. What is your highest level of education completed? *

Mark only one oval.

- High School Diploma
- 2-year college (Associates degree)
- 4-year college (Bachelors degree)
- Graduate degree
- Doctorate/Professional
- Other: _____

4. What is your level of social media usage? *

Mark only one oval.

- Never
- Occasionally
- Sometimes
- Often
- Always

Appendix H

Example of Experiment Participant Phishing Survey

Phishing IQ Test (email)

Please answer the following questions as as Legitimate, Phishing, or Ask IT Department for the sample emails provided.

* Required

1. PH-IQ-01. You receive the following email from the FBI about a banking transaction. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *

F.B.I <INFO@water.ocn.ne.jp> Apr 29 (2 days ago)

Why is this message in Spam? It's similar to messages that were detected by our spam filters. [Learn more](#)

OFFICIAL LETTER FROM FEDERAL BUREAU OF INVESTIGATION FBI
935 Pennsylvania Ave NW, Washington, DC 20535, USA
SPECIAL AGENT Andrew Castor

Dear, Beneficiary

The Federal Bureau of Investigation (FBI) Through our intelligence-monitoring network has discovered that the transaction that the Bank of America contacted you previously was Legal. Recently the fund has been legally approved to be paid to your Bank account.

So we the federal bureau of investigation (FBI) Washington Dc, in conjunction with the United Nations (UN) financial department have investigated through our Monitoring network noting that your transaction with Bank of America is legal. You have the legitimate right to complete your transaction to claim your fund.

You have to contact Bank of America or IMF and have your transaction completed.

CONTACT BANK OF AMERICA
Mr. JEFF ANDERSON
jeffanderson10036@gmail.com

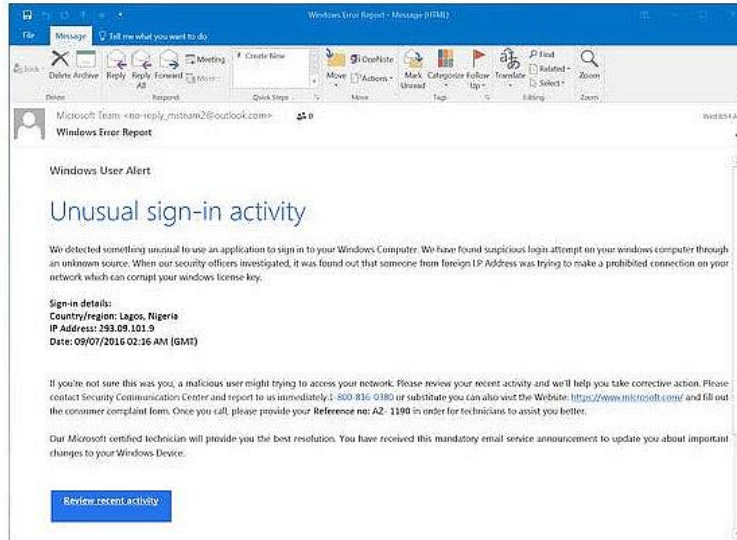
Await your response and have a great day

Yours faithfully,
SPECIAL AGENT Andrew Castor
Federal Bureau of Investigation
Washington DC, U.S.A

Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

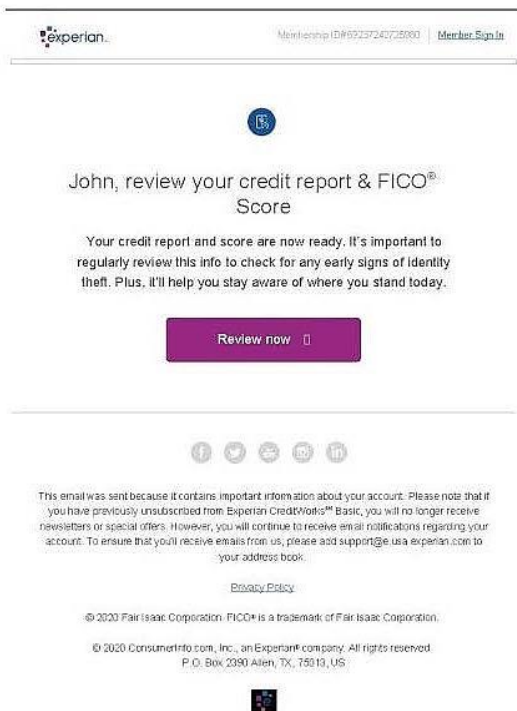
2. PH-IQ-02. You receive the following email alert from Microsoft about log in activity on your account. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



Mark only one oval.

- Legitmate
- Phishing
- Ask IT Department

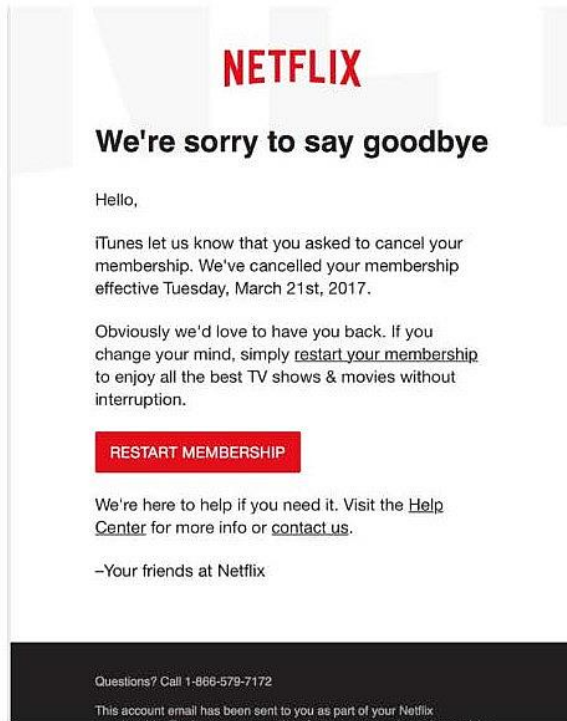
3. PH-IQ-03. You receive the following email alert from Experian about a change to your credit report. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

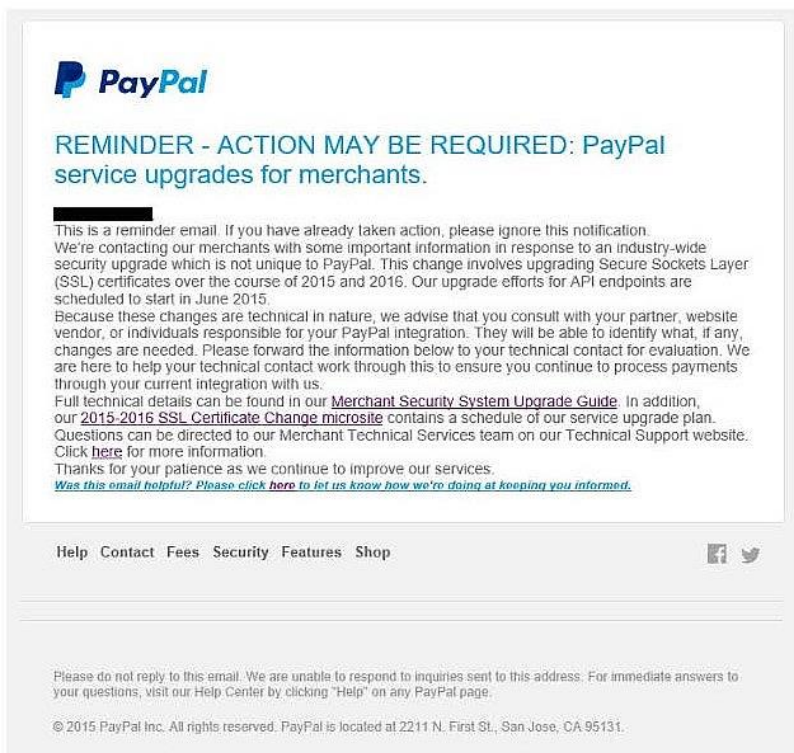
4. PH-IQ-04. You receive the following email alert from NETFLIX about your account cancellation. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

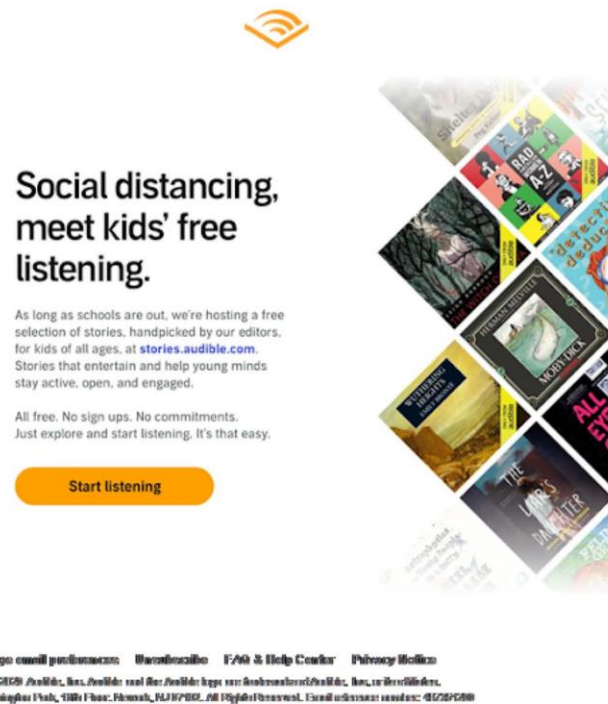
5. PH-IQ-05. You receive the following reminder email from PayPal about security upgrades to their system. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

6. PH-IQ-06. You receive the following email from Audible about a free audio book service for kids. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

7. PH-IQ-07. You receive the following email alert from Google showing a new sign in to your account. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



You received this mandatory email service announcement to update you about important changes to your Google product or account.

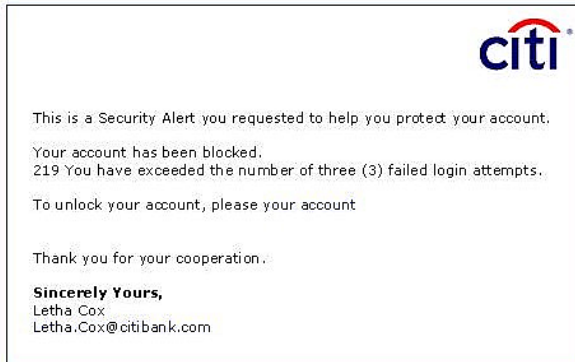
© 2015 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

8. PH-IQ-08. You receive the following email alert from CitiBank stating that your account was locked out due to three failed login attempts. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *

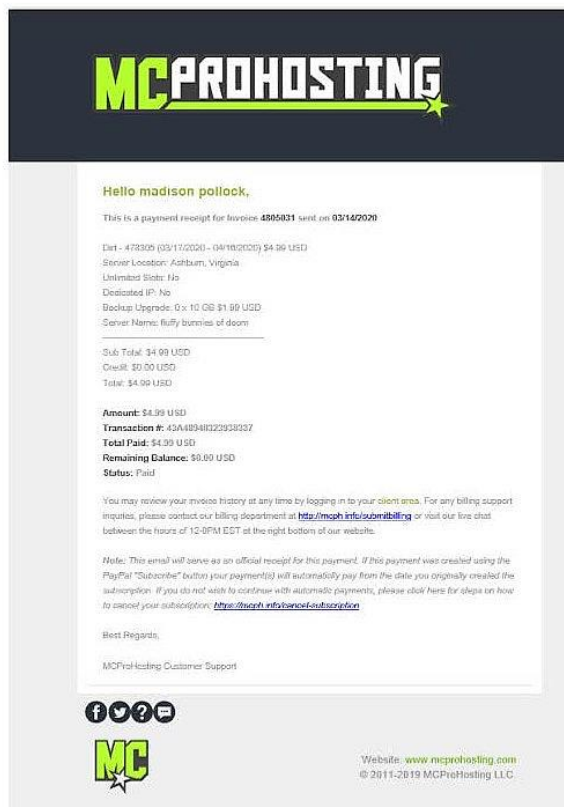
----- Forwarded Message: -----
From: "alerts@citibank.com" <ALERTS@CITIBANK.COM>
To: recipient@email.com
Subject: Security Alert: 06699
Date: Thu, 29 May 2008 12:41:41 +0000



Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

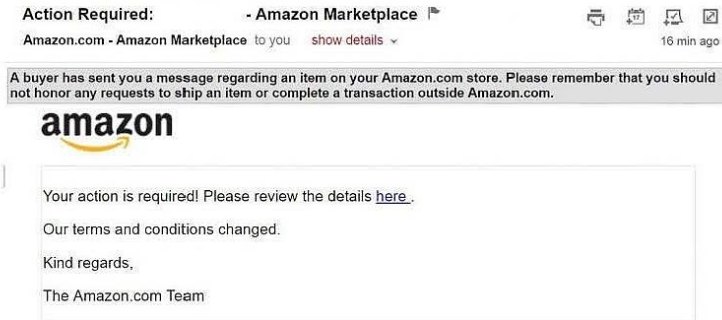
9. PH-IQ-09. You receive the following payment receipt from MCPROHOSTING for your server space rental. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

10. PH-IQ-10. You receive the following email alert from Amazon regarding an item that you are selling through their website. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

11. PH-IQ-11. You receive the following email advertisement asking you to view travel offers for the state of Wisconsin. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *



For every season, there's a reason to Discover Wisconsin! We have great reduced prices on travel packages and hotel rooms especially for you! We work to bring you some of the most compelling, adventurous and even peculiar destinations Wisconsin has to offer.

[See the limited-time offers now!](#)

Special Prices

2017 © Copyright Discover Mediaworks, Inc.

Mark only one oval.

- Legitimate
 Phishing
 Ask IT Department

12. PH-IQ-12. You receive the following email alert from Cisco WebEx asking you to update to a new version of WebEx. Is the image below of a legitimate email, a phishing email, or do you Ask IT Department? *

XYZ College Mail - Alert - WebEx update required

John Smith <JS12345@XYZ.edu>

Alert - WebEx update required

1 message

Cisco WebEx <WebEx@encrypt-mail.net>
To: XYZ College <John Smith <JS12345@XYZ.edu>

Sun, Oct 11, 2020 at 5:10 PM



Hello John,

Earlier this week, we detected a vulnerability in WebEx video conferencing and online meetings. We patched the vulnerability, but you must update your version to implement the fix.

Please update WebEx immediately.

Failure to update your version of WebEx may allow third parties to access your device, login credentials and files.

- WebEx Client Services

Mark only one oval.

- Legitimate
- Phishing
- Ask IT Department

Appendix I

Example of Experiment Participant PMSER Questions

PMSER IQ Test

Please answer the following questions as Legitimate, Potentially Malicious, or Ask IT Department for the sample search engine links provided.

* Required

1. PM-IQ-01. You searched for Motillum using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? *

[\[blurred\] - No RX Motillum LOWEST PRICES ON INTERNET ...](#)
 blog.s[blurred]
 No RX Motillum . 100mg Motillum. 750mg Motillum. Motillum usa. Motillum japan. Motillum canada. 20mg Motillum. Motillum us. Motillum uk. 50mg Motillum.

Mark only one oval.

- Legitimate
 Potentially Malicious
 Ask IT Department

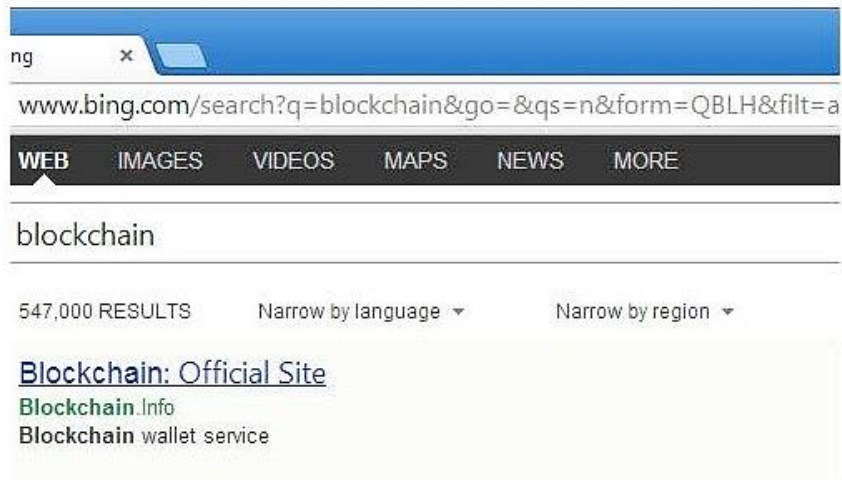
2. PM-IQ-02. You searched for tickets for the 2010 Miss Universe pageant using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? *

[Miss Universe 2010 Tickets - LeapFish Product Search](#)
 Compare Miss Universe 2010 Tickets prices, see current auction bids, find blogs and Miss Universe 2010 Tickets images with LeapFish Shopping Search.
www.leapfish.com/shopping.aspx?q=miss+universe+2010... - Cached

Mark only one oval.

- Legitimate
 Potentially Malicious
 Ask IT Department

3. PM-IQ-03. You searched for the term blockchain using a search engine browser with the following link being the top result returned. Is this a legitimate, possibly malicious link, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department
-

4. PM-IQ-04. You searched for hotels for an upcoming trip to Berlin Germany using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? *

Hotels: Booking.com™ - Über 832.000 Hotels weltweit
Anzeige www.booking.com/Hotels ▾
Buchten Sie jetzt Ihr Hotel!
Weltweit führende Online-Reisebüro - 2014 – World Travel Awards
Hotels in Hamburg - Hotels in Berlin - Hotels in München - Hotels in Amsterdam

Mark only one oval.

- Legitimate
 Potentially Malicious
 Ask IT Department

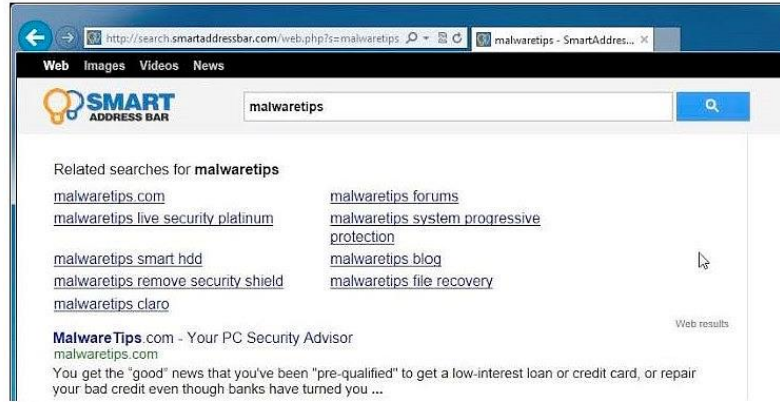
5. PM-IQ-05. You searched for killer whales at Seaworld using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? *

... - Seaworld [Killer Whale Video](#)
7 hours ago - Killer whale attacks and kills trainer at SeaWorld . Send us your photos, video or a quick note about something you've seen on the streets
www.seaworld.com/usg.php?sell=seaworld%20killer%20whale%20video

Mark only one oval.

- Legitimate
 Potentially Malicious
 Ask IT Department

6. PM-IQ-06. You searched for the malwaretips website using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department

7. PM-IQ-07. You searched for camping gear using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? *

Camping & Hiking Gear at REI: Tents, Backpacks, Stoves ...
www.rei.com/fit/camping-and-hiking - REI +
 But we don't just sell camping equipment—we help you put it to use. Check out our dozens of camping and hiking articles and videos online, camping-skills ...

Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department

8. **PM-IQ-08. You searched for the 2018 midterm elections using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? ***

Midterm elections 2018 polls

websitedukkani.com/enj0qnh/godev3a.php?snlhpyouf=midterm-elections-2018-polls ▾


16 hours ago - midterm elections 2018 polls adults who could cast their ballots stay home during every election. There were few surprises Tuesday night as Texas voters ...

Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department

9. **PM-IQ-09. You searched for COVID-19 using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? ***

www.cdc.gov > coronavirus > 2019-ncov ▾

Coronavirus Disease 2019 (COVID-19) | CDC 


Submit Double Arrow Right. FEDERAL RESOURCES. Coronavirus.gov · USA.
gov/Coronavirus. HAVE QUESTIONS? Visit CDC-INFO. Call 800-232-4636.

Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department

10. **PM-IQ-10. You searched for the Runescape download website using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? ***

The Free MMORPG - RuneScape - Online Fantasy RPG

 <https://www.runescape.com>

RuneScape now features more ways to play, brand new skills and over 200 gripping story-driven quests. Same Gielinor - Incredible graphics Play RuneScape on Windows, Mac or Linux and experience jaw-dropping visuals, lightning fast performance and an expansive viewing distance - or continue your adventure on the go with upcoming iOS and Android ...

Old School

Welcome to Old School RuneScape!
Relive the challenging levelling...

Community

Join the global RuneScape community today. Find in game events, the...

Account

Log in here to access your account for RuneScape and Old School...

Download

Download RuneScape to start playing a unique MMO set in the vast,...

Forums

For any RuneScape topic not covered by the other forums. 2,727,208...

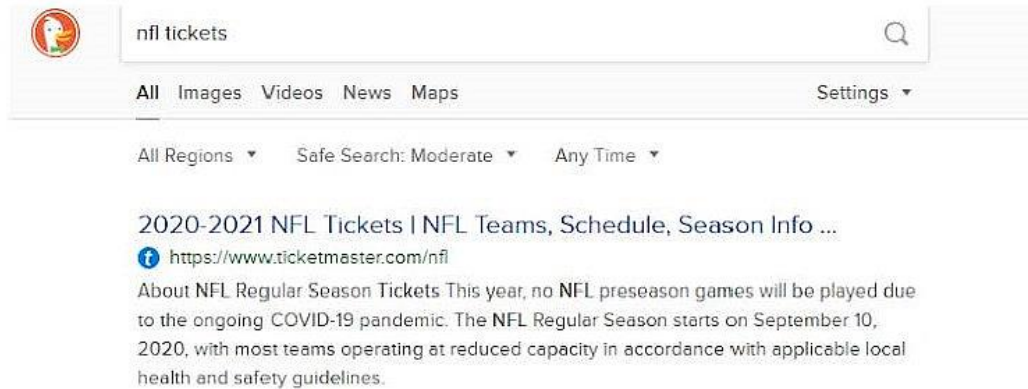
Play RuneScape

Download RuneScape to start playing a unique MMO set in the vast,...

Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department

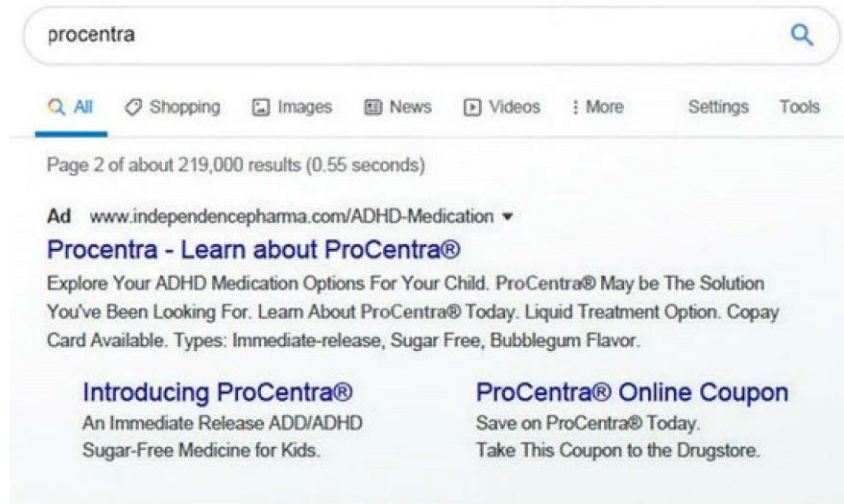
11. **PM-IQ-11. You searched for NFL tickets using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? ***



Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department
-

12. PM-IQ-12. You searched for information about the drug Procentra using a search engine browser with the following link being the top result returned. Is this a legitimate, possibility malicious link, or do you Ask IT Department? *



Mark only one oval.

- Legitimate
- Potentially Malicious
- Ask IT Department
-

Appendix J

Participant Research Recruiting Letter

Tommy Pollock: Research Project Jan 2022 tpollock@tcc.edu

1

RESEARCH PROJECT: FAQs

- Who:** Myself, the “Researcher”; You, the “Participant”
- What:** This is a Research Study using field experiments to test whether users are more likely to fall for phishing schemes in “**non-distracting**” versus “**distracting**” environments while using mobile phones or desktop/laptop computers.
- When:** Dec 2021-Jan 2022
- Where:** Online
- Why:** The main goal of this proposed research study is to design, develop, and validate experimental settings to empirically test if there are significant mean differences in users’ judgment when: exposed to two types of simulated social engineering attacks (phishing & Potentially Malicious Search Engine Results (PMSE)), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile vs. computer).

RESEARCH PROJECT: OVERVIEW

Dear Participant,

Thank you very much for volunteering to participate in my research project.

- This research consists of four short surveys in two parts using both your computer and mobile device:
 - **Part 1:** Non-Distracting Environment: Location of your choosing.
 - Survey 1: Computer, hyperlink
 - Survey 2: Mobile Phone, QR Code
 - **Part 2:** Distracting Environment: Location of your choosing in conjunction with playing the Sound File (Zoom link is provided).
 - Survey 3: Computer, hyperlink provided via Zoom
 - Survey 4: Mobile Phone, QR Code provided via Zoom
- You will be provided with a hyperlink to the surveys conducted on your computer and a QR code for your mobile device.
- Please do not use the same device to take all four parts of the survey as they will not record your answers properly. For example using the computer links using your mobile device.

Tommy Pollock: Research Project Jan 2022 tpollock@tcc.edu

2

- Once all four surveys have been completed, please email me at: tpollock@tcc.edu to confirm your results are recorded.

Thank you for your time and participation,

The Researcher, Tommy Pollock

RESEARCH PROJECT: INSTRUCTIONS

Part 1: Non-Distracting Environment

- **Survey 1- Computer:** Use [this link](#) to access the computer portion of the survey.
- **Survey 2- Mobile Phone:** Use the QR code below to access the survey with your mobile phone.



Part 2: Distracting Environment

The second part incorporates playing the Sound File simulating “distraction” while conducting the surveys on both your computer and then mobile phone.

- **Zoom Link** Use [this link](#) to access the Zoom meeting for the distracting environment portion of the research project.
- **Sound File** This will be played during the Zoom meeting to provide a controlled distracting environment for the experiment. Please use a set of headphones for the best sound quality.

Tommy Pollock: Research Project Jan 2022 tpollock@tcc.edu

3

- **Survey 3- Computer:** This link will be provided during the Zoom meeting and used in conjunction with the **Sound File** to access the computer portion of the survey
- **Survey 4- Mobile Phone:** The QR code will be provided during the Zoom meeting and used in conjunction with the **Sound File** to access the survey with your mobile phone.

**Once all four surveys have been completed, please email me at:
tpollock@tcc.edu to confirm your results are recorded.**

Again, thank you for your time and participation.

Very Respectfully,

Tommy Pollock

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
- Aste, M., Boninsegna, M., Freno, A., & Trentin, E. (2014). Techniques for dealing with incomplete data: A tutorial and survey. *Pattern Analysis and Applications*, 18(1), 1–29. <https://doi.org/10.1007/s10044-014-0411-9>
- 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](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](https://doi.org/10.1016/S0926-6410(00)00044-6)
- Botterill, D., & Platenkamp, V. (2014). Delphi method. In *Key Concepts in Tourism*

- Research* (Issue May 2019, pp. 57–60). SAGE Publications Ltd.
<https://doi.org/10.4135/9781473914674.n11>
- Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1–16.
<https://doi.org/10.2307/3250956>
- 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.
- Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. <https://doi.org/10.1016/j.jisa.2018.08.002>
- 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 emails can influence users and bypass security measures. *International Journal of Human Computer Studies*, 125(November 2018), 19–31. <https://doi.org/10.1016/j.ijhcs.2018.12.004>
- Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. *Proceedings of the 16th International Conference on World Wide Web*, 649–656. <https://doi.org/10.1145/1242572.1242660>
- 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>
- Flehmig, H. C., Steinborn, M., Langner, R., & Westhoff, K. (2007). Neuroticism and the mental noise hypothesis : Relationships to lapses of attention and slips of action in everyday life. *Psychology Science*, 49(4), 343–360. <http://www.doaj.org/doaj?func=abstract&id=266526>
- 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](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>
- Goode, J. (2018). Comparing training methodologies on employee's cybersecurity countermeasures awareness and skills in traditional vs. socio-technical programs. In *ProQuest Dissertations and Theses UMI Number: 10844844*.
- Gordon, T. J. (2009). The Delphi method. In J. C. Glenn & T. J. Gordon (Eds.), *Futures Research Methodology v3.0* (pp. 1–29).
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security*, 73. <https://doi.org/10.1016/j.cose.2017.11.015>
- Groff, B. D., Baron, R. S., & Moore, D. L. (1983). Distraction, attentional conflict, and driveline behavior. *Journal of Experimental Social Psychology*, 19(4), 359–380.

[https://doi.org/10.1016/0022-1031\(83\)90028-8](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>
- Hart, C. (2018). *Doing a literature review: Releasing the social science research imagination* (2nd ed.). Sage Publications Inc.
- 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](https://doi.org/10.1016/0010-0277(82)90023-3)
- Kahneman, D., & Tversky, A. (1983). Choices , Values , and Frames. *American Psychologist*, 39(4), 341–350. <https://doi.org/10.1037/0003-066X.39.4.341>
- 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 emails. *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>
- Kissel, R. (2013). Glossary of key information security terms. In *National Institute of Standards and Technology Interagency or Internal Report 7298r2*. <https://doi.org/10.6028/NIST.IR.7298r2>
- 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>
- Levy, Y. (2006). *Assessing the value of e-learning systems*. IGI Global.
<https://doi.org/10.4018/978-1-59140-726-3>
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, 9, 181–211.
<https://doi.org/10.1049/cp.2009.0961>
- 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
- Li, Y., Oladimeji, P., & Thimbleby, H. (2015). Exploring the effect of pre-operational priming intervention on number entry errors. *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, 1, 1335–1344.
<https://doi.org/10.1145/2702123.2702477>
- 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.
- Mavridis, D., & Moustaki, I. (2008). Detecting outliers in factor analysis using the forward search algorithm. *Multivariate Behavioral Research*, 43(3), 453–475.
<https://doi.org/10.1080/00273170802285909>
- 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>

- Mitnick, K., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. (J. Atkins (ed.)). Wiley Publishing, Inc.
- 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>
- Musuva, P. M. W., Getao, K. W., & Chepken, C. K. (2019). A new approach to modeling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, 94(August 2018), 154–175. <https://doi.org/10.1016/j.chb.2018.12.036>
- 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>
- Norman, D. A. (1981). *Steps toward a cognitive engineering: Design rules based on analyses of human error*. 378–382.
- 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 emails for older vs. young adults. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 6412–6424. <https://doi.org/10.1145/3025453.3025831>
- 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](https://doi.org/10.1016/0016-3287(94)90016-7)
- Onwuegbuzie, A. J., Bustamante, R. M., & Nelson, J. A. (2010). Mixed research as a tool for developing quantitative instruments. *Journal of Mixed Methods Research*, 4(1), 56–78. <https://doi.org/10.1177/1558689809355805>
- 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.
- Raymond, M. R., & Roberts, D. M. (1987). A comparison of methods for treating incomplete data in selection research. *Educational and Psychological Measurement*, 47(1), 13–26. <https://doi.org/10.1177/0013164487471002>
- Reason, J. (1995a). Safety in the operating theatre — Part 2: Human error and organisational failure. *Current Anaesthesia & Critical Care*, 6(2), 121–126. [https://doi.org/10.1016/S0953-7112\(05\)80010-9](https://doi.org/10.1016/S0953-7112(05)80010-9)
- Reason, J. (1995b). Understanding adverse events: human factors. *Quality and Safety in Health Care*, 4(2), 80–89. <https://doi.org/10.1136/qshc.4.2.80>
- Reason, J. T. (1984). Lapses of attention in everyday life. In R. Parasuraman & D. R. Davies (Eds.), *Varieties of attention* (pp. 515–549). Academic Press.
- Reason, J. T. (1990). *Human error* (First). Cambridge University Press.
- Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26–44. <https://doi.org/10.1016/j.cose.2016.01.004>
- 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](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](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. (1981). The framing of decisions and the psychology of choice. *Science*, 211(4481), 453–458. <https://doi.org/10.1126/science.7455683>
- 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](https://doi.org/Doi%2010.1007/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>
- Van Der Palm, D. W., Van Der Ark, L. A., & Vermunt, J. K. (2012). A comparison of incomplete-data methods for categorical data. *Statistical Methods in Medical Research*, 25(2), 754–774. <https://doi.org/10.1177/0962280212465502>
- 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>
- Vredeveltdt, A., & Perfect, T. J. (2014). Reduction of environmental distraction to facilitate cognitive performance. *Frontiers in Psychology*, 5(4), 1008–1013. <https://doi.org/10.3389/fpsyg.2014.00860>
- Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection.

Journal of the Association for Information Systems, 17(11), 759–783.

- Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, 28(2), 378–396. <https://doi.org/10.1287/isre.2016.0680>
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), xiii–xxiii. <https://doi.org/10.1.1.104.6570>
- Weissman, D. H., Roberts, K. C., Visscher, K. M., & Woldorff, M. G. (2006). The neural bases of momentary lapses in attention. *Nature Neuroscience*, 9(7), 971–978. <https://doi.org/10.1038/nn1727>
- Wilcox, R. R. (1998). How many discoveries have been lost by ignoring modern statistical methods? *American Psychologist*, 53(3), 300–314. <https://doi.org/10.1037/0003-066X.53.3.300>
- 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>
- Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674. <https://doi.org/10.1002/asi.20779>
- 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>
- Yuan, K. H., & Zhong, X. (2008). Outliers, leverage observations, and influential cases in factor analysis: Using robust procedures to minimize their effect. *Sociological*

Methodology, 38(1), 329–368. <https://doi.org/10.1111/j.1467-9531.2008.00198.x>

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>