

2021

## **Pause for a Cybersecurity Cause: Assessing the Influence of a Waiting Period on User Habituation in Mitigation of Phishing Attacks**

Amy Antonucci

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)



Part of the [Computer Engineering Commons](#), and the [Databases and Information Systems 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](mailto:nsuworks@nova.edu).

Pause for a Cybersecurity Cause: Assessing the Influence of a Waiting Period on  
User Habituation in Mitigation of Phishing Attacks

by

Amy E. Antonucci

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

College of Computing and Engineering  
Nova Southeastern University

2021

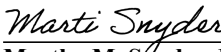
We hereby certify that this dissertation, submitted by Amy Antonucci conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

  
\_\_\_\_\_  
Yair Levy, Ph.D.  
Chairperson of Dissertation Committee

7/19/21  
Date


  
\_\_\_\_\_  
Laurie P. Dringus, Ph.D.  
Dissertation Committee Member

7/19/21  
Date

  
\_\_\_\_\_  
Martha M. Snyder, Ph.D.  
Dissertation Committee Member

7/19/21  
Date

Approved:

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

7/19/21  
Date

College of Computing and Engineering  
Nova Southeastern University

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

Pause for a Cybersecurity Cause: Assessing the Influence of a Waiting Period on  
User Habituation in Mitigation of Phishing Attacks

by  
Amy E. Antonucci  
June 2021

Social engineering costs organizations billions of dollars a year. Social engineering exploits the weakest link of information security systems, the people who are using them. Phishing is a form of social engineering in which the perpetrator depends on the victim's instinctual thinking towards an email designed to create a fear or excitement response. It is well-documented in literature that users continue to click on phishing emails costing them and their employers significant monetary resources and data loss. Training does not appear to mitigate the effects of phishing much; other solutions are necessary to mitigate phishing.

Kahneman introduced the concepts of System One and System Two thinking. System One is a quick, instinctual decision-making process. Examples of System One processes are orienting to a sudden sound or an experienced driver pressing the brake when faced with road danger. In contrast, Kahneman identified the process by which humans use a slow, logical process as System Two. System Two requires attention, is much slower, and is easily disrupted. Examples of System Two are looking for a person with a certain characteristic or checking the validity of a complex logical argument. The key aim of this study was to investigate if requiring the user to pause by presenting a countdown or count-up timer when a possible phishing email is opened will influence the user to enter System Two thinking.

This study designed, developed, and empirically tested a Pause and Think (PAT) mobile app that presented a user with a warning dialog and either a countdown or count-up timer whenever an email with a link was opened. The user was not able to interact with the email until the timer expired. The main goal of this research study was to determine whether requiring e-mail users to pause and wait for a colored warning with a timer when they are presented with a potentially malicious link has any effect on the percentage of falling to phishing attempts. The experimental field study was completed in three phases in which 42 subject matter experts and 107 participants took part. The results indicated that a countdown timer set at three seconds accompanied by red warning text was most effective ( $p < 0.001$ ) on the user's ability to avoid clicking on a malicious link or attachment. Recommendations for future research include enhancements to the PAT mobile app and investigating what effect the time of day has on susceptibility to phishing.

## Acknowledgements

My first thank you goes to my family, and especially to my mom, Pamela Lyons-Neville. She has been my main source of inspiration for my entire life. In addition to my living family, I want to acknowledge my ancestral lines on both sides of my family. I am grateful to come from strong families, both biologically and through my parents' second marriages. I am also grateful for the inspiration from my aunt and uncle, Toni Antonucci and James Jackson, who have walked this doctoral path before me, and for the support of my sister, Dulcey Antonucci, who has walked a similar yet different path than mine. I am also grateful to my dad and stepmom, Santino and Jeannie Antonucci, and to the legacy and memory of my stepdad, John Neville.

I want to thank my Nova classmates, especially Molly Cooper, Vasilka Chergarova, Mel Tomeo, Kim Smith, Tommy Pollock, John McConnell, Bob Jones, Damien Greatheart, Mark Denchy, Reid Cooper, Javier Coto, Tyler Pieron, and Jonathan Adkins.

I want to thank my WGU colleagues, especially Dana Cobbs, Lauren Provost, Jim Ashe, Carolyn Sher-DeCusatis, Mike Peterson, and to everyone who agreed to be participants!

I want to thank my friends who have been so supportive through this entire process, Charles and Diana Valentine. I'd like to thank Sarah Preston for her mentorship (and for use of her Android tablet!), and Maria Weaver for taking Elske for walks. And I want to thank Michele Davis for her support from afar. And I'd like to thank my second family, the Haugens, and especially my brother Jim.

And I want to thank Drs. Dringus and Snyder for their amazing support through this process. I love receiving support from such amazing women in IT, and I look forward to paying it forward. Together we'll advance women in technology!

And a special thank you to Dr. Yair Levy for your guidance and kindness through this entire process. I appreciated your pauses to make sure I understood what I needed to do and for your encouragement when you knew that the task before me seemed daunting. I will keep your mentorship in mind as I mentor my own students!

## Table of Contents

<b>Abstract</b>	ii
<b>List of Tables</b>	viii
<b>List of Figures</b>	x

### Chapters

<b>1. Introduction</b>	<b>1</b>
Background	1
Problem Statement	3
Dissertation Goal	5
Research Questions	7
Relevance and Significance	9
Barriers and Issues	10
Assumptions, Limitations, and Delimitations	11
Assumptions	11
Limitations	11
Delimitations	12
Summary	12
Definition of Terms	14
<b>2. Review of Literature</b>	<b>17</b>
Social Engineering	17
Phishing	28
Heuristics	40
Kahneman's System One and System Two and Decision Making	40
Habituation	46
Security in Mobile Devices	54
Phishing Mitigation Techniques	63
Polymorphic Dialogs	63
Training	66
Timers	74
Healthcare	74
Civil Engineering	76
Psychology	78
Text Color	80
Summary of What is Known and Unknown in Literature	82
<b>3. Methodology</b>	<b>85</b>
Overview of Research Design	85
Phase I	87
Phase II	91
Phase III	91
Instrument and Prototype Development	94
Instrument for Collecting SME Feedback Regarding Timer Value	94

Instrument for Collecting SME Feedback Regarding Sample E-mails	94
Instrument for Collecting Pilot Participant Feedback Regarding PAT	95
Instrument for Collecting Participant Demographic Information	95
PAT Prototype Development	95
Effectiveness of PAT Prototype	97
Reliability and Validity	99
Reliability	99
Validity	99
Sample	100
Pre-Analysis Data Screening	101
Data Analysis	102
Resources	103
Summary	103
<b>4. Results</b>	<b>106</b>
Overview	106
Phase I – SME Survey Feedback and Findings	106
Phase I – RQ1	109
Phase I – RQ2	111
Phase II – PAT Mobile App Development	117
Phase III – PAT Mobile App Delivery	120
Phase III – Pilot Testing	120
Phase III – Pre-Analysis Data Screening	120
Phase III – Participant Demographic Characteristics	121
Phase III – RQ3	123
Phase III – RQ4	125
Phase III – RQ5a	127
Phase III – RQ5b	133
Phase III – RQ5 – Age Group	138
Phase III – RQ5 – Gender Group	138
Phase III – RQ5 – Education Level Group	140
Phase III – RQ5 – Volume of Email Group	140
Phase III – RQ5 – Attention Span Score Group	143
Summary	143
<b>5. Conclusions, Implications, Recommendations, and Summary</b>	<b>147</b>
Conclusions	147
Discussion	148
Implications for Practice	148
Implications for Research	149
Limitations	149
Recommendations and Future Research	150
Summary	151

## **Appendices**

- A.** Example of SME Demographic Survey 155
- B.** Example of SME Sample Email Question 156
- C.** Example of SME Invitation Email 158
- D.** Example of Participant Recruitment Message for Facebook and LinkedIn 159
- E.** Example of Participant Invitation Email 160
- F.** Example of Participant Demographic Survey 161
- G.** Example of Participant Attention Span Test 162
- H.** Example of Phishing Email 166
- I.** Example of Phishing Email with Warning Dialog 167
- J.** Example of Phishing Email with Warning Dialog with Timer 168
- K.** Data Collection Detail 169
- L.** Institutional Review Board Exemption Letter 173

## **References 174**



## List of Tables

### Tables

1. Summary of Social Engineering Literature 26
2. Summary of Social Engineering: Phishing Literature 37
3. Summary of Kahneman's System One and System Two and Decision-Making Literature 44
4. Summary of Heuristics: Habituation Literature 52
5. Summary of Phishing Mitigation in Mobile Devices Literature 61
6. Summary of Phishing Mitigation: Polymorphic Dialogs Literature 65
7. Summary of Phishing Mitigation: Phishing Training Literature 72
8. Summary of Timers: Healthcare Literature 75
9. Summary of Timers: Civil Engineering Literature 77
10. Summary of Timers: Psychology Literature 79
11. Summary of Text Color Literature 82
12. Summary of Simulated Email Types 92
13. Summary of Research Phases 103
14. Summary of SME Demographics 107
15. Summary of SME Timer Value Selections 110
16. Summary of Verification of Sample Emails Data 111
17. Summary of Mobile App Experimental Procedure Validation 115
18. Descriptive Statistics of Study Participants 121
19. Attention Span Grouping Summary 123

20. ANOVA Results of Difference in Text Color and Timer Value in Email	
Interactions	124
21. ANOVA Results of Difference in Timer Type and Timer Value in Email	
Interactions	126
22. ANCOVA Results of Difference in Text Color and Timer Value in Email	
Interactions	128
23. ANCOVA Results of Difference in Timer Type and Timer Value in Email	
Interactions	134
24. Summary of Age Demographic with Respect to Click Mean	139
25. Summary of Gender Demographic with Respect to Click Mean	140
26. Summary of Education Level Demographic with Respect to Click Mean	141
27. Summary of Volume of Email Demographic with Respect to Click Mean	142
28. Summary of Attention Span Demographic with Respect to Click Mean	143
29. Summary of Research Question Results	146

## List of Figures

### Figures

1. Overview of Research Design Process 86
2. Example of PAT Timer Dialog 89
3. Example of SME Demographic Questions 90
4. Example of SME Timer Ranking Question 90
5. Overview of the PAT Process 98
6. PAT Login Screen 118
7. PAT Simulated Inbox 119
8. PAT Simulated Email with Timer 119
9. PAT Action After Link Tapped 119
10. Profile Plot of Text Color x Timer Value 125
11. Profile Plot of Timer Type x Timer Value 127
12. Profile Plot of Text Color x Timer Value with Age as a Covariate 131
13. Profile Plot of Text Color x Timer Value with Gender as a Covariate 131
14. Profile Plot of Text Color x Timer Value with Education Level as a Covariate 132
15. Profile Plot of Text Color x Timer Value with Email Volume as a Covariate 132
16. Profile Plot of Text Color x Timer Value with Attention Span as a Covariate 133
17. Profile Plot of Timer Type x Timer Value with Age as a Covariate 136
18. Profile Plot of Timer Type x Timer Value with Gender as a Covariate 136
19. Profile Plot of Timer Type x Timer Value with Education Level as a Covariate 137
20. Profile Plot of Timer Type x Timer Value with Email Volume as a Covariate 137
21. Profile Plot of Timer Type x Timer Value with Attention Span as a Covariate 138

- 22. Summary of Age Demographic with Respect to Click Mean 139
- 23. Summary of Gender Demographic with Respect to Click Mean 140
- 24. Summary of Education Level Demographic with Respect to Click Mean 141
- 25. Summary of Volume of Email Demographic with Respect to Click Mean 142
- 26. Summary of Attention Span Demographic with Respect to Click Mean 143

## Chapter 1

### Introduction

#### **Background**

Social engineering is a technique in which the attacker attempts to build a relationship with the victim to convince the victim to give the attacker information or to perform other actions that lead to malicious impact or financial losses (Krombholz et al., 2015).

Krombholz et al. (2015) categorized social engineering attacks into subgroups: physical, technical, and social. A physical attack is one in which the attacker uses some physical means to attack such as dumpster diving, impersonation, or having a door to a secure room held open for them. A technical attack is one in which the attacker uses purely digital means to gather information such as through software or a search engine. A social attack is one in which the attacker pretends to have some authority to convince the victim to release information. Some attacks combine two or more categories. For instance, Business Email Compromise (BEC) combines the social and technical attack categories (Zweighaft, 2017). BEC is an attack in which an e-mail that appears to be from a company employee in authority such as a Chief Executive Officer (CEO) is sent to a lower-level employee in a finance department requesting a financial withdrawal or transfer (Mansfield-Devine, 2018; Zweighaft, 2017). When the financial transaction is completed, the funds transfer to the attacker. Phishing is another example of an attack that combines the social and technical attack categories and was the focus of this study (Salahdine & Kaabouch, 2019). Phishing is an e-mail- or instant-messaging-based attack

aimed at a large group in which the attacker attempts to convince the intended victim to take some action such as click on a link. Attackers use phishing to create a fear response in their victims (Goel et al., 2017) which leads victims to use heuristics which may lead to systematic errors (Kahneman, 2011).

Kahneman (2011) referred to the process by which humans use heuristics to make a quick decision as System One. System One is a quick, instinctual decision-making process. Examples of System One processes are orienting to a sudden sound or an experienced driver pressing the brake when faced with road danger. In contrast, Kahneman (2011) identified the process by which humans use a slow, logical process as System Two. System Two requires attention, is much slower, and is easily disrupted. Examples of System Two are looking for a person with a certain characteristic or checking the validity of a complex logical argument. Hall et al. (2018) discussed System One and System Two with respect to encouraging medical students to engage System Two when making a diagnosis. They stated that medical students using System One tend to make more errors. In addition, Itri and Patel (2018) found that while heuristics can be useful in the field of medical imaging, heuristics can lead to cognitive bias. Cognitive bias is described as “a systematic error in reasoning or judgement” (p. 1097), which can lead to serious errors.

Text color can also affect user judgement (Kahneman, 2011). Acquisti et al. (2017) discussed text color in website design decisions, stating that required messaging that the designer would rather the user not notice, such as an unsubscribe link, is made in bland colors, while messaging that the designer would like the user to focus on, such as choosing to make a profile public, is shown in bright colors. This is a form of digital

nudging, which is defined as “any aspect of the choice architecture that alters people’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives” (Acquisti et al., 2017, p. 44:11). Anderson et al. (2015) stated that text color in a warning message should stand out to the user so that the user’s attention is captured.

This experimental field study used the Pause And Think (PAT) mobile app that was designed and simulated a Gmail account inbox. When an e-mail was opened, a timer dialog blocked access to the e-mail until the timer expired. The need for this work is demonstrated by the works of Anderson et al. (2016), who used functional Magnetic Resonance Imaging (fMRI) to demonstrate that users quickly habituate to static warnings, and by Amran et al. (2018) who stated that users will often consider security warnings irrelevant or even try to evade them. This dissertation built on previous research by Ball et al. (2015) and by Kahneman (2011). Ball et al. (2015) suggested that additional studies are required to understand what factors lead to habit as well as the relationship between habit and practice. They found that awareness of risks was not a significant influence over practice, and rather that habit was a stronger influence. It may be that requiring the user to pause will create a habit for pausing before opening an email even when the user is not required to do so.

### **Problem Statement**

The global research problem that this study addressed was that social engineering costs organizations billions of dollars a year (FBI, 2018; Musuva et al., 2019; Salahdine & Kaabouch, 2019; Thomas, 2018). Since social engineering is such a significant financial problem, investigating ways to mitigate it is of interest. This study focused on

the problem of why users make judgement errors when evaluating the risks involved in clicking on an unknown link in an e-mail.

Even when warned, users choose to put aside security concerns when deciding whether to follow links presented in an e-mail (Vance et al., 2018). A possible explanation for this is that users do not properly evaluate the risk involved in clicking on an unknown link, especially when overworked (Bravo-Lillo et al., 2011). Hirshleifer et al. (2019) found that financial analysts produce better forecasts when they are not mentally fatigued and use heuristics as they get more fatigued. Users also move to a heuristic process as they become more fatigued (Arazy et al., 2017), and it appears that this is also the case when they are deciding whether a displayed link is safe to follow. Tversky and Kahneman (1974) stated that heuristics are assumptions made to simplify decisions and that users can be taught to recognize when they are using heuristics to make a decision. By requiring the user to pause in this study, the user's thought stream may have been interrupted, and the user may have been switched to System Two thinking. Risbey and Lewandowsky (2017) defined a pause as a hiatus. Jensen et al. (2017) suggested that requiring the user to pause will encourage the user to reflect on the content of an e-mail message.

As with the medical students investigated by Hall et al. (2018), users are likely to engage in System Two thinking the first time they see a warning (Anderson et al., 2016), which is a message displayed to the user encouraging the user to consider the safety of taking an action such as clicking on a link (Amran et al., 2018), but tasks that are repeated appear to be processed using System One. This pattern of action often results in an error in judgement regarding the safety of a displayed link (Anderson et al., 2016).



Repetitive tasks are recognized by the brain and the effort extended to accomplish these tasks is diminished. Because of the diminished effort put forth by the brain, static, or passive, warnings lose effectiveness over time (Anderson et al., 2016) and System One takes over (Kahneman, 2011).

In addition to the fact that repetitive messaging appears to disengage users, the color of a message also appears to help or hinder user attention (Kahneman, 2011). Wogalter et al. (2002) stated that red has been found to increase the hazard rating of a warning, and that colored labels, especially red, are more noticeable than grey. Anderson et al. (2015) found no difference in user attention when a warning was presented in red rather than grayscale. They acknowledged that their finding was contrary to prior research and encouraged further research on the topic of warning text color. Using text color to digitally nudge the user may increase the likelihood of capturing the user's attention.

In summary, this research addressed the problem that users use heuristics to judge whether to click on a link in an e-mail, and that heuristics may lead to misjudgment. Thus, it appeared that, by requiring the user to pause, the user may have been led out of a heuristic thought process into a logical thought process. In addition, text color may have also moved the user into a more logical thought process.

### **Dissertation Goal**

The main goal of this research study was to determine through experimental field study whether requiring e-mail users to pause by displaying a colored warning (grey, red, or black text) with a timer (countdown, count-up, or no counter) when they are presented with a potentially malicious link has any effect on the percentage of users falling to

phishing attempts. Previous work by Musuva et al. (2019) used an experimental field study to investigate user behavior when faced with a potential phish.

The five specific goals of this research study were as follows. This study included three separate lengths of time (timer values) for which the users were required to pause. Each length of time was used separately to determine the pause duration that produced the highest statistically significant result of identifying malicious links in e-mail. Therefore, the first specific goal was to identify and validate, using cybersecurity Subject Matter Experts (SMEs), the three lengths of time to require the users to pause that should be used to assess their ability to identify malicious links in e-mail. A custom-designed mobile app, PAT, was designed and developed. PAT needed to be tested for functional correctness and validity. Therefore, the second specific goal was to assess the functional correctness and validity of PAT, along with validating the sample e-mails that included simulated potentially malicious links, using cybersecurity SMEs.

There are contradictory studies regarding the most effective text color for a warning message (Anderson et al., 2015). Since Anderson et al. (2015) reported that prior research stated that color should stimulate brain activity, yet found no difference in brain activity using red text, this study used grey, red, and black (Control) text. Therefore, the third specific goal was to determine whether there are statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black text.

Countdown timers have been found to be effective in different research fields, including medicine (Marto et al., 2016) and in pedestrian crosswalks (Keegan &

O'Mahony, 2003). Count-up timers have been used to measure vigilance (Lo et al., 2019). It may be that a countdown or count-up timer will move a user from a heuristic, System One thought process to a logical, System Two thought process. Moreover, to ensure the validity of the experiments, no timer was given to the control group. Therefore, the fourth specific goal was to determine whether there are statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer (control).

Age, gender, and education level have all been found to be statistically significant with regard to user cybersecurity behavior (Ball et al., 2015; Carlton, 2016). Attention span (Conteh & Royer, 2016) and the volume of information presented to the user (Marriott, 2018) has also been found to be statistically significant with regard to cybersecurity behavior. Therefore, the fifth specific goal was to determine whether there are statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values based on the categories of: (a) age, (b) gender, (c) education level, (d) attention span, and (e) the volume of email that the user receives in a day.

### **Research Questions**

The main research question that this study addressed was: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at

three separate timer values presented with a countdown or count-up timer with a red or grey warning message?

The five specific research questions that this study addressed were:

- RQ1: What are the three timer values to require the user to pause that should be used in this experimental field study to assess users' ability to identify malicious links in e-mail according to cybersecurity SMEs?
- RQ2: What level of functional correctness and validity of the custom-designed mobile app is sufficient according to cybersecurity SMEs?
- RQ3: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black warning text?
- RQ4: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer?
- RQ5a: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black warning

text based on the categories of: (a) age, (b) gender, (c) education level, (d) attention span, and (e) the volume of email that the user receives in a day?

RQ5b: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer based on the categories of: (a) age, (b) gender, (c) education level, (d) attention span, and (e) the volume of email that the user receives in a day?

### **Relevance and Significance**

This study is relevant and significant because it advances understanding of e-mail user behavior on a mobile device when that e-mail user is faced with a potentially malicious link. Understanding e-mail user behavior in this scenario is significant because billions of dollars a year are lost to phishing attacks (FBI, 2018; Musuva et al., 2019; Salahdine & Kaabouch, 2019; Thomas, 2018). In addition, corporate reputations are harmed, corporate secrets are stolen, and classified information is exposed (Jensen et al., 2017).

While there have been attempts to counter phishing, none have been entirely successful. Training programs for e-mail users that are designed to mitigate phishing attacks have been found to be largely unsuccessful (Burns et al., 2019; Goel et al., 2017; Gordon, Wright, Glynn, et al., 2019). Static warning messages have been found to be ineffective in the long run, and in some cases, even have an adverse effect on e-mail user reaction to phishing attempts (Junger et al., 2017). Brustoloni and Villamarín-Salomón

(2007) studied the effect of polymorphic warnings on the acceptance of unjustified risk by e-mail users when presented with a potentially malicious link. Unjustified e-mail risk is defined as an e-mail which the user is not expecting or in which the user does not know the sender. Brustoloni and Villamarín-Salomón (2007) found that, while polymorphic warnings resulted in a lower click rate of unjustified risks than static warning messages, the frequency of unjustified risks was still 80%.

This study offered promise to address this problem because the polymorphic techniques proposed are designed to engage the slow, logical thought process of the e-mail user on a mobile device, referenced by Kahneman (2011) as System Two. Engaging the e-mail user in System Two was promising because errors in judgement have been found to occur when people use heuristics, referenced by Kahneman (2011) as System One (Gerlach et al., 2019; Tversky & Kahneman, 1974). Using a countdown or count-up timer as part of the warning message was promising because it has been shown that people often assess timed events as important (Acquisti et al., 2017; Cheong, 2018; Keegan & O'Mahony, 2003; Marto et al., 2016; Newquist et al., 2012).

### **Barriers and Issues**

Since live emails were not used, it is possible that the e-mails would not be valid. To mitigate this possibility, simulated phishing e-mails that have been validated by an outside expert source were used. The outside expert source was also validated.

Finn and Jakobsson (2007) categorize phishing studies into three groups: survey, closed-lab experiments, and simulation. This study fell under the category of a closed-lab experiment which allowed evaluation of participant reaction to phishing but had the drawback of participant knowledge of the experiment. Participant knowledge of the

experiment may have made participants hypervigilant towards detecting a phish and, therefore, may have skewed the results. This study attempted to mitigate skewing of the results by not informing participants that the focus of the study was phishing. It was planned that participants be informed that the focus of study was email usage.

Since this study used colored warning text, color-blindness in the participants could have been a barrier. A question was added to the survey that participants took when they opened PAT for the first time. The question asked if they are color-blind, and, if so, whether they are red-green color-blind, blue-yellow color-blind, or completely color-blind (National Eye Institute, 2019). If a participant indicated that they are totally color blind, their results were excluded from the study.

### **Assumptions, Limitations, and Delimitations**

#### *Assumptions*

It was assumed that participants and SMEs were truthful when answering the surveys within the study. It was assumed that enough participants and SMEs would be found to achieve an acceptable sample size conducive to the statistical analysis that was performed. It was assumed that the consent form, directions, and sample e-mails were understandable by the participants. It was assumed that all participants had access to an Apple or Android mobile device capable of running PAT.

#### *Limitations*

A limitation of this study was that recruitment was managed in limited use of social media platforms which made it difficult to recruit a sufficient number of participants. Invitations were posted on Facebook and LinkedIn with a note to encourage sharing. Another limitation was that participants self-reported their color-blindness. Two other

limitations were that participants were chosen by convenience sampling and that the population used in this study was limited to English-speaking adults who use either an Android or Apple mobile phone.

### *Delimitations*

A delimitation of this study was that only Gmail was simulated. Another delimitation was that all participants and SMEs were fluent in English. A delimitation of this study was that participants owned an Android or Apple mobile device capable of running PAT.

### **Summary**

Social engineering, which includes phishing, is still an open problem that costs organizations billions of dollars a year (FBI, 2018; Musuva et al., 2019; Salahdine & Kaabouch, 2019; Thomas, 2018). In addition, phishing continues to present a significant threat to users in both their personal and professional lives leading to personal or corporate data loss (Carlton et al., 2018). Kahneman (2011) identified two processes. The first process, in which humans use a quick, instinctual thought process, he called System One. The second process, in which humans use a slow, logical thought process, he called System Two. Kahneman (2011) also stated that text color may affect judgement.

The research problem that this study addressed is that social engineering costs organizations billions of dollars a year (FBI, 2018; Musuva et al., 2019; Salahdine & Kaabouch, 2019; Thomas, 2018). This study focused on the addressable problem of why users make judgement errors when evaluating the risks involved in clicking on an unknown link in an e-mail. In this study, it may have been that moving the user to the slower, logical System Two thought process mitigated the user's susceptibility to a phishing attack.



This research proposed to mitigate phishing by moving the user from a System One, fast, heuristic mindset to a System Two, slow, logical mindset by presenting a countdown or count-up timer with colored warning text. This study used PAT, a custom mobile app, to simulate a Gmail client. Participants interacted with the app as they would when checking e-mail. The app embedded a survey that opened when the participant opened the app for the first time.

The main research question that this study addressed is: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values presented with a countdown or count-up timer with a red or grey warning message? The first specific research question addressed what the timer value should be that will be used in the countdown and count-up timers. The second specific research question addressed the validity and functionality of PAT. The third through fifth research questions addressed what effect the type of timer (countdown or count-up), the timer value, the color of warning text (grey, red, or black [control]), and demographic factors (age, gender, education level, attention span, and the volume of email that the user receives in a day) has on a user's ability to avoid clicking on a malicious link.

This study was relevant and significant because it advanced understanding of e-mail user behavior on a mobile device when that e-mail user is faced with a potentially malicious link. No attempts to counter phishing have been entirely successful. User training has had mixed success and static warnings have been found to be ineffective.

Polymorphic warnings show promise; the reason may be that polymorphic warnings move the user into a logical, System Two thought process.

Potential issues were that live e-mail was not used, so that participants may have been hypervigilant when checking the simulated e-mail, and that participants may have been color-blind. To mitigate the potential barrier of simulated e-mails rather than live e-mails, the simulated emails were adopted from an outside repository of simulated phishing emails. Participant hypervigilance was designed to be mitigated by informing participants that the focus of this study is e-mail usage. The demographic survey that appeared the first time PAT was opened included a question on color-blindness, and the answers to that question were addressed when the data were analyzed.

It was assumed that participants had access to an Apple or Android mobile device capable of running PAT. A limitation of this study was that unseen errors in data collection may have affected the results. Every effort was taken to ensure that the data were valid. A delimitation of this study was that all SMEs and participants were fluent in English.

### **Definition of Terms**

**Attention span** – “The amount of concentrated time we can spend on any single task without getting distracted by other tasks” (Bulling, 2016, p. 94).

**Business Email Compromise** – An attack in which an e-mail that appears to be from a company employee in authority is sent to a lower-level employee in a finance department requesting a financial withdrawal or transfer (Mansfield-Devine, 2018; Zweighaft, 2017).

**Cognitive bias** – “A systematic error in reasoning or judgement” (Itri & Patel, 2018, p. 1097)

**Cybersecurity** – “The prevention of damage to, unauthorized use of, exploitation of, and if needed, the restoration of electronic information and communications systems to ensure confidentiality, integrity, and availability” (Carlton, 2016, p. 14).

**Digital Nudging** – “Any aspect of the choice architecture that alters people’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives” (Acquisti et al., 2017, p. 44:11).

**Heuristic** – An assumption made to simplify a decision (Kahneman, 2011).

**Personally Identifiable Information (PII)** - Any information that can be used to identify the owner of that information (Carlton, 2016).

**Phish** – An email or instant-message sent to a potential victim in a phishing attack (Chaudhry et al., 2016).

**Phishing** – An e-mail- or instant-messaging-based attack aimed at a large group in which the attacker attempts to convince the intended victim to take some action such as click on a link (Chaudhry et al., 2016).

**Polymorphic Warning** – a warning that changes appearance with the aim of reducing user habituation (Anderson et al., 2016).

**Social Attack** – An attack in which the attacker pretends to have some authority to convince the victim to release information (Krombholz et al., 2015).

**System One** – A quick, instinctual decision-making thought process (Kahneman, 2011).

**System Two** – A slow, logical thought process (Kahneman, 2011).

**Social Engineering** – The technique in which the attacker attempts to build a relationship with the victim to convince the victim to give the attacker information or to perform other actions that lead to malicious impact or financial losses (Krombholz et al., 2015).

**Unjustified E-Mail Risk** – An e-mail which the user is not expecting or in which the user does not know the sender (Brustoloni & Villamarín-Salomón, 2007).

**Warning** – A message displayed to the user encouraging the user to consider the safety of taking an action such as clicking on a link (Amran et al., 2018).

## Chapter 2

### Review of the Literature

Topics related to this research are discussed in this review of literature. Specifically, social engineering is examined with a focus on phishing. Next, heuristics, with a focus on Kahneman's System One and System Two, decision-making, and habituation are reviewed. Literature related to mobile devices is reviewed next. Phishing mitigation techniques are next, including a review of polymorphic dialogs and training. Lastly, timers, especially in healthcare, civil engineering, psychology, and text color are discussed.

#### **Social Engineering**

Social engineering is one of the most under-researched and most effective cybercrimes (Jain et al., 2016). Social engineering is defined as “the art of exploiting the weakest link of information security systems: the people who are using them” (Jain et al., 2016, p. 94). Mihelič et al. (2019) called the human factor in social engineering a lever that is exploited by attackers. There are four stages of social engineering: (1) information gathering, (2) gain trust, or hook relationship, (3) exploit trust and execute attack, and (4) exit (Mitnick & Simon, 2003; Salahdine & Kaabouch, 2019). In the information gathering stage, the attacker performs a reconnaissance, which is an information gather about their target. In the hook relationship phase, the attacker baits the victim with fear or excitement (Goel et al., 2017). In the play exploitation and execution phase, the attacker executes the attack, and in the out phase, the attacker leaves with no or limited trace that

they were ever there. Krombholz et al. (2015) suggested four types of social engineering: physical, technical, social, and socio-technical. A physical attack is one in which the attacker does a physical action such as dumpster dive, in which an attacker will use to gather information about a potential future victim. A technical attack is one in which the attacker uses purely technical means to gather information, such as harvesting information online about future victims. A social attack is one in which the attacker uses supposed authority to convince the victim to do something (e.g., vishing or voice-phishing). An example of vishing is calling in to technical support and pretending to forget a password so that the victim will reset it. Most social attacks are done by phone (Krombholz et al., 2015). A socio-technical attack combines both social and technical attacks, using elements of both types to perform an attack. Phishing falls into this category. This study had a technical aspect, namely the countdown or count-up timer, and a social aspect, namely an attempt to move the user into a thought-provoking mindset.

Technical solutions to combat social engineering typically do not work (Krombholz et al., 2015), and Jain et al. (2016) said that there are no technical solutions to the problem of social engineering. Users are often too confident in their ability to detect a social engineering attack (Krombholz et al., 2015), partially because social engineers are becoming more devious. This means that suggestions for countering social engineering just two years ago are no longer useful. For example, in 2018, Abass advised to look for the Hyper Text Transfer Protocol Secure (HTTPS) protocol in a Universal Resource Locator (URL), but in 2020, the Anti-Phishing Working Group advised not to rely on presence of the HTTPS protocol since up to 75% of attackers now use websites using that protocol (Anti-Phishing Working Group, 2020). These data provided relevance to this

study because it shows that the field of social engineering mitigation is under constant change.

A number of studies have simulated social engineering in different settings, including a corporation (Bullée et al., 2015; Workman, 2008), five hospitals (Medlin et al., 2008), a military base (Biros et al., 2002; George et al., 2004), and a university (Mensch & Wilkie, 2011). Overall, the results from these studies showed that social engineering is still a significant issue. Just-in-time training (Biros et al., 2002; Workman, 2008) and creating an awareness of the dangers of social engineering (Bullée et al., 2015) can promote detection of social engineering. Bullée et al. (2015) created three interventions to warn against social engineering: a leaflet, a blue keychain that said, “Don’t give me to a stranger,” and a poster with a funny quote. A week after giving the interventions to three treatment groups, they deployed social engineering “attackers” with the goal of getting the keys from the participants. They reported that staff who were not given the intervention surrendered their keys at 2.84 times more often than those who were given one of the three interventions. Biros et al. (2002) asked Air Force personnel to complete tasks using a known database. The personnel were told that a disgruntled and discharged database manager manipulated data before he left. Treatments given were just-in-time training and training six weeks before the task. They found that personnel that received the just-in-time training were better able to detect false data than the personnel that received formal training six weeks prior. They also found, though, that the personnel that received just-in-time training were more likely to mark data that are valid as invalid. Biros et al. (2002) recommended just-in-time training warnings. George et al. (2004) also investigated the effect of deception training on Air Force personnel and found that

training improved understanding of deception but did not improve detection ability. They created three types of training, some of which included computer-based training. They found no difference in the interventions, and stated that, since computer-based training appeared to be just as effective as human-based training, human-based resources could be saved by using computer-based resources instead. Workman (2008) also created three types of trainings to investigate the effects of training on employees of a Fortune 500 company. The three trainings were punishment-based, ethics-based, and on social engineering. Six months after the training was given, they simulated a phishing campaign. They found that those with a greater fear response responded best to the punishment-based training, and that those with a higher level of commitment and trust responded best to the social engineering training. They reported that the ethics training had no effect.

Many studies found that users are susceptible to social engineering (Fleming, 2017; Medlin et al., 2008; Mensch & Wilkie, 2011; Wang et al., 2021). Medlin et al. (2008) simulated a social engineering attack by issuing a survey to employees of five different hospitals asking for user passwords. While the administrations of those hospitals gave permission for the surveys to be distributed, they did not endorse the survey to the employees which would have affected the validity of the study. Medlin et al. (2008) found that 73% of employees surveyed gave their personal passwords on the survey. Medlin et al. (2008) stated that the implication of their research was that systems could be easily cracked if employees are willing to release their passwords, which, in the hospital environment, could easily lead to a violation of the Health Insurance Portability and Accountability Act (HIPAA). They stated that it is imperative that employees receive



good and effective training against social engineering attacks. Fleming (2017) also stated that training is an important intervention to mitigate the effects of social engineering. He investigated unauthorized disclosures of Personally Identifiable Information (PII) and Non-public Personal Information (NPI) in the public-school system. Using an interview methodology, Fleming (2017) found that users often forgot that data needed to be protected, making them susceptible to a social engineering attack. As with Fleming (2017), Mensch and Wilkie (2011) also found that attitudes regarding social engineering were low. They studied the security behaviors of undergraduate and graduate university students and used the students' majors as a demographic variable. Mensch and Wilkie (2011) found that Information Technology (IT) and fine arts majors had the highest security attitude, and healthcare and criminology majors had the lowest security attitude. They expressed surprise that the criminology majors scored low given that these students were headed for careers in law enforcement and similar fields, and they expressed concern that healthcare majors scored low since the low score indicated a possible future violation of HIPAA.

Wang et al. (2021) created a framework to describe user vulnerabilities to social engineering and then tested the framework with 16 social engineering attack cases. They found more than thirty effect mechanism and more than forty human vulnerabilities to social engineering. These studies gave relevance to this study because they showed that social engineering is still a significant problem to be addressed.

Facebook seemed to be a popular platform for social engineering studies (Albladi & Weir, 2020; Algarni et al., 2017; Cheung et al., 2015; Dincelli & Chengalur-Smith, 2020; Ross et al., 2018; Terlizzi et al., 2017). All the studies that investigated Facebook as a

platform reported some risk of social engineering. In particular, the influence on different characteristics of Facebook components on social engineering have been investigated, including characteristics of a user (Albladi & Weir, 2020), characteristics of a profile being viewed (Algarni et al., 2017), what characteristics lead users to self-disclose on Facebook (Cheung et al., 2015; Dincelli & Chengalur-Smith, 2020), the influence of warnings on the user belief of fake news (Ross et al., 2018), and the influence of characteristics of a fake Facebook profile on having a user accept a friend request and on subsequently giving information to that profile (Terlizzi et al., 2017). Cheung et al. (2015) studied the effects of perceived cost, perceived benefit, and social influence on why Facebook users self-disclose personal information. They investigated these effects by collecting data through an online survey from participants at a large university in Hong Kong. Their results indicated that perceived benefit and social influence had the greatest effect on self-disclosure behavior on Facebook. They expressed surprise that perceived cost had no apparent effect on self-disclosure behavior and offered the explanation that the participants may not have understood the risks of self-disclosure.

Dincelli and Chengalur-Smith (2020) investigated Facebook user self-disclosing by creating Choose your Own Adventure (CYOA) type trainings. They created both textual and visual trainings, and tested participant awareness of the risk of self-disclosure by issuing a questionnaire one month after the training. They found that visual-based training was reported to be more satisfying and made learning easier. They used a learning design principle that allowed learner self-reflection and allowed the user to stop and think about what knowledge was gained. This study also required the user to pause, so this principle is relevant.

Albladi and Weir (2020) investigated the influence of Facebook user characteristics on susceptibility of becoming a victim of a social engineering attack. They used a questionnaire and a role-play scenario to collect data. They considered as independent variables user level of involvement in social media, number of social networking connections, the percentage of known friends in the social network, and social networking experience. Their goal was to predict user susceptibility to social engineering. They found that trust is the highest factor that predicts user susceptibility to social engineering. Other factors in order of influence on user susceptibility were user level of involvement in social media, cybercrime experience, social networking experience, and the percentage of known friends on Facebook. They found that fewer social connections predicted a higher susceptibility to social engineering which they had not expected.

Ross et al. (2018) set out to investigate the effects of two different kinds of warnings on fake news on Facebook. They used a scenario role-play and a questionnaire to collect data. They were surprised to learn that no warning was effective, leading to a rejection of all their hypotheses. In fact, they reported, that Facebook stopped providing warnings for fake news because the warnings had no effect. Although warnings seemed to have no effect, they suggested as future research to study different kinds of warning designs and to study the effect of different demographics on the reactions to the warnings.

Terlizzi et al. (2017) investigated the effect of a fake Facebook profile on user willingness to friend that profile and provide sensitive information to that profile. They found that, while bank employees had some caution, more training was needed on the dangers of social engineering. As future research, they recommended a similar investigation of other critical sectors such as healthcare and government.

Ayyagari and Tyks (2012) investigated a case study in which funds were stolen from a university meal plan. They found that the system administrator who was responsible for the meal plan system had no training on the system, and that the system itself had never been secured. Through further investigation, they found that a consultant firm that had been hired to upgrade the servers used social engineering to steal the credentials necessary to steal the funds. They concluded that the system needed better security, including against a social engineering attack, and that any time there is a new system administrator for the meal plan system, that that system administrator should be trained on the system.

A number of studies surveyed investigated social engineering with respect to robotics (Aroyo et al., 2018; Booth et al., 2017). Aroyo et al. (2018) stated that the goal of their study was to see how trust towards robots can be used for social engineering. They created a humanoid robot and created an Easter-egg hunt in which participants were asked individually to find the eggs in the presence of the robot. Before the hunt began, the robot participated in small talk with the participant. The goal of the small talk was to have the robot gain the trust of the participant. Part of the small talk was that the robot asked for personal information. When the participant was asked to begin the hunt, the robot offered hints to egg locations. Participants who found all the eggs in the hunt were offered a gamble: they could hunt for a bonus egg for double-or-nothing reward. The robot encouraged the gamble, and 100% of the participants who were offered the gamble took it. When asked afterwards why they listened to the robot, some of the participants stated that they trusted the robot because the robot had no reason to lie. The implication of this study is that people tend to trust entities that truly have no reason to be trusted.

Booth et al. (2017) also used a robot to test reaction to a social engineering attack. In their study, they created a small mobile robot that waited at the entrance to a secure dormitory entrance and asked passers-by to let it into the building. They found that groups of people were more likely to let the robot in than individuals. They also found that people were more willing to let the robot in if the robot claimed to be delivering food. One participant asked the robot if it had authorization to enter the building, but then let the robot in anyway when the robot did not answer the question. As with the Aroyo et al. study, Booth et al. (2017) stated that over trust in a robot can create a significant security threat.

Overall, these studies in social engineering illustrate the significant threat that social engineering presents. People seem to believe that they are safe from social engineering because they will recognize an attempt. But these studies show that even experts in IT security can fall for a social engineering attack. Also, people seem to trust entities that have no reason to be trusted such as an unknown Facebook profile or a robot. While training does seem to mitigate the effect of social engineering, many times a social engineering attack works because the victim is not alert to the attack. This fact gives relevance to this study, which attempted to move the user into an alert mode of thinking. The studies discussed in this section are summarized in Table 1.

**Table 1***Summary of Social Engineering Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Abass, 2018	Empirical	Commentary	Social Engineering Attacks	Presented suggestions for protection against social engineering
Albladi & Weir, 2020	Experimental	316 Participants	Questionnaire, Role-Play Scenario	Developed a conceptual model to test factors that influence vulnerability on social media
Algarni et al., 2017	Empirical, Grounded Theory & Survey	370 Employees from 3 Organizations	Role-Play & Questionnaire	Identified user characteristics as significant predictors of social engineering victimization
Aroyo et al., 2018	Experiment	61 Healthy Italians	Interactive Robot & Questionnaire	Robots could become a powerful tool for social engineers
Ayyagari & Tyks, 2012	Case Study	One Incident at a University in Idaho	Interviews	Illustrated IT security issues in an educational setting
Biros et al., 2002	Field Experiment	206 Military Personnel	Simulation	Warnings and JIT training can promote deception detection
Booth et al., 2018	Experimental	108 University Students	Scenario & Interview	Overtrust in robots can represent a significant threat
Bullée et al., 2015	Experimental	118 Employees	Simulation Role-Play	Creating awareness of dangers of social engineering helps to neutralize attack
Cheung et al., 2015	Experimental & Empirical	405 Facebook Users	Cross-Sectional Survey	Social influence is indicated to be strongest effect on self-disclosure.
Dincelli et al., 2020	Experimental & Design Science Research	1718 Employees	Gamified Artifact, Surveys & Vignettes	The gamified artifact reduced online-self disclosure

**Table 1***Summary of Social Engineering Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Fleming, 2017	Grounded Theory & Case Study	15 Public School Teachers or Administrators	Open-Ended Telephone Interviews	Training is needed to mitigate unauthorized release of NPI and PII
George et al., 2004	Field Experiment	125 Air Force Officers	Lecture and/or Computer-Based Training and Judgement and Knowledge Tests	Training improved understanding of deception but did not improve detection ability
Jain et al., 2016	Empirical	Commentary	Social Engineering Attacks	Emphasized human element as biggest threat to the security of a company
Krombholz et al., 2015	Empirical	Commentary	Social Engineering Attacks	Created taxonomy of social engineering attacks
Medlin et al., 2008	Experimental	118 Hospital Employees	Questionnaire	Employees are willing to share personal information
Mensch & Wilke, 2011	Exploratory	127 Graduate and Undergraduate Students	Cross-Sectional Survey	Security attitudes among college students tend to be low; Recommended training
Mitnick & Simon, 2003	Empirical	Commentary	Social Engineering Attacks	Introduced model for social engineers
Ross et al., 2018	Experimental	151 Participants	Scenario & Questionnaire	Warnings are ineffective in alerting user to false information

**Table 1***Summary of Social Engineering Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Salahdine & Kaabouch, 2019	Empirical	Commentary	Social Engineering Attacks	Categorized social engineering attacks
Terlizzi et al., 2017	Empirical	500 Brazilian Bank Employees & 100 Other Randomly-Selected Individuals	Simulation	Training is recommended to mitigate data leakage on social media
Workman, 2008	Experimental Field Study	612 Employees of a Fortune 500 Company	Questionnaire & Observation	Clarified which kind of intervention is most effective
Wang et al., 2021	Case Study	16 Social Engineering Attacks	Conceptual Model	The model provides a conceptual visualization of social engineering

*Phishing*

Finn and Jakobsson (2007) categorized phishing studies into three groups: survey, closed-lab experiment, and simulation. A survey study presents the participants with a survey asking what their reaction to an event would be (Sekaran & Bougie, 2016). Bravo-Lillo et al. (2011) used an interview survey to understand perception of risk of a chosen action. A closed-lab experiment is one in which participants are aware of the focus of the study, and, therefore, their results may be skewed. An example of a closed-lab experiment is Algarni et al.'s 2017 study. They used a role-play questionnaire in which participants were shown Facebook profiles and then asked about the trustworthiness of



those profiles (Algarni et al., 2017). Algarni et al. (2017) acknowledged that participant reaction may be skewed because the participants were aware of the study.

The third kind of study according to Finn and Jakobsson (2007) is a simulation study in which the research design mimics a real-world scenario and the participants are unaware of the study. Finn and Jakobsson (2007) discussed ethical considerations with regard to simulation studies. Simulation studies seem to be the most widely used of the three types of studies, as they have been used to understand phishing behavior (Burns et al., 2019; Goel et al., 2017; Gordon, Wright, Glynn, et al., 2019), Musuva et al. (2019) used an simulation study which had to be curtailed because a social media activist sent out an alert regarding the phishes in the investigation which led the university to end the study. To avoid ethical dilemmas, this study was a closed-lab field experiment.

While phishing is only one of 20 different kinds of social engineering defined by Salahdine and Kaabouch (2019), they stated that phishing is the most common type of social engineering attack. Thompson (2012) stated that many attacks start with a bad user decision and that anyone can be tricked by a phishing attack. Several studies presented a variety of taxonomies (Gupta et al., 2018; Rastenis et al., 2020; Salahdine & Kaabouch, 2019). Salahdine and Kaabouch (2019) organized phishing attacks into five categories: spear, whaling, vishing, interactive voice response, and BEC while Rastenis et al. (2020) gave a wider definition, which included the devices and other media used. Gupta et al. (2018) offered a taxonomy based on the phases of a phishing attack. A spear phishing attack is one in which the attacker targets a particular group of people, such as employees of a particular company or users of a particular website (Halevi et al., 2015). A whaling attack is a subset of a spear phishing attack in which the high-profile members of the

target group are targeted (Gupta et al., 2018). A vishing attack is a phone attack in which the attacker convinces the victim to give up some piece of confidential information (Salahdine & Kaabouch, 2019), and an interactive voice response attack is a subset of a vishing attack in which the attacker pretends to be an interactive voice-controlled computer (Salahdine & Kaabouch, 2019). A BEC attack is one in which the attacker pretends to be a high-ranking member of the victim's organization and asks for a secure transaction, such as a transfer of funds (Zweighaft, 2017). When the victim completes the transfer, the funds transfer to the attacker.

Rastenis et al. (2020) suggested a taxonomy for phishing that categorized the communication media, target devices, and attack techniques. The communication media categories were email, website, Instant Messenger, online social networks, blogs and forums, mobile apps, and Voice over Internet Protocol (VoIP). The target devices category included PCs, smart phones, voice devices (VoIP & phone), and Wireless Fidelity (Wi-Fi) devices. The attack techniques categories were attack initialization, data collection, and system penetration. Gupta et al. (2018) created a taxonomy based on the phases of creating an e-mail-based phishing attack. Those phases were (1) E-mail address selection, (2) E-mail content creation, (3) Sending the e-mail to recipients, (4) Waiting for the response from the e-mail recipients, (5) Phishing attack results and data gathering, (6) Usage of gathered results and data. Gupta et al. (2018) described e-mail address selection as how the attacker chooses which e-mail address to use, and included choosing known, existing addresses and generated address that would be verified in a later phase. E-mail content creation included the categories of presentation, creation strategy, personalized or not, and created by human or robot. The presentation category included a

benefit, a request, important information, or a possible failure. Creation strategy included generated, edited, or duplicated. A generated e-mail is new text for a specific phishing campaign. An edited e-mail is changed from a legitimate e-mail. A duplicated e-mail is copied from another source and not changed at all. Sending the e-mail to recipients included the categories of individual or group and systematic or not. Phishing attack results and data gathering included gathering secret data such as credentials, financial or company data, and validated e-mail addresses. Lastly, usage of gathered results included unauthorized access and financial fraud.

Several studies focused on spear-phishing (Burns et al., 2019; Butavicius et al., 2015; Halevi et al., 2015; Hanus et al., 2021; Mihelič et al., 2019; Oliveira et al., 2017), and all of the studies ran a simulated phishing campaign. Sample populations included students (Butavicius et al., 2015), employees from one large organization (Burns et al., 2019; Halevi et al., 2015; Mihelič et al., 2019), and residence of a geographic area (Oliveira et al., 2017). Butavicius et al. (2015) acknowledged that their sample population of students was a limitation and suggested future research that expanded the sample population. Halevi et al. (2015) and Oliveira et al. (2017) both investigated the demographics of their sample population and both found that women were more vulnerable to spear-phishing than men. More specifically, Oliveira et al. (2017) found that older women were the most vulnerable subset of their sample population. Oliveira et al. (2017) recommended correlating the volume of email received in a day with susceptibility to phishing, which this research did, and tailoring anti-phishing training tools to older people. Mihelič et al. (2019) found that phishing campaigns can be successful even if target's response time is short. Hanus et al. (2021) used machine learning to predict who would be a victim to

phishing. They found that spear phishing is more likely to successfully phish the user, and they found that many demographic factors have bearing on phishing victimization. They also found that the amount of attention that a user can devote to identifying a phish is significant. This is relevant to the present study because a goal of this study is to require the user to give a potential phish more attention.

Oliveira et al. (2017), Butavicius et al. (2015), and Burns et al. (2019) created treatments based on the framing of the simulated phishes. Oliveira et al. (2017) framed their phishes according to the following categories: Authority and Legal, Commitment and Ideological, Liking and Security, Perceptual Contrast and Health, Reciprocation and Social, Scarcity and Financial, and Social Proof and Social. They found that younger users were most susceptible to scarcity, while older users were most susceptible to reciprocation. Burns et al. (2019) framed their phishes according to the following categories: Group Gain, Group Loss, Individual Gain, and Individual Loss. They found that training users with individual loss messaging might increase the effectiveness of anti-phishing training. Butavicius et al. (2015) framed their phishes according to the following categories: Authority, Scarcity, and Social Proof. They found that participants were most susceptible to phishes framed with Authority.

Some of the spear-phishing studies discussed training (Burns et al., 2019; Oliveira et al., 2017). Burns et al. (2019) found that over half of their participants still clicked on a simulated phish even after training. Because of this result, they concluded that anti-phishing training is not effective. In addition, Burns et al. (2019) found that participants who were less impulsive were more likely to judge phishing as more dangerous. This

finding relates directly to this study, which aimed to move the user out of the impulsive, heuristic mindset before choosing to click or not on a potentially malicious link.

Of the studies that investigated non-spear-phishing, three of the studies used university communities (students, staff, faculty, and surrounding communities) as participants (Goel et al., 2017; Jensen et al., 2017; Musuva et al., 2019). Goel et al. (2017) invited third- and fourth-year undergraduate students to participate, while Jensen et al. (2017) and Musuva et al. (2019) invited students, faculty, and staff to participate. Another common sample was one or more organizations. Gordon, Wright, Glynn, et al. (2019) used one healthcare organization, whereas Gordon, Wright, Aiyagari, et al. (2019) used six healthcare organizations. A third type of recruitment was using social media or solicitation. Bravo-Lillo et al. (2011) used Craigslist and flyers posted in bus stops to recruit participants, and Junger et al. (2017) solicited visitors to a shopping mall. This study used social media also, recruiting participants from Facebook and LinkedIn.

Of the non-spear-phishing studies, many used a simulation (Goel et al., 2017; Gordon, Wright, Aiyagari, et al., 2019; Gordon, Wright, Glynn, et al., 2019; Jensen et al., 2017; Musuva et al., 2019), others used role-play and a survey (Parsons et al., 2019; Parsons et al., 2015; Rajivan & Gonzalez, 2018), one used open-ended interviews (Bravo-Lillo et al., 2011), and one used training and warning flyers (Junger et al., 2017). Many of the studies found that training was necessary (Jensen et al., 2017), but currently ineffective (Gordon, Wright, Aiyagari, et al., 2019; Junger et al., 2017). Goel et al. (2017) and Parsons et al. (2015) investigated content and framing in phishing e-mails. Goel et al. (2017) found that contextual messages that suggest loss, such as losing a scholarship, were the most effective. Rajivan and Gonzalez (2018) created a two-phase simulation

with Amazon Mechanical Turk (Mturk) users. In the first phase, they asked participants to craft phishes, and in the second phase, they tested participant reaction to those crafted phishes. Their results led them to theorize that attackers with higher creativity could be capable of changing and adapting their emails to evade detection, but their creativity may not determine their success in persuading end users to respond to their emails. They suggested for future research that data from this study could be used to develop linguistic models that detect adversarial phishing campaigns, Parsons et al. (2015) found that people use cues that are not good indicators of whether an email is a phish or genuine. They investigated cue categories of consistency, links, visual presentation, personalization, spelling, security, legal, sender, familiarity, urgency, and importance. They found that users did well on correctly identifying a phish or genuine email when the visual presentation was professional and when the email was personalized and important. They found that participants judged a phish poorly when it had an element of urgency. It may be that requiring the user to wait, as this study did, may overcome the sense of urgency. Musuva et al. (2019) found that a majority of university community members will disclose their password in a phishing simulation. They also discussed in depth the tools they used to launch the simulated phishing campaign so that future studies might use the same tools. While this study was not a simulated phishing campaign, simulated phishes were needed and so the discussion on phishing campaign tools is useful.

Many of the studies investigated how user characteristics correlate to phishing susceptibility (Alseadoon, 2014; Bravo-Lillo et al., 2011; Chen et al., 2018; Iuga et al., 2016; Wang et al., 2016), and one study focused on summarizing URL characteristics in a safety report (Althobaiti et al., 2021). Bravo-Lillo et al. (2011) investigated how novice

and advanced users use cues to phishing e-mails differently. They concluded that advanced and novice users do use different cues and arrive at different conclusions regarding possible risk. They stated that advanced users consider risk before clicking on a potentially malicious link, while novice users consider risk only after clicking on a potentially malicious link. Alseadoon (2014) and Iuga et al. (2016) used many of the same characteristics in their studies, including gender, age, and IT experience. Although both Alseadoon (2014) and Iuga et al. (2016) used IT experience, they measured the characteristic differently. Alseadoon (2014) measured how their participants used the Internet (surfing the web, social media, etc.), how long the participants have been online, and how much time the participants spend online in a day, and how much email the participants receive in a day. Iuga et al. (2016) measured whether their participants have been victims of phishing before, and if the participants have had any phishing awareness training. Iuga et al. (2016) also used education level. These characteristics are relevant to this study, which included age, gender, education level, attention span, and the volume of email received in a day. As with Halevi et al. (2015) and Oliveira et al. (2017), Iuga et al. (2016) also found that a participant's gender, as well as years of IT experience, have a statistically significant impact on the detection rate of phishing. Interestingly, Alseadoon (2014) found younger users more vulnerable to phishing, which contradicts the findings of Oliveira et al. (2017). Chen et al. (2018) investigated how trust in automated detection systems influences susceptibility to phishing. They found that system reliability has a profound influence on human performance. Wang et al. (2016) measured overconfidence, using two metrics of overconfidence, over estimation and over-precision. They hypothesized that cognitive effort reduces overconfidence, which is relevant to this study

since this study worked to require cognitive effort in the user. Wang et al. (2016) found that their hypothesis was supported. Althobaiti et al. (2021) created a URL feature report and tested it with eight focus group sessions. The focus groups included HCI experts, security experts, and students. The results showed that the groups generally liked the report and found that the report helped them to focus on the safety of the URL.

Some studies introduced a scale or model to explain phishing behavior (Parsons et al., 2019; Steves et al., 2020; Vishwanath et al., 2018). Parsons et al. (2019) and Vishwanath et al. (2018) created scales to measure factors in user behavior that leads to falling for a phish. Parsons et al. (2019) introduced the Susceptibility to Persuasion Strategies Scale which measured the authority, consistency, liking, reciprocity, scarcity, and social proof components of a phish. They tested the scale with a phishing simulation, and found that users who were susceptible to authority, liking, scarcity, social proof were more susceptible to phishing. They also stated that the findings showed that users tend to be susceptible situational impulsivity and suggested that teaching users to use systematic versus heuristic principles would be useful. This suggestion is directly relevant to this study since the goal of this study was to move the user into a systematic mindset.

Vishwanath et al. (2018) built a model that accounts for the cognitive, preconscious, and automatic processes that potentially leads to phishing-based deception. Steves et al. (2020) presented Phish Scale, which is a model to measure simulated phishes for use in a phishing simulation. This scale was useful for this study since simulated phishes were conducted in Phase III. The studies discussed in this section are summarized in Table 2.



**Table 2***Summary of Social Engineering: Phishing Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Algarni et al., 2017	Empirical, Grounded Theory & Survey	370 Employees from 3 Organizations	Role-Play & Questionnaire	Identified user characteristics as significant predictors of social engineering victimization
Althobaiti et al., 2021	Empirical	1,278 Employees	Model to predict user vulnerability	Model correctly predicted threats to high-severity cases 96% of time
Alseadoon, 2015	Empirical	780 Undergraduates in Australia and Saudi Arabia	A Simulated Phishing Campaign & Survey	A new model to explain the impact of users' characteristics on their detection behavior
Bravo-Lillo et al., 2011	Phenomenological & Closed-Lab	10 Novice, 20 Advanced Users	Open-Ended Interviews	Advanced and novice users use different cues and arrive at different conclusions about possible risk
Burns et al., 2019	Empirical & Simulation	250 Participants from One Organization	A Simulated Phishing Campaign	Anti-phishing training is not effective
Butavicius et al., 2015	Experimental & Simulation	121 Students from a Large South Australian University	A Simulated Phishing Campaign & Cognitive Reflection Test	Participants who were less impulsive were more likely to judge phishing as more dangerous
Chen et al., 2018	Experimental & Simulation	484 MTurk Users	A Simulated Phishing Campaign & Single-Question Survey	System reliability has a profound influence on human performance
Finn & Jakobsson, 2017	Empirical	Commentary	Phishing Attacks	Taxonomy for phishing studies
Goel et al., 2017	Theoretical & Simulation	7,225 Students	A Simulated Phishing Campaign	Contextual messages that suggest loss are the most effective types of phishing

**Table 2***Summary of Social Engineering: Phishing Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Gordon, Wright, Aiyagari et al., 2019	Empirical & Simulation	Convenience Sample of 6 Geographically Dispersed US Health Care Institutions	A Simulated Phishing Campaign	Simulated phishing campaigns may serve to educate employees
Gordon, Wright, Glenn et al., 2019	Experimental & Simulation	516 Employees of a US Healthcare System	A Simulated Phishing Campaign	A mandatory training program for the highest-risk employees did not decrease click rates
Gupta et al., 2018	Empirical	Commentary	Social Engineering Attacks	Categorized social engineering attacks
Hanus et al., 2021	Empirical	Over 1,400 employees of a SW US municipality	Simulation/Machine Learning	Many demographic factors have some bearing on phishing victimization
Halevi et al., 2015	Experimental & Simulation	40 Employees of Large Indian Company	A Simulated Phishing Campaign & Survey	Vulnerability to phishing is in part a function of users' personality
Iuga et al., 2016	Experimental & Simulation	382 Online Participants	A Simulated Phishing Campaign & Survey	Gender and the years of PC usage have a statistically significant impact on the detection rate of phishing
Jensen et al., 2017	Experimental	355 Faculty, Staff, and Students at a Midwestern University	A Simulated Phishing Campaign	Presentation of training need not be complex or costly, but it is necessary to mitigate phishing

**Table 2***Summary of Social Engineering: Phishing Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Junger et al., 2017	Experimental	278 Visitors to a Shopping Mall	Training Flyer & Questionnaire	Neither priming nor a warning influenced the degree of disclosure
Musuva et al., 2019	Experimental	241 University Community Members	A Simulated Phishing Campaign	Outlined the actual tools used to stage the phishing attack in detail
Oliveira et al., 2017	Experimental & Simulation	158 Participants from North Central Florida Area	Phone Screening & Survey	Training tools designed for older population should be created
Parsons et al., 2015	Experimental & Closed Lab	59 University Students	Role-Play and Survey	People use cues that are not good indicators of phishing or genuine email
Mihelič et al., 2019	Case Study & Simulation	407 Employees from One Organization	A Simulated Phishing Campaign	Phishing campaigns can be successful even if target's response time is short
Parsons et al., 2019	Experimental & Closed Lab	985 Working Australians	Role-Play & Web-Based Survey	Introduced Susceptibility to Persuasion Strategies Scale
Rajivan & Gonzalez, 2018	Experimental & Simulation	105 MTurk Users	Role-Play & Survey	Creativity in crafting a phish may not determine success in persuading end users to respond to the phish
Rastenis et al., 2020	Empirical	Commentary	Social Engineering Attacks	Categorized social engineering attacks
Salahdine & Kaabouch, 2019	Empirical	Commentary	Social Engineering Attacks	Categorized social engineering attacks

**Table 2**

*Summary of Social Engineering: Phishing Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Steves et al., 2020	Exploratory	73 Employees of NIST	A Simulated Phishing Campaign	Introduced Phish Scale
Thompson, 2012	Empirical	Commentary	Social Engineering Attacks	Discussed dangers of social engineering attack
Vishwanath et al., 2018	Experimental	125 Undergraduate Students	A Simulated Phishing Campaign & Survey	Built a model that accounts for the cognitive, preconscious, and automatic processes that potentially leads to phishing-based deception
Wang et al., 2016	Experimental	600 Individuals	A Simulated Phishing Campaign & Survey	Distinguished between retrospective overconfidence and perspective overconfidence

## **Heuristics**

### *Kahneman's System One and System Two and Decision Making*

In his book *Thinking Fast and Slow*, Kahneman (2011) introduced the concepts of System One and System Two as methods of describing human cognition. System One represents an instinctual thought process that comes quickly and automatically and requires little or no effort. Examples of System One are the ability to orient to a sudden sound or to detect if one object is closer than another (Kahneman, 2011). System Two is a slow, methodical thought process that requires deliberate effort. Examples of System Two are solving a complex mathematical equation or monitoring one's behavior in a

social situation (Kahneman, 2011). For typical, daily activities, System One is active, and System Two is in a low-effort mode. When System One encounters a more difficult task, it activates System Two. As a difficult task becomes more familiar, System One is able to take over the task. Kahneman (2011) stated that, given multiple ways to solve a problem, people will typically choose the path that requires the least amount of effort. As an illustration, he referenced a study in which college students were asked to solve a simple mathematical problem with an intuitive answer that was incorrect. The study indicated that the students did not check their work, although checking their work would have been easy to do (Kahneman, 2011). Kahneman (2011) also stated that task-switching is difficult, but that System Two can program the memory to override habit.

Tversky and Kahneman (1974) introduced the idea of a heuristic decision-making process that does not follow Bayesian probability. Kahneman (2011) described a heuristic as an assumption made to simplify a decision. According to Tversky and Kahneman (1974), if Bayesian probability were used, there would be evidence of using prior probabilities when making a decision. They referenced a study in which participants were given a description of a person in a group and asked if they thought that that person was a librarian or an engineer. In the study, some participants were told that there were more engineers than librarians in the group, and some were told that there were more librarians than engineers in the group. The result was that only the description of the person affected the participant's decision (Kahneman & Tversky, 1973). Tversky and Kahneman (1974) explained this departure from Bayesian probability by stating that decision-makers tend to use heuristic, intuitive judgement although that judgement may be wrong.

Gigerenzer (1991) countered Tversky and Kahneman (1974) by arguing that errors in judgement are not violations of probability theory. Gigerenzer (1991) questioned the methods of Tversky and Kahneman (1974), and stated that Tversky and Kahneman (1974) used too narrow a definition of norm and too highly selected a sample to be used in traditional probability and statistics. Kahneman and Tversky (1996) answered Gigerenzer (1991), and stated that only two of the 12 biases they referenced in 1974 apply to Gigerenzer's argument, and they countered Gigerenzer's claim that judgement heuristics are independent of context. In turn, Gigerenzer (1996) stated that the problem with heuristics is that it can be fit to any situation yet is too vague. Gigerenzer (1996) also countered the number of biases referenced by Kahneman and Tversky (1996), and stated that he found 13 biases and that five apply to his former argument. Vranas (2000) attempted to clear up misunderstandings in the debate between Kahneman and Tversky (1996) and Gigerenzer (1996). Vranas (2000) stated that Gigerenzer (1996) preferred to look at cognitive processes underlying decision making and that Gigerenzer (1996) was not stating that single-case judgements are invalid but that Gigerenzer (1996) wanted Kahneman and Tversky (1996) to present a proof that they are valid. Vranas (2000) stated that he did not think a proof was necessary and that Gigerenzer (1996) was assuming a frequentist view of statistics when it was likely that a subjectivist view was more appropriate. Both Kahneman and Gigerenzer reviewed Vranas (2000) before it was published.

A third model of decision making called the Recognition-Primed Decision (RPD) model was introduced by Klein (1993) and used by Rosa et al. (2021). Klein (1993) described the RPD model as a model in which the decision maker does not make a choice

between two or more options, but instead acts based on prior experience. Klein (1993) used the example of a firefighter chief in action at a fire. Asked afterwards how he chose what to do, the chief stated that he made no conscience choice and simply sprang into action (Klein, 1993). Rosa et al. (2021) analyzed the decisions of 478 active airline pilots and categorized the decisions into four groups: adapters, cautious, changers, and oscillators. They found that adapters made the most successful decisions of the four groups.

There have been many studies regarding how heuristics may affect user decision-making when faced with a computer security decision (Anderson et al., 2016; Bravo-Lillo et al., 2011; Gerlach et al., 2019). Many of the studies regarding heuristics used some kind of role-playing methodology in which the participants were given a scenario and asked for their response, either through interview (Arazy et al., 2017; Bravo-Lillo et al., 2011) or through action (Anderson et al., 2016; Gerlach et al., 2019). Students appeared to be common study participants in these types of investigations (Anderson et al., 2016; Arazy et al., 2017; Bravo-Lillo et al., 2011), and one study used a professional firm to recruit participants (Gerlach et al., 2019). Two of the studies distinguished between novice and advanced users (Arazy et al., 2017; Bravo-Lillo et al., 2011). Bravo-Lillo et al. (2011) distinguished advanced users by whether they had taken at least one computer security course or had worked in the computer security field for at least a year. Arazy et al. (2017) used professional university librarians as advanced users.

In general, the results of the studies regarding heuristics showed that some level of misjudgment occurs when heuristics are used (Bravo-Lillo et al., 2011; Chang & Chong, 2021; Gerlach et al., 2019). Bravo-Lillo et al. (2011) noted that advanced users differ

from novice users in that advanced users judge risk before taking action while novice users judge risk after taking an action. Chang and Chong (2021) studied COVID-19 fraud advisory cases and grouped the cases into a range of psychological vulnerabilities: affect (a feeling that demarcates the positive or negative quality of a stimulus), availability, cue-familiarity, representativeness, and scarcity heuristics. They found that users will often delude themselves into believing that an offer is real because they want it to be so. Anderson et al. (2016) stated as an implication that methods that reduce habituation should be used when displaying a warning. This implication relates directly to this study for which the goal was to reduce habituation when displaying a warning by displaying a countdown or count-up timer with the warning. The stated implication of Arazy et al. (2017) was that measuring heuristics is difficult. The studies described in this section are summarized in Table 3.

**Table 3**

*Summary of Kahneman's System One and System Two and Decision-Making Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Anderson et al., 2016	Empirical & Closed-Lab	25 Participants from University Community	fMRI	Polymorphic warnings are more effective than static warnings
Azary et al., 2017	Empirical, Survey, & Closed-Lab	12 Undergraduates for Quantitative & 3 Senior Librarians for Qualitative	Survey Using 7-Point Likert Scale & Think-Aloud	Assessments that are formed by agreement may still suffer from bias



**Table 3**

*Summary of Kahneman's System One and System Two and Decision-Making Literature –*

*(continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Bravo-Lillo et al., 2011	Phenomenological & Closed-Lab	10 Advanced Users and 20 Novice Users	A Warning Dialog & Open-Ended Interviews	Novice users often don't consider sensitivity of information they release; Phishing warning should warn of sensitivity of information
Chang & Chong, 2021	Case Study	Fraud advisories and cases	Model of five heuristic vulnerabilities	Identified range of five psychological vulnerabilities
Gerlach et al., 2019	Survey & Closed-Lab	321 Participants Recruited Through Professional Survey Firm	Pre-Existing News Mobile App & Questionnaire	High level of stereotypical thinking and systematic misjudgment shown
Gigerenzer, 1991	Grounded Theory	Decision Makers	A Scenario in Which a Decision Must be Made	Countered Kahneman's finding that decision makers use heuristics rather than statistical probability
Gigerenzer, 1996	Grounded Theory	Decision Makers	A Scenario in Which a Decision Must be Made	Countered Kahneman and Tversky (1996)
Kahneman, 2011	Empirical	Decision Makers	A Scenario in Which a Decision Must be Made	The structures of System One and System Two
Kahneman & Tversky, 1973	Grounded Theory	Predictors	A Scenario in Which a Prediction Must be Made	Previous information tends not to be used when making a prediction

**Table 3**

*Summary of Kahneman's System One and System Two and Decision-Making Literature –  
(continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Kahneman & Tversky, 1996	Grounded Theory	Decision Makers	A Scenario in Which a Decision Must be Made	"To correct Gigerenzer's (1991) misleading description of our work and his tendentious presentation of the evidence" pg. 583
Klein, 1993	Phenomenological & Closed-Lab	Firefighter Commanders	A Scenario in Which an Automatic Reaction is Required	Introduced Recognition-Primed Decision (RPD) model
Rosa et al., 2021	Empirical	478 Active Pilots	Simulation	Adapters were most successful of four coded groups
Tversky & Kahneman, 1973	Grounded Theory	Decision Makers	A Scenario in Which a Decision Must be Made	Introduced the idea of a heuristic decision-making process that does not follow Bayesian probability

### *Habituation*

In addition to cybersecurity, habituation is also a topic of interest in driver safety studies and in marketing. All the driver safety studies discussed here used a driving simulator to test driver habituation (Aminuddin & Nasir, 2019; Baldwin et al., 2017; He et al., 2011; Super et al., 2016; Zhang & Kumada, 2017). Three of the studies used an Electroencephalogram (EEG) to measure user reaction and habituation (Aminuddin & Nasir, 2019; Baldwin et al., 2017; Super et al., 2016). Some of the studies discovered that some kind of stimulation helps the driver to not habituate and leads the driver to be more aware of their surroundings. The stimulations used differed. Aminuddin and Nasir (2019)

used a radio, He et al. (2011) simulated heavy wind, Super et al. (2016) used recorded speech, and both Baldwin et al. (2017) as well as Zhang and Kumada (2017) asked their participants to do a measured task between driving simulations. These stimulations related to this study since a countdown or count-up timer can be considered a form of stimulation. Baldwin et al. (2017) stated that the main contribution of their study was that they were able to detect the internal cognitive state while driving. They stated that the implication of this contribution was that identifying periods of likely mind wandering could serve as a useful research tool for assessment of driver attention and could potentially lead to future in-vehicle safety countermeasures.

Consumer marketing is another area in which habituation is of interest. Martin (2008) advised marketers to “treat consumers like dogs” (p. 147) while using the concepts of behavioral conditioning when developing an advertising strategy. A number of studies concluded that shopping habits should not be overlooked by marketing professionals (Phang et al., 2018; Soraghan, 2019; Tadajewski, 2019). Mark et al. (2019) concluded that catalogs are still useful because they help to reinforce shopping habits of consumers. These studies all used different instruments. Mark et al. (2019) used transaction data of 1,000 customers of one anonymous retailer and a hidden Markov model. Phang et al. (2018) used a questionnaire to collect data from 180 young adults about their habits of shopping through a mobile app. Their finding was that hedonic motivation and habits play the most significant roles in intention to shop via mobile apps. Soraghan (2019) used observations, think-aloud techniques, and semi-structured interviews to collect data from 26 female shoppers of major United Kingdom grocery stores. She found that label nudging is not very useful, partially because habits are not overcome. Soraghan (2019)

speculated that grocery stores create a time pressure, which leads shoppers to use habit to move more quickly. This speculation is relevant to this study since the countdown or count-up timer was purposefully designed to slow down the user. Lastly, Tadajewski (2019) used a genealogical methodology. Specifically, he used theoretical arguments, conceptual ideas, and practice-based value systems to determine that we are “walking bundles of habit” (p. 456).

Some studies presented models of consumer behavior that incorporated habituation (Martin & Morich, 2011; Nadler & McGuigan, 2018; Osman, 2020). Martin and Morich (2011) and Nadler and McGuigan (2018) both used theoretical commentary to introduce their models. Martin and Morich (2011) used the categories of pilot, autopilot, and co-pilot. They defined pilot as the thought process that would be used in a new situation, which Kahneman (2011) calls System Two. The categories of autopilot and co-pilot would be both considered System One by Kahneman. Martin and Morich (2011) differentiated autopilot and co-pilot by stating that autopilot is completely automatic, and co-pilot is used in situations in which some conscious thought is needed, but not a fully conscious mind is needed. They stated that heuristics are used in the co-pilot category. Nadler and McGuigan (2018) encouraged marketers to look for patterns in consumer data that could be explained by heuristics and habits. Osman (2020) used an open-ended one-question survey to collect data from 399 volunteers from English-speaking countries. The question asked for an example in which the unconscious mind was influenced in some way. The answers were coded, and marketing was the most suggested category of five. The other four categories were research, therapy, political, and media.

There have been several studies regarding habituation in cybersecurity. These include investigating user habituation regarding Android privacy notices (Harbach et al., 2014), mapping habituation in the brain (Anderson et al., 2014a), the design of privacy notices (Karegar et al., 2020; Minakawa & Takada, 2017; Sunshine et al., 2009), and recovery from habituation (Kim & Wogalter, 2009). The types of studies used were closed-lab experimental (Anderson et al., 2014a; Harbach et al., 2014; Kim & Wogalter, 2009; Minakawa & Takada, 2017) and closed-lab between-subject studies (Karegar et al., 2020; Sunshine et al., 2009). The most common sample was students (Anderson et al., 2014a; Harbach et al., 2014; Kim & Wogalter, 2009; Minakawa & Takada, 2017), although one used Facebook users (Karegar et al., 2020), and one used Internet users in general (Sunshine et al., 2009).

All the studies included in this section ran a scenario with some kind of warning dialog. To gather results, some of the studies used some kind of tracking device, namely an fMRI (Anderson et al., 2014a), or an eye-tracking device (Karegar et al., 2020), and some used the time the participants used in interacting with the dialog (Karegar et al., 2020; Minakawa & Takada, 2017). The time used when interacting with the dialog may inform the timer value chosen by SMEs in Phase I of this study. Some studies used whether the warning dialog was clicked in multiple phases (Anderson et al., 2014a; Harbach et al., 2014; Karegar et al., 2020; Kim & Wogalter, 2009; Minakawa & Takada, 2017). Some used a questionnaire (Karegar et al., 2020; Kim & Wogalter, 2009; Minakawa & Takada, 2017; Sunshine et al., 2009) and one used a think-aloud methodology (Sunshine et al., 2009).

Although all of the studies in this section used scenarios with warning dialogs, most of them focused on different technologies. Anderson et al. (2014a) as well as Kim and Wogalter (2009) showed their participants series of images of warnings, Harbach et al. (2014) investigated user reaction to Android privacy notices, and Karegar et al. (2020) investigated different types of warning notices that required user interaction. Minakawa and Takada (2017) showed warning dialogs with sound, animation, and *Kawaii*, which is a Japanese word meaning cute (Minakawa & Takada, 2017). In the context of Minakawa and Takada (2017), *Kawaii* referred to the traditional Japanese animation form in which figures are designed to be cute. Sunshine et al. (2009) used Secure Socket Layer (SSL) certificate warning notices.

The results of using warnings were mixed. Most of the studies found warnings to be useful (Harbach et al., 2014; Karegar et al., 2020; Kim & Wogalter, 2009; Sunshine et al., 2009), but two did not (Anderson et al., 2014a; Minakawa & Takada, 2017). Rather than investigating whether warnings were useful, Anderson et al. (2014a) set out to map the area of the brain that was active when the users viewed the series of warnings. The brain mappings showed that the participants' visual area of the brain sharply decreased as they continued to view the warnings. They concluded that users cannot help but to ignore warnings to which they have habituated. This is relevant to this study since the countdown or count-up timer changed, and thus reduce habituation. Harbach et al. (2014) found that customized Android privacy notices were more effective than standard privacy notices. They reported that many participants chose not to allow the installation because of the personalized notice showing actual data. Overall, Harbach et al. (2014) found that the personalized privacy message led participants to take notice when they would have

otherwise dismissed the message without considering it. Karegar et al. (2020) found that the number of participants who used a drag-and-drop interface and who could recall why they shared data was significantly higher than participants in the other treatment groups. Kim and Wogalter (2009) found that user attention decreased as the warnings continued. Minakawa and Takada (2017) found that the Kawaii effect significantly decreased habituation when compared to the control group. Sunshine et al. (2009) found that the participants were more likely to heed the SSL warning notice when higher-risk website such as a bank website, and that participants tended to ignore the warning notice when accessing a lower-risk website such as a library website. Like Harbach et al. (2014), they also found that the custom warning notices were more likely to guide the participant into the correct action. Sunshine et al. (2009) stated that the best-case scenario would be to not show warnings at all, but rather to simply block access to websites that are not authorized by an SSL certificate, but they acknowledged that that scenario would be hard to accomplish.

Of the studies that stated future work, most of them suggested replicating their study with some kind of change (Harbach et al., 2014; Karegar et al., 2020; Minakawa & Takada, 2017). Karegar et al. (2020) stated that they would like to replicate phase two of the study at a future time, recognizing the priming effect of the questionnaire. They stated as an implication of their findings that drag-and-drop privacy dialogs should be developed and used. Minakawa and Takada (2017) stated that they would like to repeat their study, stating that the novelty of using Kawaii in this manner may have affected the results. Harbach et al. (2014) stated that they would like to study the long-term effect of customized Android privacy warnings. Anderson et al. (2014a) suggested using these

findings to develop warnings to reduce habituation as future work and stated as an implication of their study that any warning design should take habituation into consideration. This is relevant to this study since the warning design was meant to take habituation into account. Kim and Wogalter (2009) suggested incorporating text color and size into warning notices. This study incorporated text color into the warning text.

Overall, the studies in this section confirmed the presence of user habituation when viewing warning notices. It was found that warning notices that change (Minakawa & Takada, 2017), incorporate personal data (Harbach et al., 2014; Sunshine et al., 2009), or require some kind of user interaction (Karegar et al., 2020) are the most effective to reduce user habituation. Two of studies in this section recommended taking user habituation into account when designing warning dialogs (Anderson et al., 2014a; Kim & Wogalter, 2009). The studies described in this section are summarized in Table 4.

**Table 4**

*Summary of Heuristics: Habituation Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Aminuddin & Nasir, 2019	Experimental	20 Healthy Subjects	Driving Simulator & EEG	Driving focus is better if there is stimulation
Anderson et al., 2014	Empirical & Closed-Lab	24 Undergraduate and Graduate Students	fMRI	Located specific region in brain that exhibits habituation
Baldwin et al., 2017	Experimental	9 Participants	Driving Simulator & EEG	Detected the internal cognitive state while driving
Harbach et al., 2014	Survey, Narrative, & Closed-Lab	36 Students	Android App Permission Dialogs, Questionnaire & Think-Aloud	Users that receive personalized permission warning dialogs were significantly less likely to grant the requested permission



**Table 4***Summary of Heuristics: Habituation Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
He et al., 2011	Experimental	18 Members of the University of Illinois Community	Driving Simulator & Eye and Head Tracker	Mind wandering can engender a failure to monitor the environment while driving.
Karegar et al., 2020	Empirical & Closed-Lab	80 Facebook Users	Privacy Notices, Questionnaire, & Eye Tracking	Drag and drop action resulted in significantly more user attention
Kim & Wogalter, 2009	Survey & Closed-Lab	72 University Students	Repeated Visual Warnings & Questionnaire	Attention decreased as warnings continued
Mark et al., 2019	Experimental	1000 Customers of One Anonymous Retailer	Transaction Data & Hidden Markov Model	Catalogs help to reinforce habit in customers
Martin & Morich, 2011	Empirical	Commentary	Literature Review	Presents new model of consumer behavior that incorporates heuristics
Minakawa & Takada, 2017	Experimental & Closed-Lab	16 University Students	Security Warning Dialogs & Questionnaire	Effect of only Kawaii does not appear to reduce habituation, but dialog with audio, animation, and Kawaii does
Nadler & McGuigan, 2018	Empirical	Commentary	Behavioral Economic Model	Discusses a model in which behavioral economics depends on heuristics and habit
Osman, 2020	Experimental	399 Volunteers from English-Speaking Countries	Open-Question Survey	Marketing was the most mentioned category of ways in which the unconscious mind is influenced
Phang et al., 2018	Experimental	180 Young Adult Consumers	Questionnaire	Hedonic motivation and habits play the most significant roles in intention to shop via mobile apps

**Table 4***Summary of Heuristics: Habituation Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Soraghan, 2019	Ethnographic	26 Female Shoppers from Major UK Grocery Stores	Observations, Think-Aloud Techniques, & Semi-Structured Interviews	Label nudging is not very useful, partially because habits are not overcome
Sunshine et al., 2009	Narrative & Closed-Lab	100 Internet Users	SSL Warning Dialogs & Think-Aloud	Custom warnings were headed more significantly than standard warnings. Users still ignored warnings and misunderstood why warnings were triggered.
Super et al., 2016	Experimental	7 Healthy Subjects	Driving Simulator & EEG	Meaningful sound can avoid habituation
Tadajewski, 2019	Genealogical	Consumers	Theoretical Arguments, Conceptual Ideas, & Practice-Based Value Systems	Marketing must orient towards habit-creation
Zhang & Kumada, 2017	Experimental	40 Participants	Driving Simulator	Lower mental workload leads to mind-wondering

### Security in Mobile Devices

When compared to phishing using a desktop computer, phishing using a mobile device has not been widely studied (Bottazzi et al., 2015; Mukhopadhyay & Argles, 2011). A number of sources offered a taxonomy of mobile device attacks and discussed the unique security challenges that mobile devices present (Amro, 2018; Bitton et al., 2018; Chorghé & Shekokar, 2016; Goel & Jain, 2018; Ndibwile et al., 2017; Virvilis et

al., 2014). Bitton et al. (2018) categorized attacks into Applications, Communications and Browsing, Communication Channels, and Devices. Applications refers to exploits embedded in mobile apps, and Communication and Browsing refers to the data that passes between the user and the attacker. This is differentiated from Communication Channels in that Communication Channels refers to the channel technology itself. Examples include peripherals such as a memory card or an open Wi-Fi network. The Devices category includes vulnerabilities stemming from the device itself, such as an unlocked or jail-broken smart phone. Amro (2018) categorized phishing attacks into BEC, Service Updates, Promotional Offers, Spear Phishing, and Whaling. A Service Update attack mimics a service update request from a legitimate service such as Drop Box or Google Drive (Amro, 2018). A Promotional Offers attack mimics a promotional offer to obtain goods such as coupons, tickets, or gifts (Amro, 2018). Joo et al. (2017) classified smishing attacks as Application-based, Web-based, and Network-based. Smishing is an amalgamation of Short Message Service (SMS) and phishing and is used to describe SMS-based phishing attacks.

Challenges unique to a mobile device platform include a smaller screen which leads users not to see certain phishing cues that they might in a larger screen (Goel & Jain, 2018; Ndibwile et al., 2019) and which requires that some browser features be eliminated, including anti-phishing security features (Ndibwile et al., 2017; Virvilis et al., 2014). URLs are usually hidden by default in a mobile browser, decreasing user attention to any phishing cues in the URL (Chorghe & Shekokar, 2016). Users do not give as much attention to cues in mobile device browsers as they do in desktop browsers because of the smaller screen (Amro, 2018). Users also tend to trust their mobile device because their

device is usually close to them (Amro, 2018). Goel and Jain (2018) discussed the security challenge of the physical mobile device, which typically has additional vulnerabilities such as a camera, the user's physical location, and access to SMS.

Anti-phishing techniques suggested include blacklists (Amro, 2018; Chorghe & Shekokar, 2016; Goel & Jain, 2018; Virvilis et al., 2014), detecting a suspicious app (Chorghe & Shekokar, 2016), inspecting packets originating from an HTTPS get request (Bottazzi et al., 2015), using a QR code (Chorghe & Shekokar, 2016; Mukhopadhyay & Argles, 2011), using a lightweight phishing detection algorithm in a browser (Liu et al., 2021; Ndibwile et al., 2017; Ndibwile et al., 2019), and checking a URL for an Internet Protocol (IP) address (Wu et al., 2014). Blacklists are imperfect because they must be updated and therefore cannot detect a zero-day attack (Chorghe & Shekokar, 2016; Goel & Jain, 2018). A zero-day attack is one in which the vulnerabilities which an attack exposes are exploited on the same day on which the attack is exposed to the public (Goel & Jain, 2018). Chorghe and Shekokar (2016) stated as future work their intent to implement an anti-phishing tool that will be able to detect a zero-day attack, and Virvilis et al. (2014) stated plans to further study the effectiveness on blacklists in anti-phishing techniques on mobile platforms. Orunsolu et al. (2017) stated future work plans to set more powerful rules for URL detection and to include source code in the verifier. A number of studies presented algorithms that use machine learning, including a naïve Bayesian algorithm (Bottazzi et al., 2015; Joo et al., 2017; Kumar & Chaudhary, 2017; Orunsolu et al., 2017). Wu et al. (2014) presented an application that uses optical character recognition to extract text from a mobile device screenshot. From the extracted text, the application identifies the sender and URL. If the identity of the sender and the

URL are different, the app sends a warning to the user. Ndibwile et al. (2017) presented UnPhishMe, which is an algorithm that simulates a user login with invalid credentials and detects phishing based on the website's response. Liu et al. (2021) used a neural network to create a malicious webpage detection model. They found that the framework they built had a higher detection efficiency when compared to similar frameworks. Orunsolu et al. (2017) presented a lightweight Android app that works by verifying the URL of the target web page.

Two of the studies investigated user awareness of security risks in a smartphone environment (Koyuncu & Pusatli, 2019; Ophoff & Robinson, 2014). Both studies surveyed smartphone users; one surveyed smartphone users by taking an in-person poll in a Turkish shopping center (Koyuncu & Pusatli, 2019), and another used an online questionnaire to survey South African smartphone users (Ophoff & Robinson, 2014). Both studies found smartphone security awareness to be low, and both found that some kind of knowledge (formal education (Ophoff & Robinson, 2014) and IT expertise (Koyuncu & Pusatli, 2019)) to be a positive influence on security awareness. Koyuncu and Pusatli (2019) used age as a demographic and found that the oldest demographic (older than 50) had the lowest security awareness, followed by the youngest demographic (younger than 21). Ophoff and Robinson (2014) suggested as future work to investigate the influence of gender on security awareness. Both age and gender were demographic variables in this study.

Of the studies reviewed, the next most common characteristic of interest after security awareness was security attitude. Three studies reviewed investigated security attitude among smartphone users (Alsaleh et al., 2017; Chin et al., 2012; Imgraben et al., 2014).

As with the studies investigating security awareness, these studies also used some kind of survey to investigate the attitudes of smartphone users. Alsaleh et al. (2017) used structured interviews. Chin et al. (2012) also used structured interviews, but then followed up the interviews with observations. Imgraben et al. (2014) used paper and online surveys. While the overall contribution from Imgraben et al. (2014) was that users do not perceive a security threat on their smartphones, they did report that just over half of the users surveyed reported that they would not open an email from an unknown source. In addition Imgraben et al. (2014) reported that 70% of their users would not accept a Facebook friend request from an unknown source. In contrast to the overall result reported by Imgraben et al. (2014), Chin et al. (2012) reported that users are more concerned with smartphone security than with laptop security. Participants reported that they are less likely to do high-security tasks, such as check a bank account or enter a social security number on a smartphone, because of security concerns. Alsaleh et al. (2017) investigated the factors related to user smartphone security attitude. They reported that some users lock their smartphone mostly because they do not want friends or family members to be able to access their phone, but also that some users do not lock their smartphone because they feel as though they have nothing to protect. Implication of these studies included the idea that smartphone app designers could include security indicators in their apps (Chin et al., 2012) and improve support for user-oriented security features (Alsaleh et al., 2017).

Several studies investigated user security behavior with smartphones (Chassidim et al., 2020; Chen & Li, 2017; Das & Khan, 2016; Mi et al., 2020; Ngoqo & Flowerday, 2015; Nowitz, 2018; Nowrin & Bawden, 2018). Several of these studies also used

surveys (Chen & Li, 2017; Das & Khan, 2016; Mi et al., 2020; Nowrin & Bawden, 2018), but two used a mobile app mockup (Chassidim et al., 2020; Lindegren et al., 2021), one used a simulated phishing campaign (Nowitz, 2018), and one used an awareness measurement tool and scorecard (Ngoqo & Flowerday, 2015). Nowitz (2018) used phishes that had previously gotten through a university filter as a basis for the simulated phishes in their study. Nevertheless, they reported that the study was cut short because their simulated phishes were reported as suspicious. This study required simulated phishes, and, while the technique of using previous actual phishes as a basis may be useful, the fact that the phishes were reported as suspicious may negate the usefulness of the technique. All of these studies used smartphone users as participants, and some used university community members including students (Mi et al., 2020; Ngoqo & Flowerday, 2015; Nowrin & Bawden, 2018) and staff members (Nowitz, 2018). Ngoqo and Flowerday (2015) included gender in their demographics and noted that males tended to be more security aware than females. Two of these studies were longitudinal in nature (Mi et al., 2020; Ngoqo & Flowerday, 2015). Chen and Li (2017) reported that anticipated regret may influence user security actions and recommended emotion-based warnings. This is relevant to this study in that emotional reaction was expected, but the goal of this study was to mitigate that emotional reaction. Chen and Li (2017) also recommended security training that emphasizes personal skill and knowledge. Nowitz (2018) also discussed emotional reaction, stating that users are more susceptible to a message indicating gain than to a message indicating loss. Das and Khan (2016) found that user security behavior is low and warned that user security behavior puts organizations at risk. They reported that Android users exhibited higher security behavior

that Apple users. While this study did not differentiate between Android and Apple users, both were in the study by design, and the data between the two types of users could be analyzed in future research. Mi et al. (2020) found that user planning and self-control of actions mediated the relationship between user intention and user security behavior. Chassidim et al. (2020) also investigated user intent to install security applications. They found that intention to install increases as more security features are offered and that users are willing to compromise on medium levels of privacy intrusiveness. They proposed visual indicators at install time to let users know which apps have security features. Lindegren et al. (2021) used a mobile app to test user reaction to dialogs, drag-and-drop, and swiping interfaces. Their goal was to slow the user down and cause the user to think about the pending action. This study is relevant to the present study because a goal of the present study is to cause the user to pause and think about the pending action. In addition, Lindegren et al. (2021) used age, gender, and education level as demographics, which are also used in this study. Nowrin and Bawden (2018) observed moderate security behavior among users and noted that not all mobile security features were used equally. They suggested as future work to expand the study to other universities and stated that their study could help educators raise information security awareness among students and help authorities create appropriate strategies. Ngoqo and Flowerday (2015) proposed a framework which can be used to forecast the information security behavior profiles of student mobile phone user. The studies discussed in this section are summarized in Table 5.



**Table 5***Summary of Security in Mobile Devices Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Alsaleh et al., 2017	Experimental	30 Smartphone Users	Structured Qualitative Interviews	Identified factors that could influence smartphone user security behavior
Amro, 2018	Empirical	Mobile Browser Users	Anti-Phishing Techniques in Mobile Apps	Gave summary of anti-phishing techniques for mobile browsers
Bitton et al., 2018	Empirical	Mobile Device Users	Mobile Phishing Security Awareness	Gave taxonomy of mobile users' security awareness
Bottazzi et al., 2015	Case Study	Android Device Users	MP-Shield Android App	Presents MP-Shield, an Android application, implemented as a proxy service on top of the TCP/IP stack
Chassidim et al., 2020	Experimental	300 Smartphone Users	Mobile App Mockups	A low privacy invasion might signal that the security application provides less security
Chen & Li, 2017	Experimental	284 Smartphone Users	Survey	Both privacy concern and coping appraisal have a significant impact on the intention to adopt security defensive software
Chin et al., 2012	Experimental	60 Smartphone Users	Structured Interviews & Observations	Users are more apprehensive about performing privacy-sensitive tasks on their smartphones than their laptops.
Chorghe & Shekokar, 2016	Empirical	Android Device Users	Anti-Phishing Techniques on Android Devices	Gave summary of anti-phishing techniques for mobile browsers
Das & Khan, 2018	Experimental	500 Smartphone Users	Face-to-Face Survey	Overall level of security behavior is low

**Table 5***Summary of Security in Mobile Devices Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Goel & Jain, 2018	Empirical	Mobile Device Users	Phishing and Anti-Phishing Techniques in Mobile Apps	Gave an overview of mobile phishing attacks and countermeasures
Imgraben et al., 2014	Experimental	250 Smartphone Users	Survey	Users do not perceive cybersecurity to be a real threat
Koyuncu & Pusatli, 2019	Experimental	155 Smartphone Users	Survey	Awareness level of participants was fairly low
Lindegren et al., 2021	Empirical	60 Smartphone Users	Simulation/Post-Test Questionnaire	Drag-and-drop and swiping showed better results
Liu et al., 2021	Theoretical	Commentary	An advanced mobile malicious webpage detection framework	MMWD has higher detection efficiency when compared to similar frameworks
Mi et al., 2020	Longitudinal & Experimental	173 University Students	Survey	Planning and action control mediate the relationship between intention and security behavior
Mukhopadhyay & Argles, 2011	Empirical	Mobile Device Users	A Mobile App Using a QR Code & Security Analysis	Presents anti-phishing single-sign-on QR-code based model for mobile devices
Ndibwile et al., 2017	Empirical & Closed-Lab	40 Users from Information Science, Biological Science and Material Science Fields	UnPhishMe Android App & Questionnaire	UnPhishMe is effective in detecting web-based phishing attacks
Ndibwile et al., 2019	Empirical & Closed-Lab	206 Users with Varying Educational Background	Smart Eyeglasses & Custom Phishing Game on Android Smartphone	Awareness is not enough to avoid phishing attacks; Automatic assistance for phishing attacks should be provided

**Table 5**

*Summary of Security in Mobile Devices Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Ngoqo & Flowerday, 2015	Longitudinal Action Research	90 University Students	Awareness Measurement Tool and Scorecard	Proposed a new method for tracking and categorizing student mobile phone user security behavioral profiles
Nowitz, 2018	Field Experiment	141 University Staff Members	Simulated Phishing Campaign	Users are more susceptible to gain message than loss message
Nowrin & Bawden, 2018	Experimental	348 University Students	Quantitative Survey	Moderate security behavior was observed; Users did not use mobile security features equally
Ophoff & Robinson, 2014	Exploratory & Experimental	619 South African Smartphone Users	Questionnaire	Found association between expertise and adoption of smartphone security controls
Orunsolu et al., 2017	Empirical	Android Device Users	An Android App That is a Lightweight Anti-Phishing URL Verifier	An Android app that is a lightweight anti-phishing URL verifier
Virvilis et al., 2014	Empirical	5 Desktop Browsers and Their Mobile Counterparts	Manuel Inspection of Phishing URLs	Many mobile browsers do not sufficiently protect the user against phishing

## **Phishing Mitigation Techniques**

### *Polymorphic Dialogs*

A polymorphic dialog is one that changes in appearance each time it displays (Anderson et al., 2016; Brustoloni & Villamarín-Salomón, 2007; Egelman et al., 2008). Overall, all the studies in this section found polymorphic warnings to be more effective than static warnings. In particular, Vance et al. (2018) found that polymorphic dialogs

were heeded more significantly after three weeks than static dialogs. De Keukelaere et al. (2009) found that custom warning messages that received as input the user's experience were more effective. Brustoloni and Villamarín-Salomón (2007) found that polymorphic warnings help to mitigate unjustified risk. This relates to this study since a countdown or count-up timer in a warning dialog is a form of polymorphic dialog. The findings in these studies suggest that this study may have been successful in achieving its goal.

Most of the studies included in this section used a closed-lab experimental design (Anderson et al., 2016; Brustoloni & Villamarín-Salomón, 2007; De Keukelaere et al., 2009; Egelman et al., 2008) and one was a longitudinal study (Vance et al., 2018). The closed-lab studies asked the participants to interact with a polymorphic dialog in some way. The longitudinal study used an fMRI to examine the effectiveness of polymorphic dialogs over the course of three weeks.

A variety of instruments were used. Two of the studies used an fMRI (Anderson et al., 2016; Vance et al., 2018) as a way of gathering data, one study used custom-developed software (De Keukelaere et al., 2009), and two of the studies used browser warnings that already existed before the study (Brustoloni & Villamarín-Salomón, 2007; Egelman et al., 2008). Anderson et al. (2016) designed a study in the background color of a warning dialog was randomly changed. They used an fMRI and showed that participant brain activity was greater when viewing polymorphic dialogs than when viewing static dialogs. Egelman et al. (2008) found that the active warnings that were placed in the user's workflow were more effective than passive warnings.

Overall, the implications were that polymorphic dialogs are more effective than static dialogs so that future systems should use dialogs that change in some way (Anderson et

al., 2016; Brustoloni & Villamarín-Salomón, 2007; De Keukelaere et al., 2009; Egelman et al., 2008; Vance et al., 2018). De Keukelaere et al. (2009) stated as future work to create a longitudinal study to investigate the long-term effects on custom messaging that takes the user's previous actions as input. Anderson et al. (2016) suggested as future work to use field methodologies to increase external validity. This relates to this study which was a field methodology. Vance et al. (2018) suggested that future researchers could investigate factors that may lead to the ineffectiveness of security indicators. This relates to this study because it may be that heuristics lead to the ineffectiveness security indicators and a goal of this study was to move users out of a heuristic mindset. The studies discussed in this section are summarized in Table 6.

**Table 6**

*Summary of Phishing Mitigation: Polymorphic Dialogs Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Anderson et al., 2016	Empirical & Closed-Lab	25 University Community Members	fMRI	Polymorphic Warnings are more effective than standard warnings
Brustoloni & Villamarín-Salomón, 2007	Empirical & Closed-Lab	13 University Community Members	Warning Scenario & Justified and Unjustified Risks Accepted	Polymorphic Warnings with and without sound reduce frequency of unjustified risks
De Keukelaere et al., 2014	Empirical & Closed-Lab	32 Participants	Prototype Web-Mail Client & Questionnaire	Participants who received adaptive warnings opened fewer attachments than participants who received static warnings
Egelman et al., 2008	Empirical & Closed-Lab	60 Participants from General Population;	Interaction with Browser Warning & Exit Survey	Active warning more effective than passive warning
Vance et al., 2018	Empirical & Closed-Lab	16 Participants from Large University	fMRI	Mapped how habituation of attention to security warnings maps to actual behavior

### *Training*

There is disagreement regarding whether anti-phishing training is effective. Bax et al. (2021), Burns et al. (2019), Caputo et al. (2013), Goel and Jain (2018), Gordon, Wright, Glynn, et al. (2019), and Junger et al. (2017) found anti-phishing training to be largely ineffective. Alnajim and Munro (2009), Baslyman and Chiasson (2016), Chatchalermpun and Daengsi (2021), Jenkins and Durcikova (2013), Kumaraguru (2009), Sun et al. (2017), and Volkamer et al. (2018) found anti-phishing training to be largely effective. This disagreement suggests that anti-phishing training as it is implemented today may not be effective, but that a solution that uses components of anti-phishing training may be useful. Dhamija et al. (2006) stated that training is necessary, but that many users do not use the right cues to detect phishing. One of the goals of this study was to train users to pause and think, which could be considered an aspect of current anti-phishing training but does not use anti-phishing training itself in its current form. Miranda (2018) stated that a phishing training program can help to mitigate risk of phishing. He also stated that training should be repeated periodically and gave a framework for e-mail-based anti-phishing training. Bax et al. (2021) used a survey instrument and found that when users respond to a perceived reward that users exhibit maladaptive behavior.

Baslyman and Chiasson (2016) classified anti-phishing training into three categories: online training tutorials, embedded training systems, and educational games. Online training tutorials are tutorials that are offered out of context, whereas embedded training systems are offered in context immediately after the user falls to a phishing attack. Educational games can take the form of an online game (Sun et al., 2017) or a physical board game (Baslyman & Chiasson, 2016).

Gordon, Wright, Glynn, et al. (2019) found that a mandatory online training tutorial was less effective than an embedded training system. They found that the immediate training had more impact than the online training tutorial. In addition, mandatory training did not decrease the click rate on phishing emails. Gordon, Wright, Glynn, et al. (2019) suggested that future work could expand to more organizations and gather employee role demographics. Jenkins and Durcikova (2013) also compared an online training tutorial with an embedded system (which they called a just-in-time reminder) and recommended a combination of both trainings. They stated that an online training tutorial will help to change attitudes and beliefs in users, but that changing attitudes and beliefs is not enough. Chatchalermpun and Daengsi (2021) ran a phishing simulation, and then sent an email explaining the simulated phish to all users who were victims of that phish. They ran another simulation and found that response to the simulated phish decreased by 16%. Users still need to be reminded, so that an embedded system is necessarily as well. They also stated that an embedded-only system is not sufficient because users will ignore a just-in-time reminder if they have the wrong attitude or belief. Jenkins and Durcikova (2013) suggested as future work to measure objective security behavior. Harrison et al. (2019) compared three types of training and found that mindfulness-based training was more effective than rules-based training. Jensen et al. (2017) also found mindfulness-based training more effective than rules-based training. This finding is relevant to this study since the goal of the study was to produce a kind of mindfulness in the user.

Several studies investigated embedded training (Alnajim & Munro, 2009; Burns et al., 2019; Caputo et al., 2013; Jensen et al., 2017; Kumaraguru, 2009; Nguyen et al., 2021; Volkamer et al., 2018; Wash & Cooper, 2018). Only some of these studies found

embedded training to be useful. Caputo et al. (2013) found training to be ineffective because it was ignored. Others did find embedded training to be useful. Kumaraguru (2009) found that participants made significantly better decisions after training and that the participants retained the training for at least seven days. They introduced an embedded training system called PhishGuru and studied embedded training by comparing the effects of an all-text security notice, a notice with a graphics/text combination, and a notice in the form of a comic strip. They found that the all-text security notices were the least effective, and the comic strip notice was the most effective, although some participants felt that the comic-strip notice was too childlike. Kumaraguru (2009) suggested that future researchers apply embedded training in other scenarios and test other mediums of training. Alnajim and Munro (2009) found that embedded alerts were more effective than the anti-phishing emails. Alnajim and Munro (2009) proposed an anti-phishing approach which compared online training in the form of anti-phishing email tips with embedded training in a web browser. Nguyen et al. (2021) used crowdsourcing to provide a safety report for emails received. Crowdsourcing refers to a method in which a task is performed by a large, unidentified group of people (Nguyen et al., 2021). They found that providing a crowdsourced report reduced anxiety and encouraged warning acceptance in users. They found that individuals who used the crowdsourced report had significantly higher message judgement accuracy.

A few studies used an experimental simulation study that used a phishing campaign to study embedded training (Burns et al., 2019; Caputo et al., 2013; Wash & Cooper, 2018). Burns et al. (2019) found that post-event training with an individual loss message was most effective and suggested that future researchers investigate with multiple rounds



of framed training. Caputo et al. (2013) found that the difference in the framing types was not statistically significant and explained the lack of significance by stating that many of the participants ignored the training. Caputo et al. (2013) suggested that their study be replicated while somehow compelling the participants to read the training. Wash and Cooper (2018) found that anti-phishing advice was more likely to be followed when it appears to come from an expert. Jensen et al. (2017) compared rule-based embedded training with a mindfulness approach. They found that the mindfulness training resulted in less susceptibility to phishing attacks than rule-based training and recommended combining the two types of training in future studies. Jensen et al. (2017) suggested that mindfulness may be a useful tool in other information technology fields.

Junger et al. (2017) and Volkamer et al. (2018) investigated the effects of training that were not online. Junger et al. (2017) distributed paper flyers on phishing. Before and after distributing the flyers, they asked the participants for private information, namely their partial bank account number. They noted that the flyer did not make a statistically significant difference in the percentage of participants who disclosed information and stated that the participants did not connect the flyer with the request for private information. Volkamer et al. (2018) investigated video-based training and found that participants did significantly better both immediately after watching the video and eight weeks later.

Several studies investigated training through gaming (Hale et al., 2015; Sheng et al., 2007; Sun et al., 2017; Weanquoi et al., 2018; Wen et al., 2019). Most of the studies creates an electronic game (Baslyman & Chiasson, 2016; Hale et al., 2015; Sheng et al., 2007; Sun et al., 2017; Weanquoi et al., 2018; Wen et al., 2019). All studies reported a

better understanding of anti-phishing techniques after the game was played. Sheng et al. (2007) found no significant difference among the gender or age demographics. Sheng et al. (2007) created Anti-Phishing Phil, which was designed to teach users how to identify phishing URLs, where to look for cues for trustworthy or untrustworthy sites in web browsers, and how to use search engines to find legitimate sites. They used learning science principles and recommended that future studies use these principles as well. Wen et al. (2019) created a game called What.Hack and compared it to Anti-Phishing Phil. They found that their game was more effective and engaging than Anti-Phishing Phil. Hale et al. (2015) created a web simulation platform called CyberPhishing. CyberPhishing simulates an e-mail inbox, which is relevant to this study which was designed to also simulate an e-mail inbox. Links and attachments in the CyberPhishing simulation work as they would in a real situation, and this study also designed links and attachments to work as they would in a real situation. Hale et al. (2015) found that a majority of participants were able to correctly identify a phish while playing the game. Sun et al. (2017) created a game for children in which the players complete a game-based challenge and then a learning task. The participants could not continue to the learning task until they completed the game-based challenge. Sun et al. (2017) found that learners tended to learn from their mistakes. Weanquoi et al. (2018) created a game called A Bird's Life in which the player is a bird and must choose good worms over bad worms. The bad worms represented phishes. They found that the game had a positive impact on students' learning about phishing attacks. Their stated future work was to continuously improve the game based on player feedback.

Baslyman and Chiasson (2016) created a board game, which they validated with an expert panel of three SMEs. The participants participated in pre-test interviews, played the game, and then completed a questionnaire which used a five-point Likert scale. Since the pre-test and post-test were the same questions, validity of results comes into question since the participants may have answered how they believed the researchers wanted them to answer. Baslyman and Chiasson (2016) found that after playing the game, participants had better understanding of phishing scams and learnt how to better protect themselves. Baslyman and Chiasson (2016) intend to simplify game instructions and to expand the game for future studies.

Stated implications included that organizations are susceptible to spear phishing (Burns et al., 2019) and that text-based training is not sufficient to teach anti-phishing techniques (Kumaraguru, 2009). Jenkins and Durcikova (2013) stated that behavior and intention may not be enough to mitigate information disclosure. Caputo et al. (2013) stated that a way must be found to convince users to read training.

Many studies related to phishing training recruited university community members as participants (Dhamija et al., 2006; Harrison et al., 2019; Jenkins & Durcikova, 2013; Jensen et al., 2017; Sheng et al., 2007; Wash & Cooper, 2018; Weanquoi et al., 2018; Wen et al., 2019) and some recruited corporate employees (Anderson et al., 2015; Burns et al., 2019; Caputo et al., 2013; Gordon, Wright, Glynn, et al., 2019; Kumaraguru, 2009). Junger et al. (2017) recruited visitors to a shopping mall. Three studies recruited participants according to personal attributes rather than physical location (Alnajim & Munro, 2009; Baslyman & Chiasson, 2016; Sun et al., 2017). Sun et al. (2017) recruited children aged between nine and 12. Alnajim and Munro (2009) recruited participants

with no phishing awareness, and Baslyman and Chiasson (2016) recruited some computer science experts as part of their sample population (four out of 21 participants). The studies discussed in this section are summarized in Table 7.

**Table 7**

*Summary of Phishing Mitigation: Phishing Training Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Alnajim & Munro, 2009	Empirical & Closed-Lab	36 Participants with No Phishing Awareness	Embedded Alert in Web Browser & Pre-Test Questionnaire	Post-event training more effective than sending anti-phishing tips by email
Baslyman & Chiasson, 2016	Empirical & Closed-Lab	21 Participants, 4 were Computer Science Experts	Board Game & Questionnaire	After playing the game, participants had better understanding of phishing scams and learnt how to better protect themselves
Bax, et al., 2021	Empirical	616 Participants	Questionnaire	Rewards influence maladaptive behavior in response to email phishing threats
Burns et al., 2019	Empirical & Simulation	260 Employees from Single Organization	Phishing Campaign	Post-event training with individual loss message most effective
Caputo et al., 2013	Empirical & Simulation	1359 Employees from a Medium-Sized DC-Based Industrial Organization	Phishing Campaign	Training is not effective because it was ignored; Framing did not make a statistically significant difference

**Table 7**

*Summary of Phishing Mitigation: Phishing Training Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Chatchalermpun & Daengsi, 2021	Case Study	20,300 Workers	Simulation	Training is effective in mitigating phishing
Dhamija et al., 2006	Empirical	22 University Community Members	Web Site	Many users do not use the right cues to detect phishing
Gordon et al. 2019	Empirical & Simulation	6416 Employees at 1 Tertiary-Care Medical Center	Phishing Campaign	Immediate training had more impact than online course; Mandatory training did not decrease click rate
Hale et al., 2015	Empirical	14 Participants	CyberPhishing Game Platform	Created a web simulation platform called CyberPhishing
Harrison et al., 2019	Empirical	422 University Community Members	Three Different Types of Anti-Phishing Training	Mindfulness-based training was significantly better than rules-based training for improving phishing detection rate
Jenkins & Durcikova, 2013	Empirical & Simulation	194 Students	Online Simulation	Attitude influenced intention, but intention did not mitigate information disclosure
Jensen et al., 2017	Empirical & Simulation	355 Faculty, Staff, and Students at a Midwestern University	Computer-Based Training Programs and Simulated Phishing Campaign	Mindfulness training resulted in less susceptibility than rule-based training
Junger et al., 2017	Survey	278 Visitors at a Shopping Mall	Training Leaflet & Questionnaire	Priming/brief training didn't help; participants did not make connection between leaflet and questions
Kumaraguru, 2009	Empirical & Simulation	311 employees of Large Portuguese Company	Embedded Training System: PhishGuru	Participants in training made significantly better decisions after training; Knowledge retained for at least 7 days; Difference in training type not significant

**Table 7**

*Summary of Phishing Mitigation: Phishing Training Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Miranda, 2018	Literature Review and Synthesis		Phishing Training Best Practices	Outlined structure for email-based phishing training
Nguyen et al., 2021	Empirical	438 Students	Simulation of Crowdsourced Warning System	Individuals had significantly higher message judgement accuracy
Sheng et al., 2007	Empirical	42 University Community Members	Anti-Phishing Phil	Anti-phishing game helped players to identify phishing

## **Timers**

Few studies were found regarding social engineering that employed timers. Molinaro (2019) used a countdown timer during which her participants were asked to distinguish phishing e-mails from valid e-mails, but the timer was not the focus of her study.

However, work related to timers in other research fields have been conducted. The sections below provide information about research from other fields related to timers.

### *Healthcare*

In the field of healthcare, the research showed that timers are used to remind workers of a task or of a medical emergency. Three studies incorporated a mobile app including for an Android tablet (Lindahl et al., 2019; Uddin et al., 2017) and for a smartphone (Hung et al., 2020). Marto et al. (2016) found that introducing a countdown timer with a reminder that stroke is an emergency to an emergency stroke patient's room decreased

the time between when the patient arrived in the emergency room and the time the patient received a drug that is able to dissolve a clot. Lindahl et al. (2019) created an Android tablet app that allows patients to self-administer a blood-pressure test. In the app, the timer reminded the patient to sit still for five minutes. Lindahl et al. (2019) reported that 99% of 100 pregnant women followed the timer guidance and were able to complete the blood-pressure test. Uddin et al. (2017) created an Android tablet app to reduce Operating Room (OR) turnover time. Uddin et al. (2017) presented a timer in the OR with successive green then yellow then red as the timer counted down. If the timer expired, the user was asked to indicate why there was a delay. Uddin et al. (2017) reported that the countdown timer was effective in reducing OR turnover time and reported as future research to place the system in the gastrointestinal lab as well.

Hung et al. (2020) created a smartphone app to guide hospital cleaning staff in the cleaning of patient beds. The app alerted staff to which beds needed to be cleaned and provided a countdown timer to indicate the deadline for cleaning the bed. Hung et al. (2020) stated that there was a significant decrease in time required for cleaning beds when the app was in use. The studies discussed in this section are summarized in Table 8.

**Table 8**

*Summary of Timers: Healthcare Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Hung et al., 2020	Experimental	Hospital Bed- Cleaning Staff	App for Bed- Cleaning Management & Questionnaire	Significant decrease in time to clean a bed

**Table 8***Summary of Timers: Healthcare Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Lindahl et al., 2019	Experimental	100 Pregnant Women	Tablet App for Blood Pressure self-Measurement & Questionnaire	Majority of participants were able to take accurate blood pressure readings
Marto et al., 2016	Experimental	Stroke Patients	Timer in ER	Time to treat was reduced with the presence of the timer
Uddin et al., 2017	Experimental	232 OR Cases	An Android Tablet App Designed to Reduce OR Turnover Time	Countdown timer found to be effective

*Civil Engineering*

The civil engineering literature regarding timers investigated Pedestrian Countdown Signals (PCS) at intersections. Researchers from different parts of the world have investigated PCS, including India (Biswas et al., 2017), Canada (Rothman et al., 2019), Ireland (Keegan & O'Mahony, 2003), China (Tang et al., 2020), and the US (Kitali et al., 2018). A PCS is a countdown timer that indicates to a pedestrian waiting to cross a road at an intersection when it is safe to cross (Keegan & O'Mahony, 2003). Many of the studies were cross-sectional (Biswas et al., 2017; Rothman et al., 2019), and one was a survey (Keegan & O'Mahony, 2003). Biswas et al. (2017) studied the effect PCS and Driver Countdown Signals (DCS) had on the interaction between drivers and pedestrians. They found that the number of drivers that drove through a red light increased when a DCS was present, and that as the DCS neared zero, drivers moved into the crosswalks,



blocking pedestrian movement. They concluded that PCS and DCS have an overall positive effect on traffic flow but an overall negative effect on pedestrian safety. In contrast, Keegan and O'Mahony (2003) reported findings that pedestrian safety increased because PCS decreased the number of pedestrians that crossed the road during a do not walk signal. They also reported that pedestrians often overestimate the time required to cross, stating that pedestrians would start to cross when there wasn't enough time left on the PCS. Keegan and O'Mahony (2003) stated that, because their study showed promise for the positive influence of PCSs, PCSs were being introduced to more of the Dublin area. Kitali et al. (2018) used a before-after study with the empirical Bayes method to analyze secondary data. They found that drivers used PCS as cues and that PCS improved driver safety. Rothman et al. (2019) also used secondary data to study the effects of PCS on pedestrian-motor-vehicle collisions. They found that the effects of PCS on pedestrian-motor-vehicle collisions varied based on age and location. Tang et al. (2020) studied the effect of PCSs on the behavior of electric bike users. They found that there were more near-violations at intersections with timers. The studies discussed in this section are summarized in Table 9.

**Table 9**

*Summary of Timers: Civil Engineering Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Biswas et al., 2017	Experimental	Pedestrians in Crosswalks at Signaled Intersections	Driver and Pedestrian Countdown Timers	As driver countdown timer ended, drivers moved into crosswalks

**Table 9***Summary of Timers: Civil Engineering Literature – (continued)*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Keegan & O'Mahony, 2003	Experimental	Pedestrians in Crosswalks at Signaled Intersections	PCS & Questionnaire	PCS reduce number of pedestrians that cross during don't walk signal
Kitali et al., 2018	Correlational	Drivers at Signaled Intersections	PCS & Secondary Data	PCS significantly improve driver safety
Rothman et al., 2019	Correlational	14,911 Pedestrian Motor Vehicle Collisions (PMVC)	PCS & Secondary Data	The effects of PCS on PMVC may vary by age and location
Tang et al., 2020	Empirical	3,128 Electric Bike Users	Observation	More near-violations at intersections with timers

*Psychology*

Many areas of psychology have been represented by studies that include timers including somnology (Lo et al., 2019), urgent decision making (Barque-Duran et al., 2017; Cheong, 2018), standardized testing (Brooks et al., 2003), child psychology (Newquist et al., 2012), and remote team communication (Fine, 2016). Fine (2016) found that a common timer between two remote team members increased performance. Cheong (2018) found that a timer increased urgent decision making skill regarding whether to evacuate a home in danger of fire as long as the psychological pressure from the timer was not too high. Barque-Duran et al. (2017) presented their participants with a simulated moral dilemma and found that a timer resulted in a more utilitarian choice, especially on

a smartphone versus a Personal Computer (PC). In contrast, Newquist et al. (2012) found that a timer did not help children make a decision requiring more self-control, and Brooks et al. (2003) found a non-significant difference between the scores of timed and untimed standardized test-takers. Lo et al. (2019) used a count-up timer to measure participant vigilance in a sleep study. The studies discussed in this section are summarized in Table 10.

**Table 10**

*Summary of Timers: Psychology Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Barque-Duran et al., 2017	Experimental	250 Amazon MTurk Workers	Simulated Trolley Problem & Questionnaire	Time pressure resulted in a more utilitarian choice
Brooks et al., 2003	Experimental	360,000 Students	Standardized Test	Small improvement for untimed students before grade 6, small improvement for timed students after grade 6
Cheong, 2018	Experimental	300 Subjects	Map-Based Representations & Questionnaire	Time pressure increased performance as long as the pressure wasn't too high
Fine, 2016	Experimental	8 Groups of 2 Students	Bomb Diffusion Game	Common timer aided task performance
Lo et al., 2019	Experimental	Adolescents Aged 15-19	Polysomnography	Adolescents with split sleep schedule were less impaired than adolescents with continuous sleep
Newquist et al., 2012	Experimental	3 Children from Ages 3 to 5	Edibles & Toys	The timer was not effective for enhancing self-control

## **Text Color**

There appears that very limited research exists that investigated the effect of text color in phishing warning notices. Anderson et al. (2015) investigated the effect of color warning images versus greyscale warning images, and other studies investigated text color, but not in the cybersecurity field (Bazilinskyy et al., 2019; Grummon et al., 2019; Mehta et al., 2017; Silver et al., 2002; Wogalter et al., 2002). Bazilinskyy et al. (2019) studied the effect of text color on electronic warning notices on the front bumper of automated cars to warn pedestrians at an intersection because the driver of the car may not be paying attention. Grummon et al. (2019) investigated the effect of color on high-sugar warning notices on products such as cola. Mehta et al. (2017) studied the effect of color of a chat wait dialog on the number of prank chats to a child help line. Silver et al. (2002) studied the effect of color on a warning label on crayons and on muriatic acid.

There are inconsistencies with regard to the effect of text color on the hazard perception of a warning. Wogalter et al. (2002) stated that red has been found to increase the hazard rating of a warning, and that colored labels, especially red, are more noticeable than grey. Grummon et al. (2019) found a that warning notice with white text on a red background to be the most effective, but Mehta et al. (2017) found that those who have higher attention-seeking behavior tended to disregard red warnings and Anderson et al. (2015) found that participants did not make better decisions when presented with a red warning image vs a grey warning image. Bazilinskyy et al. (2019) found that color itself did not significantly affect pedestrian action, but that it acted as a reinforcer to the text message on pedestrian action. Silver et al. (2002) stated that the colors that communicate hazard from highest to lowest perception are black, blue, red, and orange. They

acknowledged that black as the highest perceived hazard warning color contradicts others who found that red is the highest perceived warning color and offered the explanation that darker colors are perceived as more hazardous.

All of the studies reviewed used some kind of simulation in which the participants saw a variety of colored or greyscale messages. In three different studies, Mehta et al. (2017) showed messages in red, blue, or white and found that, while red messaging seemed to have the opposite desired effect of warning, blue and white did not show a statistically significant difference in user reaction. Anderson et al. (2015) compared red to greyscale warnings by displaying the warnings to the participants and using an EEG to measure the participants' reaction to the warnings. They found no difference in decision-making ability when the red vs greyscale warnings were shown. Anderson et al. (2015) acknowledged that the finding of no difference between greyscale and colored warnings contradicted past studies and recommended further studies in other colors such as blue. Mehta et al. (2017) also recommended that future studies compare warnings in blue versus white and also that the effect of the color red on compliance be investigated further in other settings. Nadeem and Junger (2019) chose blue for the warning notice to laptop users not to leave laptops unattended because it is a "warm, communicative, and a peaceful color" (p. 13). The studies discussed in this section are summarized in Table 11.

**Table 11***Summary of Text Color Literature*

Study	Methodology	Sample	Instrument/ Constructs	Main Findings or Contribution
Anderson et al., 2015	Experimental	61 Volunteers from Large Private University	Browser Warnings & EEG	Found no difference in P300 readings when viewing red vs grayscale
Bazilinskyy et al., 2019	Experimental	1319 Participants from 75 Countries	Photo of Car with Colored Text Message & Questionnaire	Text message more persuasive than color; color acted as reinforcer
Grummon et al., 2019	Experimental	1413 US Adult MTurk Workers	High Sugar Food Warning Labels on Cola & Questionnaire	Warning with white text and red background most effective
Mehta et al., 2017	Experimental	4152 Users	Child Helpline Chat Wait Screen	Red can lead to non-compliant behavior
Nadeem & Junger, 2019	Experimental	22 Laptop Owners	Warning Sign in a Study Hall	Significant reduction in laptops left in the presence of a warning sign
Silver et al., 2002	Experimental	124 Undergraduate Students	Warning Labels & Questionnaire	Black, blue, red, and orange were perceived as highest to lowest hazard, respectively
Wogalter et al., 2002	Empirical	Commentary	Warnings	Guidelines for warning design

**Summary of What is Known and Unknown in Literature**

It is known that social engineering is one of the most under researched and most effective cybercrimes (Jain et al., 2016) and that technical solutions to social engineering don't typically work (Krombholz et al., 2015). There are many different types of phishing attacks (Salahdine & Kaabouch, 2019). Phishing still persists because users are baited with fear or excitement (Goel et al., 2017). The phishing techniques are dynamic and so

that no solution works in the long-term. The best way to counteract phishing is unknown (Krombholz et al., 2015).

It is known that humans use heuristics to make quick, instinctual decisions (Kahneman, 2011) and that sometimes the use of heuristics can lead to misjudgments (Bravo-Lillo et al., 2011; Gerlach et al., 2019). Measuring heuristics is difficult (Arazy et al., 2017). Habituation occurs when users are exposed to the same warning dialog repeatedly which leads users to move to a heuristic thought process (Anderson et al., 2014b; Kim & Wogalter, 2009). Requiring user interaction reduces habituation (Harbach et al., 2014; Karegar et al., 2020).

Phishing is more effective on a mobile device, at least partially because of the smaller screen (Amro, 2018; Goel & Jain, 2018), but it is unknown how to stop phishing attacks on a mobile device, including how to stop a zero-day attack (Chorghé & Shekoker, 2016). Polymorphic dialogs help to reduce habituation (Anderson et al., 2016; Brustoloni & Villamarín-Salomón, 2007) and that polymorphic dialogs are more effective than static dialogs (Anderson et al., 2016; Brustoloni & Villamarín-Salomón, 2007; De Keukelaere et al., 2009; Egelman et al., 2008; Vance et al., 2018). It is unknown what the long-term effect of polymorphic dialogs is (De Keukelaere et al., 2009) or whether anti-phishing training is effective.

It is unknown how effective timers are in phishing mitigation techniques although it is known that timers are effective in many cases in healthcare (Hung et al., 2020; Marto et al., 2016; Uddin et al., 2017), civil engineering (Biswas et al., 2017; Rothman et al., 2019), and psychology (Fine, 2016) in moving a person into a logical thought process. It

is unknown how widely effective timers are in these fields since some studies found timers to be ineffective (Brooks et al., 2003; Newquist et al., 2012).

It is also unknown what effect text color has when used in cybersecurity warnings although it is known that color is more effective than greyscale (Anderson et al., 2015). There is disagreement regarding how effective the color red is in indicating a hazard. It is unknown what effect blue has when used as a text color in hazard warnings.



## Chapter 3

### Methodology

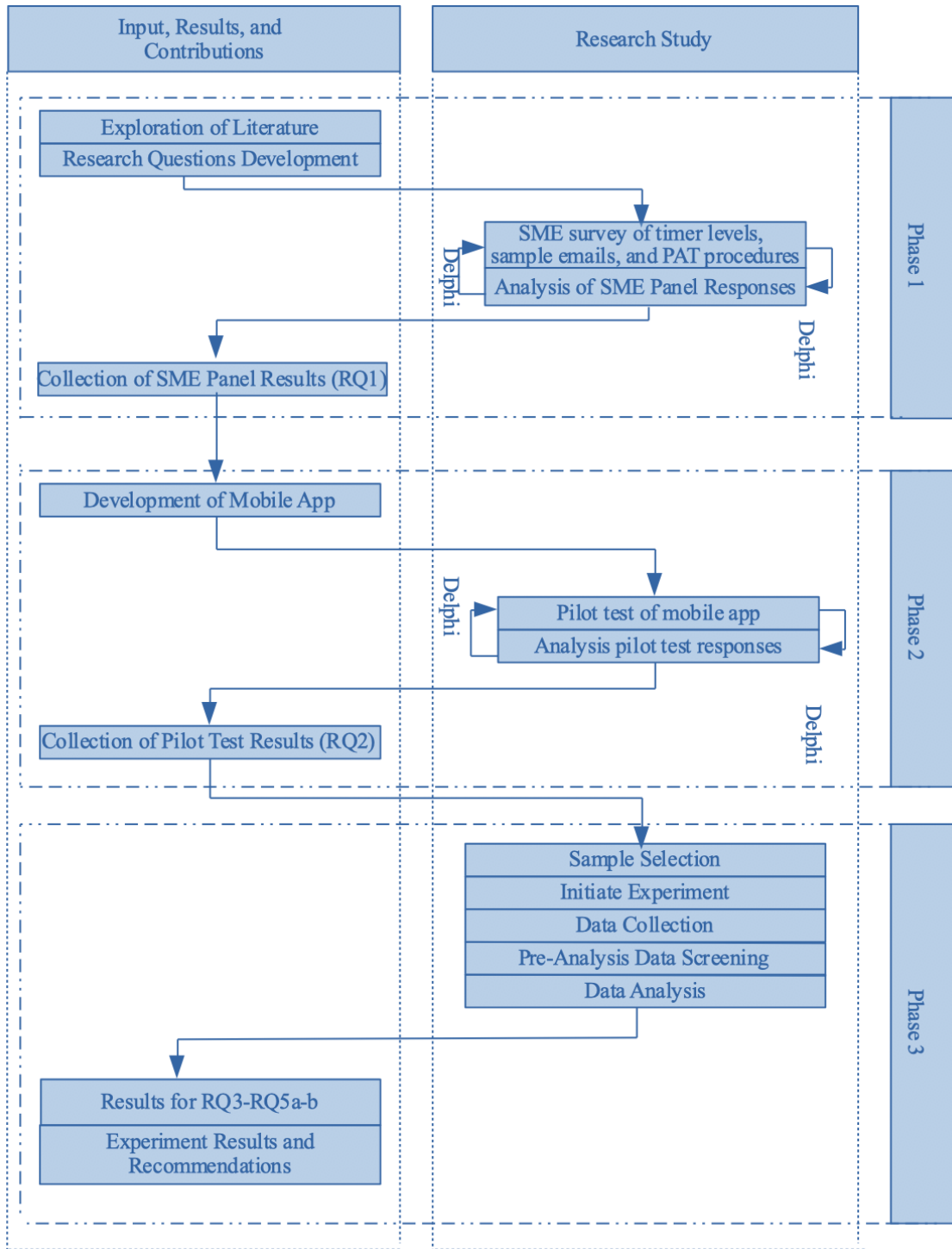
#### **Overview of Research Design**

This research was conducted in three phases as shown in Figure 1. It was hypothesized that PAT would help users to detect phishing by displaying a warning dialog in colored text and with a timer to move them into a more logical thought process. This research design was defined as an experimental field study design. A quantitative approach was used to collect SMEs opinion on the value for the countdown or count-up timer in the warning dialog and on the validity of the sample e-mails, all of which were part of Phase I. PAT was designed and developed during Phase II. A quantitative survey was used to collect SMEs feedback on the functional correctness of PAT. Phase III used a quantitative approach to collect data from participants who used the app.

In Phase I, a quantitative survey was used to collect opinion data from approximately 25 SMEs on which timer value should be used in the countdown and count-up timer and on the validity of the sample e-mails and on the experimental procedures of PAT.

**Figure 1**

*Overview of Research Design Process*



Phase II was a developmental stage in which the mobile app was created and tested by a pilot group of participants. Phase III was the experimental study in which approximately 100 participants used the mobile app to check simulated e-mail as well as interact with simulated phishes and the countdown and count-up timer warning dialog.

A mobile app was created to test the ability of users to avoid phishes when presented with a countdown or count-up timer and colored warning text. The goal of the app was to assist users in overcoming the instinctual reaction that is the hallmark of System One. The app simulated a Gmail inbox and presented a timer when the user was presented with a simulated email that has either a link or an attachment.

The independent variables were the timer type (countdown, count-up, or no timer), the timer value (the three values of which were determined in Phase I), and the text color (grey, red, or black). The dependent variable was the number of times a malicious URL or attachment was clicked. The demographic factors were moderating variables.

### *Phase I*

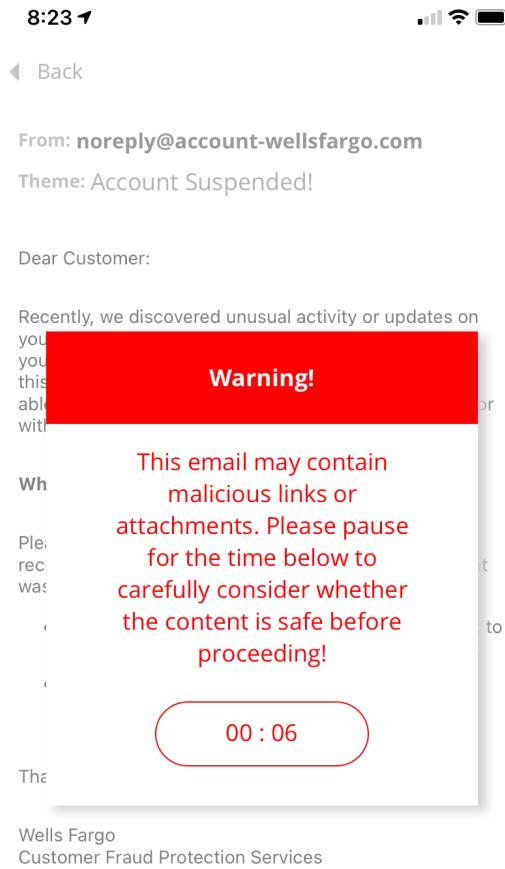
Phase I used a quantitative survey to collect opinions from SMEs. The purpose of the survey was to collect timer values, validate sample emails, and validate the experimental procedures of PAT. The survey had four sections. The first section was a demographic questionnaire to document the expertise of the SMEs. The beginning of the SME demographic survey can be found in Appendix A. The second section provided a mockup of what the timer looks like in the custom app so that the SMEs could visualize the countdown or count-up timer and then asked what the timer value should be. The SMEs were asked to rank the timer values given.

It was necessary to choose valid timer values to increase the validity of the entire study. The third section asked the SMEs to rate thirty sample emails individually. For each sample email, the SMEs were asked to identify the email as phishing or legitimate and whether the email should be kept, adjusted, or replaced. If the SMEs chose the option to adjust or replace, they were asked to specify how (in the case of adjust), or why (in the case of replace). The SMEs were also asked for additional feedback. An example of a sample email question from the SME survey is shown in Appendix B.

The survey was distributed via Google Forms and used the Delphi method (Ramim & Lichvar, 2014) for section two to narrow the timer values to three values. For the second round, the survey was shortened to include only section two. Prior research has utilized the Delphi method to gain a consensus in cybersecurity (Carlton, 2016; Ramim & Lichvar, 2014). The Delphi method uses an iterative feedback loop in which feedback from the last iteration is used to inform the next iteration until a consensus is reached. Kendall's  $W$  values are used to assess agreement among raters (Schmidt, 1997). Schmidt (1997) recommended a threshold of .5 for Kendall's  $W$  values, so this threshold was adopted to determine the timer value to be used in the countdown or count-up timer. Figure 2 through Figure 4 show sections one and two of an example SME survey. Figure 2 shows what the timer dialog looked like which displayed after the introduction section in the SMEs survey. Figure 3 shows the questions in the demographic portion of the SMEs survey, and Figure 4 shows the timer question from the SMEs survey that asked the SMEs to rank the possible timer values. Each SME received an email invitation (Appendix C) to participate in the survey. The results of this survey were used to answer RQ1 and RQ2.

**Figure 2**

*Example of PAT Timer Dialog*





### *Phase II*

Phase II entailed the design, development, and testing of PAT. PAT was created twice, once for Android devices and once for Apple devices. PAT simulates a basic Gmail client that allows the user to check their e-mail. PAT includes a demographic survey that is displayed the first time the app is opened. The demographic survey is embedded in the app. The results from the survey were stored with no PII in a spreadsheet document on the app back-end. When the participant interacted with a simulated e-mail that has a URL or an attachment, the id of that email and whether the user clicked on the URL or the attachment were stored with no PII in a spreadsheet document on the app back-end. The user was assigned a User Identification Number (UIN). A warning and a timer as shown in Figure 2 displayed each time the user receiving the treatment opened a simulated e-mail that contained a URL or attachment. The user was not able to bypass the timer and had to wait until the timer was expired before interacting with the simulated e-mail. Each time the user interacted with a simulated e-mail for which a timer displayed, the id of that e-mail and if the user clicked on the URL was stored.

### *Phase III*

In phase III, approximately 110 participants, who were recruited via Facebook and LinkedIn, were asked to interact with PAT. An example of the recruitment post is in Appendix D, and an example of the participant invitation letter is in Appendix E. Because of a limitation in the PAT app back-end, which is discussed in the limitation section, recruitment happened in phases. First 10 participants were recruited for the pilot study such that Apple and Android users were equally represented. The pilot group was used to

verify the mobile app and data collection. Use of the app was observed, the countdown and count-up timers were manually timed, and data collection was verified. Then 50 participants were recruited for the control group. It was not disclosed to the participants that they were in the control group. When the control group had finished participation, then 50 more participants were recruited for the experimental group.

The participants were asked for feedback regarding the app. The Delphi method was used. The findings and recommendations of the participants in the pilot study were incorporated into the app and the process repeated for a second iteration.

Yan et al. (2015) studied user behavior for one week. Since this study was also analyzing user behavior, participants were asked to use PAT for seven days. Alert Logic (2018) stated that the average user receives 16 malicious emails per month. For this study, simulated emails were randomly assigned to all participants from a pool of all emails stored in the back-end. The pool contained 10 legitimate text-only emails, and five each of the following: legitimate with a link, legitimate with an attachment, phishing with a link, and phishing with an attachment. Each participant received the same simulated emails each day, and each participant received five simulated emails per day. A summary of the types of simulated email that were used is summarized in Table 12.

**Table 12**

*Summary of Simulated Email Types*

Email types	Link	Attachment	Number of Emails in the Sample
Legitimate text-only	No	No	10
Legitimate link	Yes	No	5
Legitimate attachment	No	Yes	5
Phishing link	Yes	No	5
Phishing attachment	No	Yes	5



PAT collected and stored non-PII data from the participants. When participants downloaded PAT, they were given a UIN that was used to link their data to their profile. The participants were asked to take a short survey, which included demographic questions. Participant age, gender, education level, attention span, and the amount of email they receive were stored. The survey also asked whether the participant is completely color-blind (National Eye Institute, 2019). Attention span was measured with an attention span test adopted from Psychology Today (n.d.) which was embedded in the app survey. The results of the demographic survey were used towards answering RQ5a-b. An example of the participant demographic survey is shown in Appendix F. An example of the attention span questions is in Appendix G.

After the participants finished the survey, the participants saw a simulated inbox listing. Participants were able to interact with any e-mail in the simulated inbox as though it were a real e-mail. The app had pre-coded simulated e-mails that displayed in a random order. Some of the simulated e-mails mimicked a legitimate e-mail, and some simulated a phishing, and each simulated e-mail was identified by a unique email number (i.e., ID). New e-mails displayed on each day of the study to simulate receiving new e-mail. Some simulated e-mails had a URL or an attachment, and some did not. If a participant receiving the timer treatment opened an e-mail that has a URL in the body of the message or an attachment, a timer was displayed, and they were not able to interact with the e-mail until the timer expired. When they did interact with the email, the data collected was: (1) the unique email number of the simulated e-mail, and (2) if the participant clicked on the link or attachment. The app also captured and stored whether a countdown, count-up, or no timer was used, the value of the timer used, and whether grey, red, or black text was

used. These data were used towards answering RQ3 through RQ5a-b. The data was stored in a spreadsheet document on the app back-end. No PII was captured or stored. An example of a simulated phishing email with no dialog is in Appendix H. An example of a simulated phishing email with a warning but no timer is in Appendix I, and an example of a phishing email with a warning and a timer is in Appendix J.

### **Instrument and Prototype Development**

#### *Instrument for Collecting SMEs Feedback Regarding Timer Value*

So that a valid timer value could be used in Phases II and III of this research, SMEs were asked in Phase I for a valid timer value using a Google Forms survey. The survey asked the SMEs for demographic information to confirm their expertise, presented a mockup of the timer, asked the SMEs to rank eight timer values. An example of the timer ranking question is in Figure 4. The data was analyzed using Google Form's data analysis tools and Kendall's W values. Kendall's W values measure agreement among survey participants using a least squares solution (Schmidt, 1997). The three values that have the most agreement among the SMEs were used in Phases II and III.

#### *Instrument for Collecting SMEs Feedback Regarding Sample E-Mails*

A quantitative survey was developed to capture the SMEs' feedback regarding what simulated sample e-mails should be used in this study. SMEs were provided with a set of legitimate e-mails and phishes and were asked whether to (1) "Keep", (2) "Adjust", or (3) "Replace" each e-mail. If the SMEs proposed "Adjust" or "Replace", they were asked in to provide feedback on how to adjust or why to replace that e-mail.

### *Instrument for Collecting Pilot Participant Feedback Regarding PAT*

A quantitative survey was developed to capture the SMEs' feedback that included a step-by-step process of what users eventually saw. SMEs were provided with a set of experimental protocols and be asked whether to (1) "Keep", (2) "Adjust", or (3) "Replace" each step of the experiments. If the SMEs proposed "Adjust" or "Replace", they were asked to provide feedback on how to adjust or why to replace that step.

### *Instrument for Collecting Participant Demographic Information*

In Phase III of this study, participants were presented with a demographic survey when they opened the app for the first time. This survey asked participants for their age, gender, education level, attention span, and the volume of email they received in a day. The attention span questions were adopted from the attention span test on Psychology Today (n.d.). The survey also asked whether the participant is completely color-blind (National Eye Institute, 2019). If participants answered that they are completely color-blind, they were excluded from the study.

### *PAT Prototype Development*

Using the data from the SMEs survey in Phase I, PAT, which simulates a Gmail inbox, was developed. PAT has two versions, one for use on Apple devices, and one for use on Android devices. PAT simulates a basic Gmail client and overlays a dialog when the participant opens an email that contains a link or an attachment. The dialog requires participants receiving the treatment to pause by including a countdown or count-up timer, along with a grey or red warning. The experimental group was not able to dismiss the warning dialog until the timer expired. The timer was set to one of three different values. These three values were determined in Phase I of this study. The control group received a

warning in black text with no timer and were able to access email immediately after dismissing the warning dialog. For the control group, dismissing the warning dialog was possible immediately after it appeared.

Requirements for this app were:

1. The first time a user opens PAT, the user is presented with a demographic survey which the user needs to complete before continuing. PAT sends the survey responses to a spreadsheet form in which no PII is collected or stored. Each participant is assigned a UIN.
2. On the primary PAT screen, users are presented with simulated Gmail inbox. Users are able to tap an email listing which opens that email. As the email opens, one of two actions occurs:
  - a. If there is no URL or attachment in the email, the email opens and the user is able to read it
  - b. If there is a URL or attachment in the email, a warning dialog appears with different options for the following variables:
    - i. Warning text color (grey, red, or black)
    - ii. A countdown or count-up timer or no timer
    - iii. In the cases of a countdown or count-up timer, a starting timer value determined from Phase I
3. When the user interacts with either timer, the following data is collected and sent to a spreadsheet form:
  - a. The color of the warning text
  - b. Whether a countdown or count-up timer or no timer was displayed

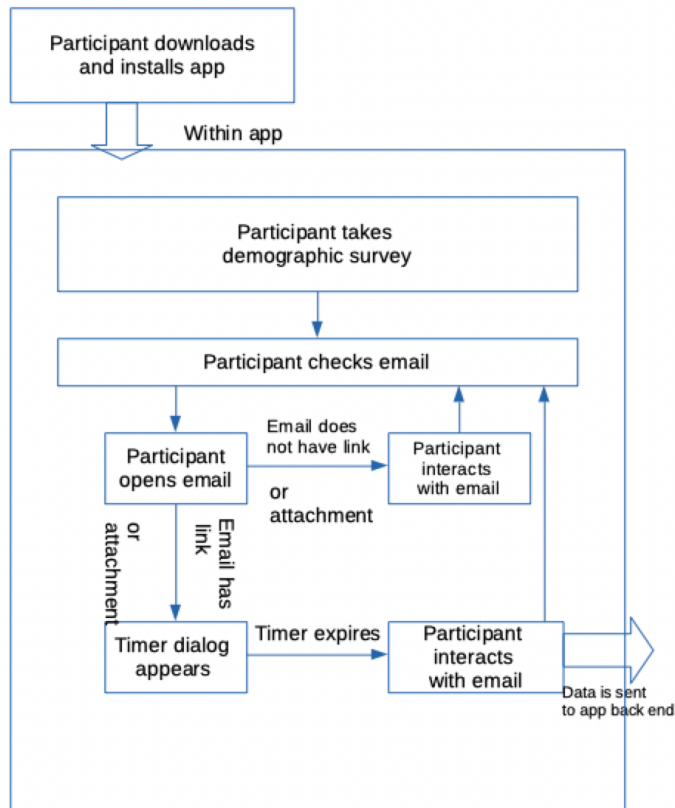
- c. In the case of a countdown or count-up timer, the starting value of the timer
  - d. The unique email number of the simulated e-mail
  - e. Whether or not the user clicked on the URL
4. PAT does not provide any other functionality.

An overview of the PAT functionality is given in Figure 5.

#### *Effectiveness of the PAT Prototype*

The survey in Phase I provided a valid timer value for use in PAT. Phase II included validation testing for PAT which included the functionality of the app and validation of the correct collection of data. It was also confirmed that no PII is collected. In Phase III, there was a pilot study so that any validation or functionality issues regarding PAT could be identified.

This research followed an experimental field study research design which included quantitative measures (Creswell & Creswell, 2018). An experimental field study design is a valid methodology when conducting developmental research (Ivankova et al., 2006). There were three data collection points in this research design. In Phase I, data were collected from a quantitative expert panel survey which asked SMEs to rank timer values. The Delphi method with Kendall's W values was used to find a consensus among the SMEs. Data was collected in Phase I from a quantitative expert panel regarding the validity of the sample e-mails. By receiving SMEs feedback for the timer value and sample e-mails, validity was increased. In Phase II, the sample e-mails were coded to display in a random order.

**Figure 5***Overview of the PAT Process*

The sample emails displayed in a random order increased validity since displaying e-mails in a random order reduced the probability that one particular e-mail influenced participant reaction to another e-mail. The Delphi method was also used in Phase II until the SMEs agreed that PAT was functionally sound, valid, and reliable. In Phase III, quantitative data was collected from participants as they use PAT.

## **Reliability and Validity**

### *Reliability*

Reliability is the measure of how consistent experimental results are as time passes (Sekaran & Bougie, 2016). A study is considered reliable if the same input consistently produces the same output (Ellis & Levy, 2009). Stability reliability refers to how an instrument produces output over a period of time (Ellis & Levy, 2009; Sekaran & Bougie, 2016). PAT was tested for stability reliability using the Delphi method in Phase II. Parallel-form reliability refers to when two sets of measures on the same instrument are highly correlated (Sekaran & Bougie, 2016). PAT was tested for parallel-form reliability in Phase III since there was a pilot test.

### *Validity*

Sekaran and Bougie (2016) stated that there are two kinds of validity—external and internal. External validity refers to how confident the researchers are that results of their study are generalizable to other settings, people, and events (Sekaran & Bougie, 2016). Internal validity refers to how much confidence there is in an instrument that it measures what it is intended to measure (Sekaran & Bougie, 2016). Since this research was a field experiment, it was expected that the external validity would be high (Sekaran & Bougie, 2016). This study addressed internal validity by using the Delphi method with Kendall's W values to gain a consensus for a timer value in Phase I, by testing PAT functionality in Phase II, and by running a pre-test in Phase III. External validity was addressed by the simulation of an existing e-mail service and by asking the participants to check e-mail as they normally would. Straub (1989) discussed the importance of instrument validation. By testing the completeness and correctness of the mobile app designed and created for

this study, the instrument validity of PAT was addressed. Threats to validity that may have affected this study were testing effects and selection bias effects. Testing effects refer to the participant's awareness of being observed influencing their action (Sekaran & Bougie, 2016). Since this study was a closed-lab experiment, participant knowledge that this investigation was examining user actions when encountering a phish may have made participants hyper-vigilant when using the app (Finn & Jakobsson, 2007). Participants were asked to use the app as normally as they can and to imagine that they were checking e-mail as they would normally. Selection bias effects refer to how participants are selected for this study (Sekaran & Bougie, 2016). Since participants were chosen by convenience sampling through Facebook and LinkedIn rather than by simple random sampling, selection bias may have affected the results.

### **Sample**

The sample was chosen by convenience sampling from LinkedIn and Facebook. A targeted message with an invitation to participant was posted on Facebook and LinkedIn. Users of these websites who are directly connected to the researcher were requested to share the invitation through the website. Stokes et al. (2019) used Facebook and LinkedIn to recruit nurses and received response rates of 25% and 5% respectively. While LinkedIn had a significantly lower response rate, Stokes et al. (2019) found that the socioeconomic differences between participants from LinkedIn and Facebook to be significant. Therefore, both social media platforms were used in an attempt to receive more variety in the sample.

Sekaran and Bougie (2016) stated that, for each sample that is broken into subsamples, a minimum of 30 participants for each category is recommended. Given that



the timer values Independent Variable (IV) has three categories, the target sample size was 100 participants. Carlton (2016) invited 975 individuals and collected 245 responses generating response rate of 25.1%. Ball (2012) surveyed 2380 individuals and collected 396 responses generating a response rate of 16%. Therefore, the anticipated response rate was approximately 20% and at least 500 individuals were invited to participate in this study.

### **Pre-analysis Data Screening**

According to Mertler and Vannatta (2010), there are four primary reasons for screening data: (1) data accuracy, (2) assessing incomplete data, (3) assessing extreme values (outliers), and (4) assessing the relationship between the data and assumptions made.

With regard to assessing incomplete data, all fields in the participant survey were required, so there was no incomplete data. Any participants that indicated that they are completely colorblind were excluded. In addition, PAT was checked for correctness, and all participants received at least four phishing emails through the PAT through random simulated email assignment. Mahalanobis Distance was used to determine which data are outliers (Mertler & Vannatta, 2010). The data collected were screened using Mahalanobis Distance to find outliers and the outliers were evaluated for removal from further analysis.

## **Data Analysis**

In Phase I, an expert panel and the Delphi method with Kendall's W values were used to identify and validate the three separate levels to be used in the countdown and count-up timers. This process was used to answer RQ1. In addition, the Delphi method was used to assess the functional correctness and validity of PAT. A pilot study of 10 participants used the app. Any feedback that affected the function or validity of PAT was fixed before the next cycle. This process was used to answer RQ2.

The data collected in Phase II were analyzed using factorial ANOVA and factorial ANCOVA. Factorial ANOVA is used to test for significant differences between two or more IVs as well as any significant interaction between those two IVs (Mertler & Vannatta, 2010). Factorial ANOVA was used to answer RQ3 and RQ4. In RQ3, the IVs were the text color and the timer value. In RQ4, the IVs were the timer type and the timer value. The DV for both RQ3 and RQ4 were the number of times a malicious URL was clicked.

While factorial ANOVA is used to study only the effect of the IVs on the DV, factorial ANCOVA is used to study the effects of covariate variables that may affect the relationship between the IVs and the DV (Mertler & Vannatta, 2010). These covariate variables are often environmental or describe human characteristics. Therefore, factorial ANCOVA was used to answer RQ5a-b, which considered the effect demographic variables (age, gender, education level, attention span, and volume of email). A data collection detail summary is in Appendix M. Table 13 summarizes the research phases.

**Table 13***Summary of Research Phases*

Research Question	Phase	Sample	Methodology	Analysis
RQ1	Phase I	25 SMEs	Delphi	Consensus via means and Kendall's W analysis
RQ2	Phase I	25 SMEs	Delphi	Consensus via means and Kendall's W analysis
RQ3	Phase III	100 users	Quantitative survey	ANOVA
RQ4	Phase III	100 users	Quantitative survey	ANOVA
RQ5a-RQ5b	Phase III	100 users	Quantitative survey	ANCOVA

**Resources**

Before this research study could begin, permission was obtained from Nova Southeastern University's Institutional Research Board (IRB). LinkedIn (<https://www.linkedin.com>) was used to find SMEs willing to participate in Phase I of this study. Google Forms (<https://docs.google.com/forms/u/0/>) was used to develop the surveys for Phase I and for the participant demographic survey. The development of PAT was conducted. In Phase III, the data that were collected by the mobile app were stored in an Excel spreadsheet document which was downloaded from the app back-end.

**Summary**

The overall research methodology was presented in this chapter. An experimental field study research design using quantitative measures was used to validate, test, collect, and analyze research data. The goal of this research was to answer the following research questions:

The main research question that this study addressed was: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values presented with a countdown or count-up timer with a red or grey warning message?

RQ1: What are the three timer values to require the user to pause that should be used in this experimental field study to assess users' ability to identify malicious links in e-mail according to cybersecurity SMEs?

RQ2: What level of functional correctness and validity of the custom-designed mobile app is sufficient according to cybersecurity SMEs?

RQ3: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black text?

RQ4: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer?

RQ5a: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black text based

on the categories of: (a) age, (b) gender, (c) education level, (d) the volume of email the user receives in a day, and (e) attention span?

RQ5b: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer based on the categories of: (a) age, (b) gender, (c) education level, (d) the volume of email the user receives in a day, and (e) attention span?

The RQs were addressed over three phases. Phase I collected feedback from a SME expert panel survey regarding the value to use in the countdown and count-up timer. Phase II encompassed the design, development, and testing of PAT. Phase III was a field study in which 100 participants used the app to simulate checking a Gmail account. When the participants first opened the app, they were asked to take a demographic survey. The app overlaid a warning dialog whenever the participant encountered an email with a link or attachment. When the participant interacted with an email that has a link or attachment, the unique email number of the simulated email and whether the participant clicked on the link was stored.

## Chapter 4

### Results

#### **Overview**

This chapter presents the results of the data collection and analysis from this research study. The main goal was to determine whether requiring e-mail users to pause by displaying a colored warning (grey, red, or black text) with a timer (countdown, count-up, or no counter) when they are presented with a potentially malicious link has any effect on the percentage of users falling to phishing attempts. For Phase I, 257 SMEs participated by completing the SMEs survey and a Delphi methodology was used, which resulted in two rounds to reach consensus. The SMEs validated the three timer values to use, the sample emails to use, and the experimental process used in the PAT mobile app. Phase II used the results from Phase I and consisted of the PAT app development. Phase III included a pilot test with 10 testers, in which PAT was adjusted based on the results, and the main data collection utilizing 106 participants. SPSS version 26 was used to calculate ANOVA and ANCOVA which were used to analyze the data collected in Phase III.

#### **Phase I – SMEs Survey Feedback and Findings**

RQ1 was answered using the findings from the SMEs survey. An invitation was posted on Facebook and LinkedIn requesting participation from cybersecurity experts and an encouragement to share the post. The result was that 257 responses were collected. However, many of these responses appeared to be invalid, and 214 responses were

excluded for a remaining total of 42 responses. Determining validity was based on responses in the email validation section. If a participant selected adjust or replace and did not provide comments as to how or why for more than half of the emails, their results were excluded from the study. Table 14 provides descriptive statistics of the 42 SMEs. The SMEs included network security or cybersecurity engineers (16.67%), cybersecurity analysts (35.71%), information security managers (11.90%), information technology auditors (7.14%), a cybersecurity administrator (2.38%), cybersecurity consultants (9.52%), and cybersecurity architects (16.67%). The years of experience held by the SMEs were between one and three years (30.95%), between three and five years (33.33%), between five and ten years (19.05%), and more than ten years (16.67%). No SMEs had less than one year of experience. The number of certifications held by the SMEs included no certifications (9.52%), one certification (42.86%), two certifications (33.33%), three certifications (9.52%), and four or more certifications (4.76%).

**Table 14**

*Summary of SME Demographics (N = 42)*

Demographic Item	N	%
<b>Current Position</b>		
Network Security or Cybersecurity Engineer	7	16.67%
Cybersecurity Analyst	15	35.71%
Information Security Manager	5	11.90%
Information Technology Auditor	3	7.14%
Cybersecurity Administrator	1	2.38%
Cybersecurity Consultant	4	9.52%
Cybersecurity Architect	7	16.67%

**Table 14***Summary of SME Demographics (N = 42) – (continued)*

Demographic Item	N	%
Experience in Cybersecurity		
Less than one year	0	0.00%
At least one year, but less than 3 years	13	30.95%
At least three years, but less than 5 years	14	33.33%
At least 5 years, but less than 10 years	8	19.05%
10 years or more	7	16.67%
Number of Cybersecurity Certifications		
None	4	9.52%
One	18	42.86%
Two	14	33.33%
Three	4	9.52%
Four or More	2	4.76%
Highest level of Education Completed		
High School Diploma	0	0.00%
2-Year College (Associates degree)	2	4.76%
4-Year College (Bachelor's degree)	26	61.90%
Graduate degree	8	19.05%
Doctorate/Professional	6	14.29%
Age		
18-19	0	0.00%
20-29	17	40.48%
30-39	15	35.71%
40-49	6	14.29%
50-59	4	9.52%
over 60	0	0.00%



Phase I addressed RQ1: What are the three timer values to require the user to pause that should be used in this experimental field study to assess users' ability to identify malicious links in e-mail according to cybersecurity SMEs? This research question was answered with data from the Timer Survey section of the SME survey and a two-round Delphi process. When selecting their first choice for timer value, 15 SMEs (35.71%) chose 1-second, two SMEs (4.76%) chose 3-seconds, four SMEs (9.52%) chose 5-seconds, four SMEs (9.52%) chose 7-seconds, three SMEs (7.14%) chose 10-seconds, three SMEs (7.14%) chose 20-seconds, and eight SMEs (19.05%) chose 30-seconds. When selecting their second choice for timer value, two SMEs (4.76%) chose 1-second, 14 SMEs (33.33%) chose 3-seconds, three SMEs (7.15%) chose 5-seconds, one SME (2.38%) chose 7-seconds, seven SMEs (16.67%) chose 10-seconds, eight SMEs (19.05%) chose 20-seconds, and no SMEs (0%) chose 30-seconds. When selecting their third choice for timer value, one SME (2.38%) chose 1-second, five SMEs (11.90%) chose 3-seconds, 11 SMEs (26.19%) chose 5-seconds, nine SMEs (21.43%) chose 7-seconds, two SMEs (4.76%) chose 10-seconds, two SMEs (4.76%) chose 20-seconds, and three SMEs (7.14%) chose 30-seconds. The first-round data was summarized and given to six SMEs to gain a consensus of the final three values to use. A summary of the first-round SME timer value selections is shown in Table 15.

**Table 15***Summary of SME Timer Value Selections (N = 42)*

Timer value	N	%	Timer value	N	%
First Choice			Second Choice		
1-second	15	35.71%	1-second	2	4.76%
3-seconds	2	4.76%	3-seconds	14	33.33%
5-seconds	4	9.52%	5-seconds	3	7.14%
7-seconds	4	9.52%	7-seconds	1	2.38%
10-seconds	3	7.14%	10-seconds	7	16.67%
20-seconds	3	7.14%	20-seconds	8	19.05%
30-seconds	8	19.05%	30-seconds	0	0.00%
Third Choice			Fourth Choice		
1-second	1	2.38%	1-second	2	4.76%
3-seconds	5	11.90%	3-seconds	1	2.38%
5-seconds	11	26.19%	5-seconds	5	11.90%
7-seconds	9	21.43%	7-seconds	10	23.81%
10-seconds	2	4.76%	10-seconds	12	28.57%
20-seconds	2	4.76%	20-seconds	4	9.52%
30-seconds	3	7.14%	30-seconds	4	9.52%
Fifth Choice			Sixth Choice		
1-second	1	2.38%	1-second	4	9.52%
3-seconds	3	7.14%	3-seconds	2	4.76%
5-seconds	2	4.76%	5-seconds	13	30.95%
7-seconds	14	33.33%	7-seconds	2	4.76%
10-seconds	9	21.43%	10-seconds	3	7.14%
20-seconds	2	4.76%	20-seconds	1	2.38%
30-seconds	4	9.52%	30-seconds	7	16.67%
Seventh Choice			Eighth Choice		
1-second	1	2.38%	1-second	16	38.06%
3-seconds	13	30.95%	3-seconds	2	4.76%
5-seconds	3	7.14%	5-seconds	1	2.38%
7-seconds	1	2.38%	7-seconds	1	2.38%
10-seconds	1	2.38%	10-seconds	5	11.90%
20-seconds	20	47.62%	20-seconds	2	4.76%
30-seconds	1	2.38%	30-seconds	15	35.71%

*Phase I – RQ2*

Phase I also addressed RQ2: What level of functional correctness and validity of the custom-designed mobile app is sufficient according to cybersecurity SMEs? This research question was answered with the Verification of Sample Emails and the Mobile App Experimental Procedure sections of the SME survey. In the Verification of Sample Emails section, of 10 sample phishing emails, the majority of SMEs correctly identified only one phishing sample email as phishing. Many of the phishing sample emails were adjusted or replaced based on SME quantitative feedback. Of 20 legitimate sample emails, most SMEs correctly identified 14 legitimate sample emails as legitimate. The majority of SMEs recommended keeping all sample emails. The Verification of Sample Emails data is summarized in Table 16.

**Table 16**

*Summary of Verification of Sample Emails Data (N = 42)*

Sample Email	N	%	Sample Email	N	%
Email 1: Legitimate URL			Email 2: Legitimate URL		
Phishing	11	26.19%	Phishing	17	40.48%
Legitimate	27	64.29%	Legitimate	20	47.62%
Unsure	4	9.52%	Unsure	5	11.90%
Email 1: Validation			Email 2: Validation		
Keep	40	95.24%	Keep	39	92.86%
Adjust	1	2.38%	Adjust	3	7.14%
Replace	1	2.38%	Replace	0	0.00%
Email 3: Legitimate text only			Email 4: Phishing attachment		
Phishing	14	33.33%	Phishing	17	40.48%
Legitimate	25	59.52%	Legitimate	21	50.00%
Unsure	3	7.14%	Unsure	4	9.52%
Email 3: Validation			Email 4: Validation		
Keep	39	92.86%	Keep	42	100.00%
Adjust	2	4.76%	Adjust	0	0.00%
Replace	1	2.38%	Replace	0	0.00%

**Table 16***Summary of Verification of Sample Email Data (N = 42) – (continued)*

Sample Email	N	%	Sample Email	N	%
Email 5: Legitimate URL			Email 6: Legitimate URL		
Phishing	11	26.19%	Phishing	15	35.71%
Legitimate	21	50.00%	Legitimate	25	59.52%
Unsure	10	23.81%	Unsure	2	4.76%
Email 5: Validation			Email 6: Validation		
Keep	41	97.62%	Keep	41	97.62%
Adjust	1	2.38%	Adjust	1	2.38%
Replace	0	0.00%	Replace	0	0.00%
Email 7: Legitimate URL			Email 8: Phishing attachment		
Phishing	5	11.90%	Phishing	19	45.24%
Legitimate	32	76.19%	Legitimate	21	50.00%
Unsure	5	11.90%	Unsure	2	4.76%
Email 7: Validation			Email 8: Validation		
Keep	36	85.71%	Keep	38	90.48%
Adjust	5	11.90%	Adjust	3	7.14%
Replace	1	2.38%	Replace	1	2.38%
Email 9: Phishing URL			Email 10: Legitimate URL		
Phishing	19	45.24%	Phishing	10	23.81%
Legitimate	19	45.24%	Legitimate	29	69.05%
Unsure	4	9.52%	Unsure	3	7.14%
Email 9: Validation			Email 10: Validation		
Keep	36	85.71%	Keep	37	88.10%
Adjust	5	11.90%	Adjust	3	7.14%
Replace	1	2.38%	Replace	2	4.76%
Email 11: Phishing attachment			Email 12: Phishing attachment		
Phishing	17	40.48%	Phishing	18	42.86%
Legitimate	22	52.38%	Legitimate	21	50.00%
Unsure	3	7.14%	Unsure	3	7.14%
Email 11: Validation			Email 12: Validation		
Keep	36	85.71%	Keep	37	88.10%
Adjust	4	9.52%	Adjust	3	7.14%
Replace	2	4.76%	Replace	2	4.76%

**Table 16***Summary of Verification of Sample Email Data (N = 42) – (continued)*

Sample Email	N	%	Sample Email	N	%
Email 13: Phishing URL			Email 14: Legitimate text only		
Phishing	12	28.57%	Phishing	12	28.57%
Legitimate	28	66.67%	Legitimate	26	61.90%
Unsure	2	4.76%	Unsure	4	9.52%
Email 13: Validation			Email 14: Validation		
Keep	37	88.10%	Keep	33	78.57%
Adjust	5	11.90%	Adjust	6	14.29%
Replace	0	0.00%	Replace	3	7.14%
Email 15: Phishing URL			Email 16: Legitimate text only		
Phishing	17	40.48%	Phishing	6	14.29%
Legitimate	9	21.43%	Legitimate	32	76.19%
Unsure	6	14.29%	Unsure	4	9.52%
Email 15: Validation			Email 16: Validation		
Keep	35	83.33%	Keep	34	80.95%
Adjust	7	16.67%	Adjust	6	14.29%
Replace	0	0.00%	Replace	2	4.76%
Email 17: Legitimate text only			Email 18: Phishing URL		
Phishing	15	35.71%	Phishing	18	42.86%
Legitimate	25	59.52%	Legitimate	22	52.38%
Unsure	2	4.76%	Unsure	2	4.76%
Email 17: Validation			Email 18: Validation		
Keep	38	90.48%	Keep	37	88.10%
Adjust	4	9.52%	Adjust	4	9.52%
Replace	0	0.00%	Replace	1	2.38%
Email 19: Legitimate text only			Email 20: Legitimate URL		
Phishing	16	38.10%	Phishing	17	40.48%
Legitimate	21	50.00%	Legitimate	24	57.14%
Unsure	5	11.90%	Unsure	1	2.38%
Email 19: Validation			Email 20: Validation		
Keep	36	85.71%	Keep	34	80.95%
Adjust	6	14.29%	Adjust	4	9.52%
Replace	0	0.00%	Replace	0	0.00%

**Table 16***Summary of Verification of Sample Email Data (N = 42) – (continued)*

Sample Email	N	%	Sample Email	N	%
Email 21: Legitimate text only			Email 22: Legitimate attachment		
Phishing	18	42.86%	Phishing	17	40.48%
Legitimate	19	45.24%	Legitimate	21	50.00%
Unsure	5	11.90%	Unsure	4	9.52%
Email 21: Validation			Email 22: Validation		
Keep	34	80.95%	Keep	37	88.10%
Adjust	7	16.67%	Adjust	5	11.90%
Replace	1	2.38%	Replace	0	0.00%
Email 23: Legitimate URL			Email 24: Phishing attachment		
Phishing	19	45.24%	Phishing	12	28.57%
Legitimate	19	45.24%	Legitimate	26	61.90%
Unsure	4	9.52%	Unsure	4	9.52%
Email 23: Validation			Email 24: Validation		
Keep	38	90.48%	Keep	41	97.62%
Adjust	3	7.14%	Adjust	0	0.00%
Replace	1	2.38%	Replace	1	2.38%
Email 25: Legitimate attachment			Email 26: Legitimate attachment		
Phishing	12	28.57%	Phishing	10	23.81%
Legitimate	25	59.52%	Legitimate	31	73.81%
Unsure	5	11.90%	Unsure	1	2.38%
Email 25: Validation			Email 26: Validation		
Keep	37	88.10%	Keep	39	92.86%
Adjust	4	9.52%	Adjust	2	4.76%
Replace	1	2.38%	Replace	1	2.38%
Email 27: Legitimate URL			Email 28: Phishing URL		
Phishing	10	23.81%	Phishing	14	33.33%
Legitimate	29	69.05%	Legitimate	27	64.29%
Unsure	3	7.14%	Unsure	1	2.38%
Email 27: Validation			Email 28: Validation		
Keep	35	83.33%	Keep	38	90.48%
Adjust	5	11.90%	Adjust	3	7.14%
Replace	2	4.76%	Replace	1	2.38%

**Table 16**

*Summary of Verification of Sample Email Data (N = 42) – (continued)*

Sample Email	N	%	Sample Email	N	%
Email 29: Legitimate URL			Email 30: Legitimate text only		
Phishing	14	33.33%	Phishing	6	14.29%
Legitimate	23	54.76%	Legitimate	29	69.05%
Unsure	5	11.90%	Unsure	7	16.67%
Email 29: Validation			Email 30: Validation		
Keep	35	83.33%	Keep	38	90.48%
Adjust	6	14.29%	Adjust	4	9.52%
Replace	1	2.38%	Replace	0	0.00%

In the Mobile App Experimental Procedure section of the SME survey, SMEs were asked whether major components of the PAT process should be kept, adjusted, or removed. The majority of SMEs recommended keep for all of the components of PAT. A summary of data for the Mobile App Experimental Procedure section is in Table 17.

**Table 17**

*Summary of Mobile App Experimental Procedure Validation (N = 42)*

Question	N	%	Question	N	%
1. Pilot Experimental Procedure: Post invitation on Facebook and Linked In			2. Pilot Experimental Procedure: When a potential pilot participant expresses interest, send a welcome email with directions to download PAT along with steps to take to test the app.		
Keep	38	90.48%	Keep	38	90.48%
Adjust	4	9.52%	Adjust	4	9.52%
Remove	0	0.00%	Remove	0	0.00%

**Table 17**

*Summary of Mobile App Experimental Procedure Validation (N = 42) – (continued)*

Question	N	%	Question	N	%
3. Pilot Experimental Procedure: The pilot participants will be asked to fill out a Google survey with the results of their test. They will be directed to email the researcher if they encounter issues not covered on the survey.			4. Pilot Experimental Procedure: If issues not covered on the survey are encountered, the pilot participant will be asked to meet the researcher over Zoom so that the researcher can understand the issue		
Keep	37	88.10%	Keep	36	85.71%
Adjust	5	11.90%	Adjust	4	9.52%
Remove	0	0.00%	Remove	2	4.76%
5. Main Experimental Procedures: Post invitation on Facebook and Linked In.			6. Main Experimental Procedures: When a potential participant expresses interest, send a welcome email to them that includes directions to download and install PAT.		
Keep	39	92.86%	Keep	36	85.71%
Adjust	3	7.14%	Adjust	6	14.29%
Remove	0	0.00%	Remove	0	0.00%
7. Main Experimental Procedures: When a participant first uses the app, the variable values for timer value, timer type (countdown/count-up) and text color (red/grey/black) will be randomly assigned and used for the duration of that participant's participation in the study.			8. Main Experimental Procedures: The participant will be asked to create an account. After the account is created, the participant will receive a notification reminder each morning until the app is uninstalled to interact with PAT. While the participant's email address will be captured, the email address will be paired with an arbitrarily assigned participant id which will be used later to identify that participant's data.		
Keep	37	88.10%	Keep	34	80.95%
Adjust	4	9.52%	Adjust	6	14.29%
Remove	1	2.38%	Remove	2	4.76%



**Table 17***Summary of Mobile App Experimental Procedure Validation (N = 42) – (continued)*

Question	N	%	Question	N	%
9. Main Experimental Procedures: Upon opening the app for the first time and after account creation, the participant will be asked to complete the demographic survey within the app (data from this step will be sent to a Google spreadsheet doc).			10. Main Experimental Procedures: Each time the participant interacts with an email, if the email has a link or an attachment, the following data will be sent to a Google form: text color, timer type, timer value, sample email id, participant id, and whether or not participant followed the link or attachment.		
Keep	37	88.10%	Keep	39	92.86%
Adjust	5	11.90%	Adjust	3	7.14%
Remove	0	0.00%	Remove	0	0.00%

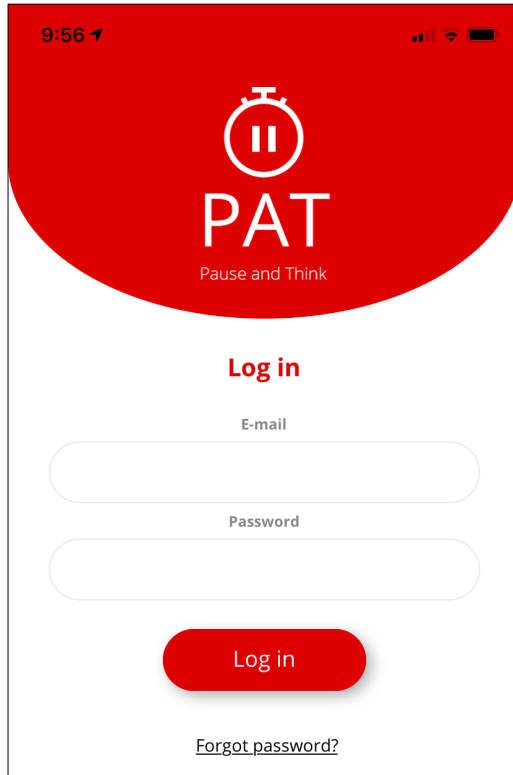
**Phase II – PAT Mobile App Development**

Phase II consisted of the development of PAT. The development of PAT used SME feedback on timer value, sample email verification, and the mobile app experimental procedures. PAT was tested and deployed to both the Apple Store and Google Play. Development of the app included two-factor authentication to ensure participant validity and uniqueness. The PAT login screen is shown in Figure 6.

After the participants registered and logged in for the first time, they were asked demographic questions that included, age, gender, education level, volume of email, and a set of five questions designed to capture the value of the participant's attention span. The demographic survey was reviewed by the NSU IRB before it was presented to participants.

**Figure 6**

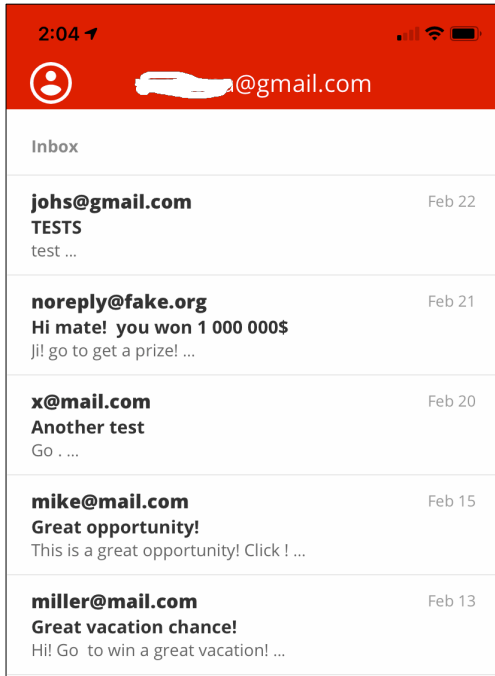
*PAT Mobile App – Login Screen Example*



When the participant logged in at least one day after registering, a simulated inbox was displayed as shown in Figure 7. Simulated emails were coded based on SMEs feedback in Phase I. When a participant in the experimental group tapped on an email with a link or attachment, the simulated email opened and a timer dialog was displayed, as shown in Figure 8. After the timer dialog self-dismissed, if the participant tapped on the link, an acknowledgement of the tap was displayed, as shown in Figure 9.

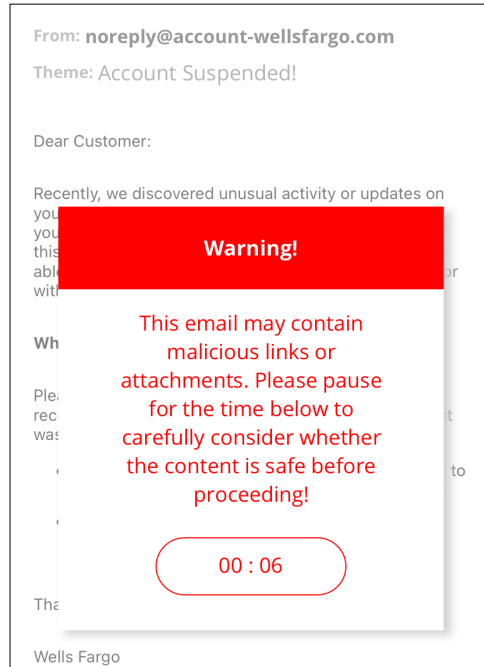
**Figure 7**

*PAT Simulated Inbox*



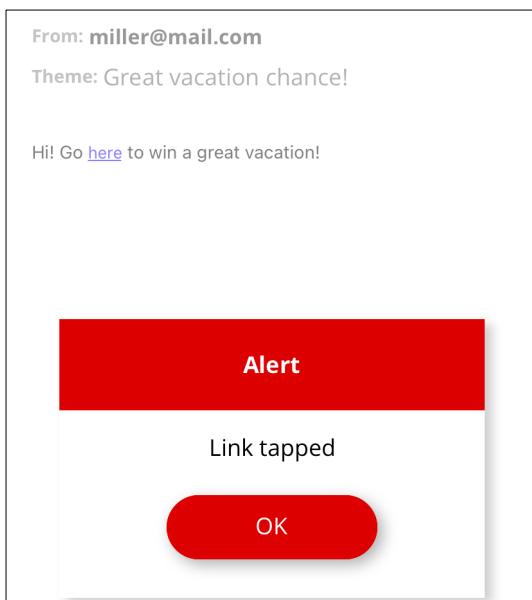
**Figure 8**

*PAT Simulated Email with Timer*



**Figure 9**

*PAT Action After Link Tapped*



### **Phase III – PAT Mobile App Delivery**

Phase III involved participant download, installation, and use of PAT. Data collection occurred between April 5, 2021, and April 28, 2021. The participants were recruited through Facebook and LinkedIn. A total of 117 participants downloaded the PAT mobile app and participated in the study.

#### *Phase III – Pilot Testing*

Of the 117 participants who participated, 10 were pilot testers. Five each of the pilot testers were Apple and Android users. Each tester was given a list of actions to take with the app. Each tester met with the researcher in person or online and the researcher watched the tester use the app. Minor issues were found and fixed.

#### *Phase III – Pre-Analysis Data Screening*

Other than the pilot testers, 107 users participated in the study. One user indicated that they were completely color blind. The results from that user were excluded from the study. The total remaining number of participants was 106. Any email interaction records that indicated that the participant did not open the email were excluded from the study. The number of email interactions collected was 3,746 (106 participants interacting with five emails per day for seven days on average). The data were filtered to include only email interactions with the simulated phishing emails for a remaining total of 1,796 email interactions. The data were screened using Mahalanobis Distance, and, using a p value of .001, no record was found to be a multivariate outlier.

*Phase III – Participant Demographic Characteristics*

The 106 participants included several demographic characteristics. Demographic information is shown in Table 18. Of device types, 63 (58.33%) used Apple and 43 (39.81%) used Android.

**Table 18**

*Descriptive Statistics of Study Participants (N = 106)*

Demographic Item	N	%
Apple or Android		
Apple	62	58.49%
Android	44	41.51%
Age		
18 - 25	1	0.94%
26-35	13	12.26%
36-45	28	26.42%
46-55	40	37.74%
56-65	18	16.98%
66-75	5	4.72%
older than 75	1	0.94%
Gender		
Female	70	66.04%
Male	36	33.96%
Education Level		
Below High School	0	0.00%
High School	2	1.89%
Some Higher-Education Credits	11	10.38%
Associate's Degree	6	5.66%
Bachelor's Degree	27	25.47%
Master's Degree	41	38.68%
Doctorate Degree or comparable	19	17.92%
Volume of Email Received		
1-10 emails per day	8	7.55%
11-30 emails per day	32	30.19%
31-60 emails per day	27	25.47%
61-90 emails per day	19	17.92%
91-120 emails per day	8	7.55%
121-150 emails per day	5	4.72%
More than 150 emails per day	7	6.60%

**Table 18***Descriptive Statistics of Study Participants (N = 106) – continued*

Demographic Item	N	%
Attention Span		
Very low attention span	5	4.72%
Low attention span	15	14.15%
Somewhat low attention span	21	19.81%
Average attention span	26	24.53%
Somewhat high attention span	19	17.92%
High attention span	15	14.15%
Very high attention span	5	4.72%

Of the participant ages, one was 18-19 (0.93%), 13 were 26-35 (12.04%), 28 were 36-45 (25.93%), 40 were 46-55 (37.04%), 18 were 56-65 (16.67%), five were 66-75 (4.63%), and one was over 75 (0.93%). Of participant genders, 70 were female (64.81%) and 36 were male (33.33%). Of education level, no participants had a Below High School education and two (1.85%) had a High School education. Eleven (10.19%) participants had Some Higher Education Credits, six (5.56%) had an Associate Degree, 27 (25.00%) had a Bachelor's Degree, 41 (37.96%) had a Master's Degree, and 19 (17.59%) had a Doctorate Degree or comparable. Of volume of email, eight (7.41%) had 1-10 emails per day, 32 (29.63%) had 11-30 emails per day, 27 (25.00%) had 31-60 emails per day, 19 (17.59%) had 61-90 emails per day, eight (7.41%) had 91-120 emails per day, five (4.63%) had 121-150 emails per day, and seven (6.48%) had more than 150 emails per day. Attention span was aggregated from the five attention span demographic survey questions so that a lower score means a lower attention span. The first four attention span questions were negatively worded using a score of (1) for 'Very untrue of me' to (7) for 'Untrue of me'. The fifth attention span question was positively worded using a score of

(7) for ‘Very untrue of me’ to (1) for ‘Untrue of me’. Each question was scored and added so that the minimum score was five, meaning that the participant scored the lowest attention span choice in each of the five questions. The maximum score was 33, which means that the highest-scoring participant scored two fewer than the possible maximum of 35 (five questions times a score of seven per question). The range of scores was then grouped so that scores of five through eight were coded as Very low attention span, scores of nine through 12 were coded as Low attention span, scores of 13 through 16 were scored as Somewhat low attention span, scores of 17 through 20 were scored as Average attention span, scores of 21 through 24 were scored as Somewhat high attention span, scores of 25 through 28 were scored as High attention span, and scores of 29 through 33 were scored as Very high attention span. The attention span grouping is summarized in Table 19.

**Table 19**

*Attention Span Grouping Summary*

Score group	Coding
5-8	Very low attention span
9-12	Low attention span
13-16	Somewhat low attention span
17-20	Average attention span
21-24	Somewhat high attention span
25-28	High attention span
29-33	Very high attention span

*Phase III – RQ3*

Phase III addressed RQ3: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed

with a warning in (a) grey, (b) red, or (c) black text? To answer RQ3, 3,746 email interactions were collected (106 participants interacting with 5 emails per day for 7 days on average). The data were filtered to include only email interactions with the simulated phishing emails for a remaining total of 1,796 email interactions. ANOVA was used to test for significant differences between groups. The results of the ANOVA showed there were significant differences among all groups for Text Color, Timer Value, and Text Color x Timer Value. The F-value for Text Color was 20.852 and had a significance of  $p < .001$ . The F-value for Timer Value was 3.700 and had a significance of  $p < .05$ . The F-value for Text Color x Timer Value was 2.899 and had a significance of  $p < .01$ . The results of the ANOVA to answer RQ3 are shown in Table 20.

**Table 20**

*ANOVA Results of Difference in Text Color and Timer Value in Email Interactions*

*(N=1796)*

Source	Sum of Squares	Df	Mean Square	F	Sig.
Between Treatments	11.787	11	1.072	7.385	.000***
Text Color	6.051	2	3.025	20.852	.000***
Timer Value	1.611	3	.537	3.700	.011*
Text Color x Timer Value	2.524	6	.421	2.899	.008**
Within Treatments	258.841	1784	.145		
Total	6188.000	1796			

\*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

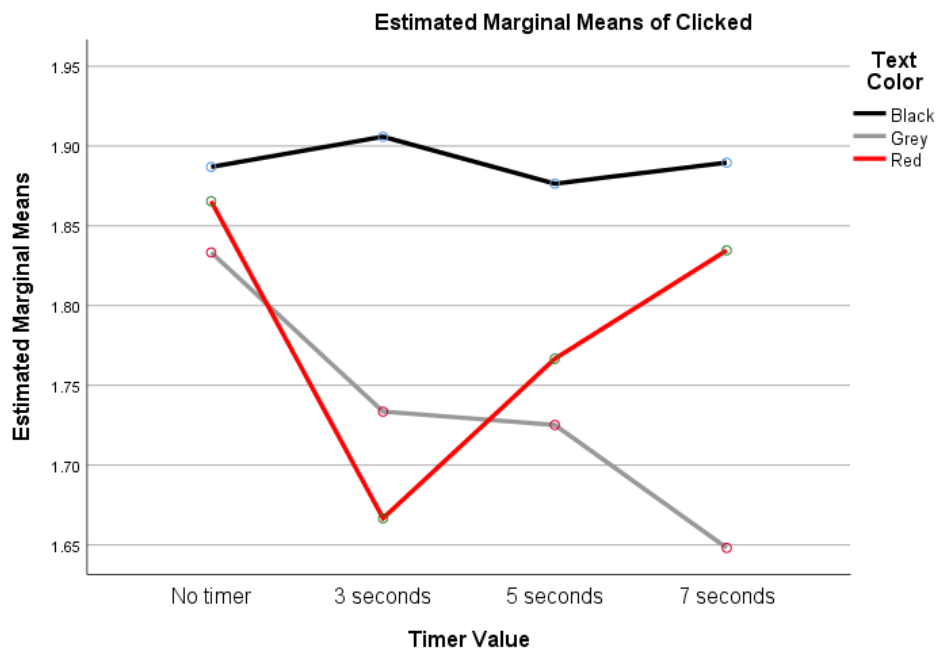
The profile plot of Text Color x Timer Value is shown in Figure 10. The value of the Estimated Marginal Means of Clicked range from one, meaning Not Clicked, to two, meaning Clicked. The black line indicates the mean click rate for email interactions that included a dialog box in black text. Likewise, the grey line represents the mean click rate for email interactions that included a dialog box in grey text, and the red line indicates the



mean click rate that included a dialog box in red text. The profile plot indicates that grey and red text performed better overall than black text, meaning that the user was less likely to click on a malicious link if the text color was in grey or red. The profile plot shows that the best combination of text color and timer value was grey text at 7-seconds. This combination had the lowest click mean at 1.65. The second-best combination was red text at 3-seconds. The click mean for this combination was approximately 1.67.

**Figure 10**

*Profile Plot of Text Color x Timer Value*



*Phase III – RQ4*

Phase III addressed RQ4: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer? To answer RQ4, the data

were filtered to include only email interactions with the simulated phishing emails.

ANOVA was used to test for significant differences between groups. The results of the ANOVA showed there were significant differences only in the Timer Type x Timer Value group. The F-value for Timer Type x Timer Value was  $p < .05$ . The results of the ANOVA to answer RQ4 are shown in Table 21.

**Table 21**

*ANOVA Results of Difference in Timer Type and Timer Value in Email Interactions*

*(N=1796)*

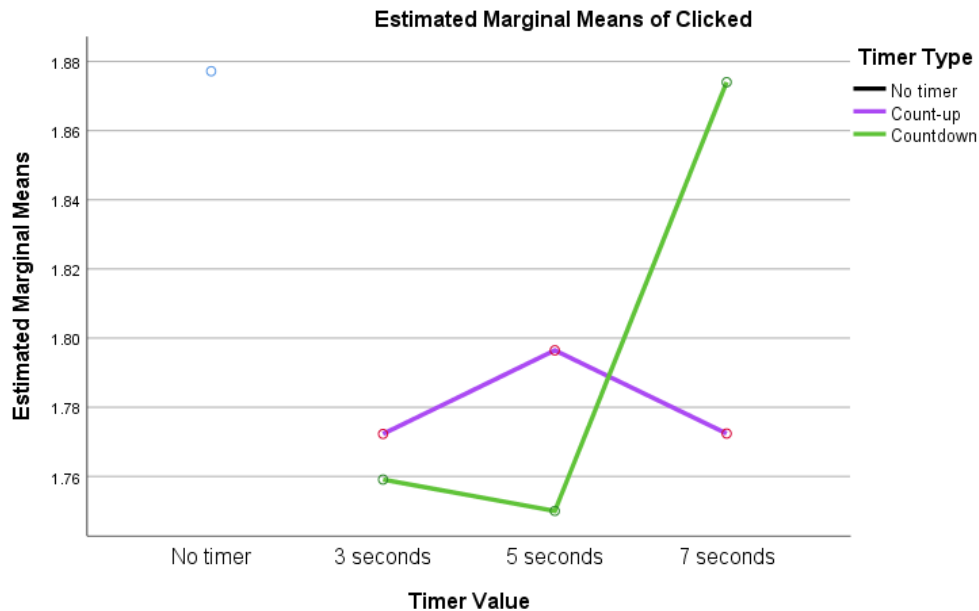
Source	Sum of Squares	Df	Mean Square	F	Sig.
Between Treatments	5.172	6	.862	5.810	<b>.000***</b>
Timer Type	.049	1	.049	.328	.567
Timer Value	.655	2	.327	2.207	.110
Timer Type x Timer Value	1.039	2	.520	3.501	<b>.030*</b>
Within Treatments	265.456	1789	.148		
Total	6188.000	1796			

\*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

The profile plot for Timer Type x Timer Value is shown in Figure 11. No timer is represented by only a dot because there was no timer value for dialogs with no timer. The worst combinations of Timer Type and Timer Value were no timer and no time and a countdown timer at 7-seconds, both at a mean click rate of approximately 1.88. The best combination of Timer Type and Timer Value was a timer counting down for 5-seconds at a mean click rate of approximately 1.75.

**Figure 11**

*Profile Plot of Timer Type x Timer Value*



### *Phase III – RQ5a*

Phase III addressed RQ5a: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black text based on the categories of: (a) age, (b) gender, (c) education level, (d) the volume of email the user receives in a day, and (e) attention span? To answer RQ5a, the data were filtered to include only email interactions with the simulated phishing emails. ANCOVA was used to test for significant differences between groups with each demographic indicator as a covariate. The results of ANCOVA using all five demographic indicators (age, gender, education level, email volume, and attention span) showed significance. When age was used as a covariate, the F-value for Text Color was  $p < .001$  and the F-value for Text Color x

Timer Value was  $p < .05$ . When gender was used as a covariate, the F-value for Text Color was  $p < .001$ , the F-value for Timer Value was  $p < .05$ , and the F-value for Text Color x Timer Value was  $p < .01$ . When education level was used as a covariate, the F-value for Text Color was  $p < .001$ , the F-value for Timer Value was  $p < .01$ , and the F-value for Text Color x Timer Value was  $p < .05$ . When email volume was used as a covariate, the F-value for Text Color was  $p < .001$ , the F-value for Timer Value was  $p < .05$ , and the F-value for Text Color x Timer Value was  $p < .01$ . When attention span was used as a covariate, the F-value for Text Color was  $p < .001$ , the F-value for Timer Value was  $p < .05$ , and the F-value for Text Color x Timer Value was  $p < .01$ . The results of the ANCOVA answering RQ5a are shown in Table 22.

**Table 22**

*ANCOVA Results of Difference in and Text Color and Timer Value in Email Interactions*  
( $N=1796$ )

Source	Sum of Squares	Df	Mean Square	F	Sig.
<b>Age</b>	.135	1	.135	.931	.335
Between Treatments	11.922	12	.994	6.847	<b>.000***</b>
Text Color	5.770	2	2.885	19.884	<b>.000***</b>
Timer Value	.135	1	.135	.931	.335
Text Color x Timer Value	2.428	6	.405	2.789	<b>.011*</b>
Within Treatments	258.706	1783	.145		
Total	6188.000	1796			

\*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

**Table 22***ANCOVA Results of Difference in and Text Color and Timer Value in Email Interactions**(N=1796) –continued*

Source	Sum of Squares	Df	Mean Square	F	Sig.
<b>Gender</b>	.027	1	.027	.185	.667
Between Treatments	11.814	12	.985	6.782	.000***
Text Color	6.050	2	3.025	20.841	.000***
Timer Value	1.613	3	.538	3.703	.011*
Text Color x Timer Value	2.545	6	.424	2.923	.008**
Within Treatments	258.814	1783	.145		
Total	6188.000	1796			
<b>Education Level</b>	2.093	1	2.093	14.533	.000***
Between Treatments	13.880	12	1.157	8.032	.000***
Text Color	6.101	2	3.051	21.185	.000***
Timer Value	1.810	3	.603	4.191	.006**
Text Color x Timer Value	2.257	6	.376	2.612	.016*
Within Treatments	256.748	1783	.144		
Total	6188.000	1796			
<b>Email Volume</b>	.960	1	.960	6.641	.010*
Between Treatments	12.748	12	1.062	7.345	.000***
Text Color	6.074	2	3.037	20.998	.000***
Timer Value	1.607	3	.536	3.705	.011*
Text Color x Timer Value	2.547	6	.424	2.935	.007**
Within Treatments	257.880	1783	.145		
Total	6188.000	1796			

\*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

**Table 22***ANCOVA Results of Difference in and Text Color and Timer Value in Email Interactions**(N=1796) –continued*

Source	Sum of Squares	Df	Mean Square	F	Sig.
Attention Span	.023	1	.023	.160	.690
Between Treatments	11.810	12	.984	6.780	.000***
Text Color	6.042	2	3.021	20.813	.000***
Timer Value	1.626	3	.542	3.733	.011*
Text Color x Timer Value	2.523	6	.421	2.897	.008**
Within Treatments	258.818	1783	.145		
Total	6188.000	1796			

\*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$ 

Profile plots of Text Color x Timer Value with each covariate were performed and appear in Figures 12 through 16. Figure 12 shows the profile plot of Text Color x Timer Value with age as a covariate. Figure 13 shows the profile plot of Text Color x Timer Value with gender as a covariate. Figure 14 shows the profile plot of Text Color x Timer Value with education level as a covariate. Figure 15 shows the profile plot of Text Color x Timer Value with email volume as a covariate. Figure 16 shows the profile plot of Text Color x Timer Value with attention span as a covariate.

Figure 12

*Profile Plot of Text Color x Timer Value with Age as a Covariate*

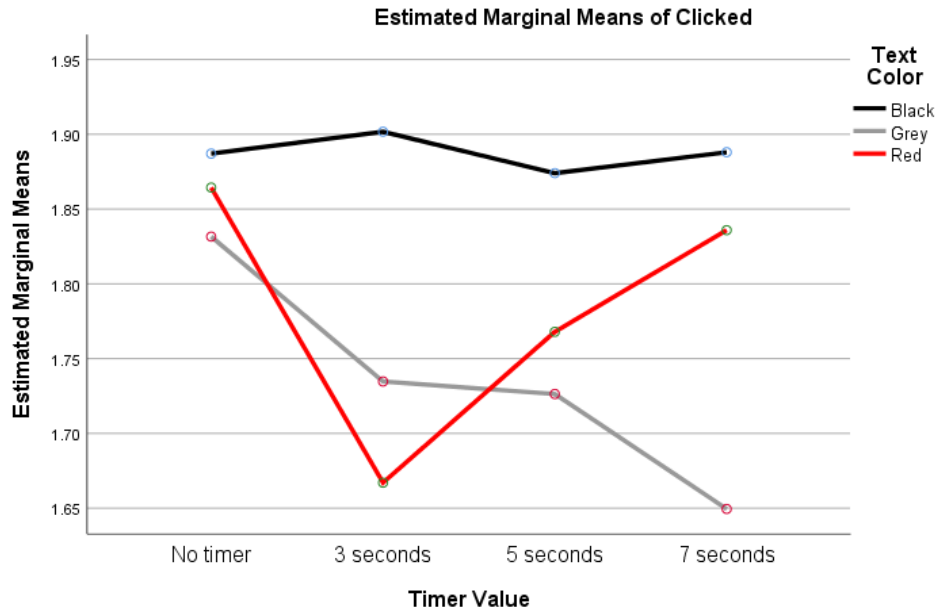
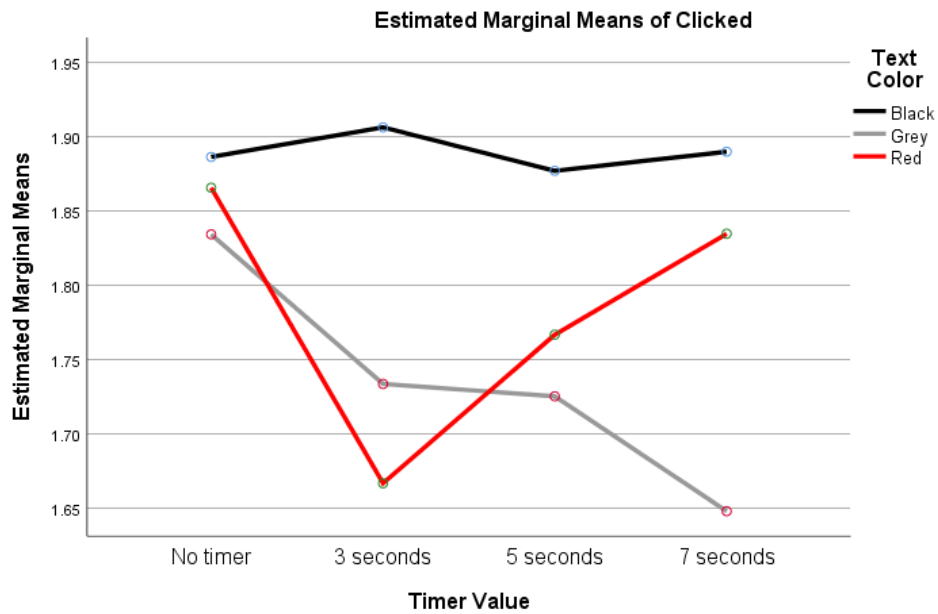


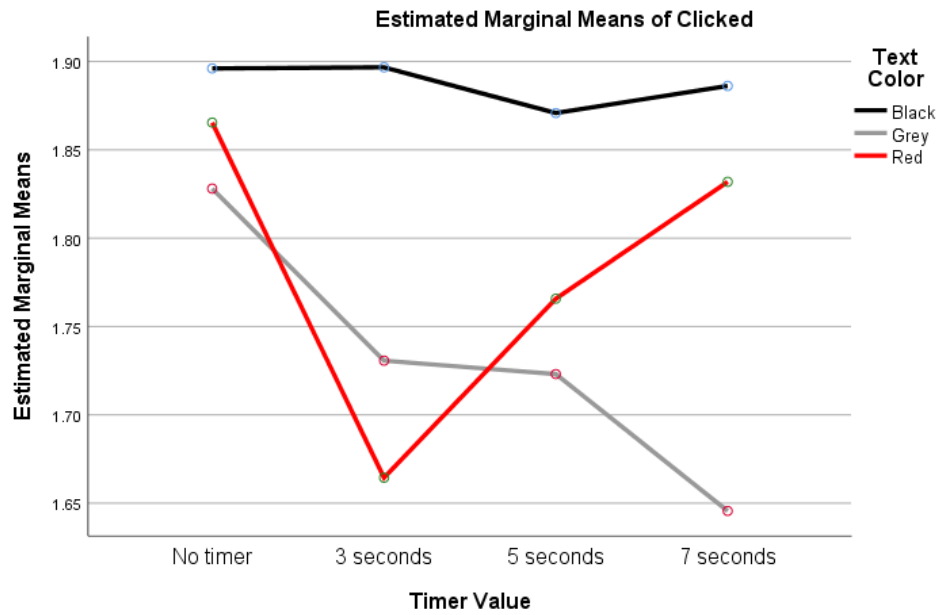
Figure 13

*Profile Plot of Text Color x Timer Value with Gender as a Covariate*

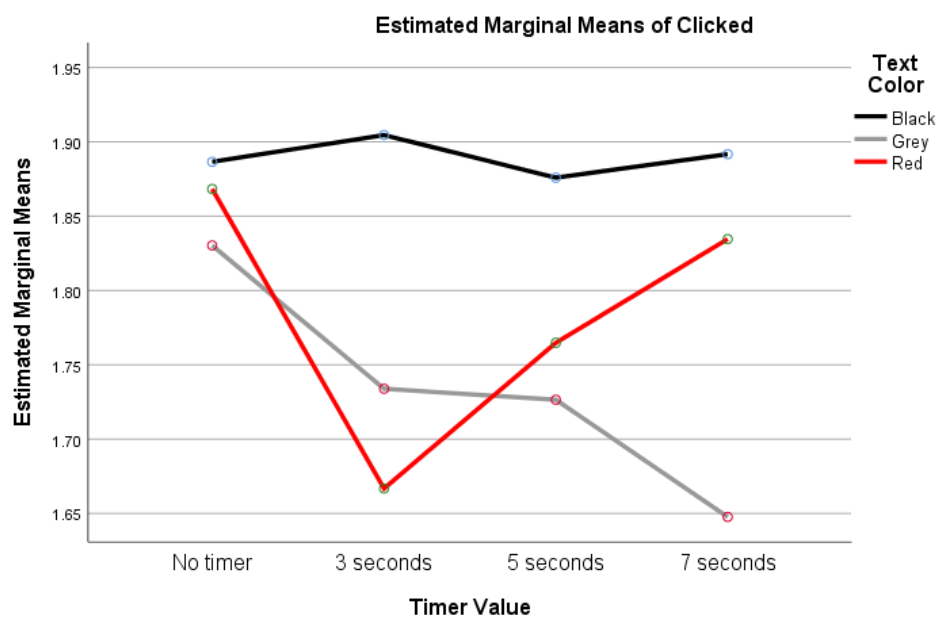


**Figure 14**

*Profile Plot of Text Color x Timer Value with Education Level as a Covariate*

**Figure 15**

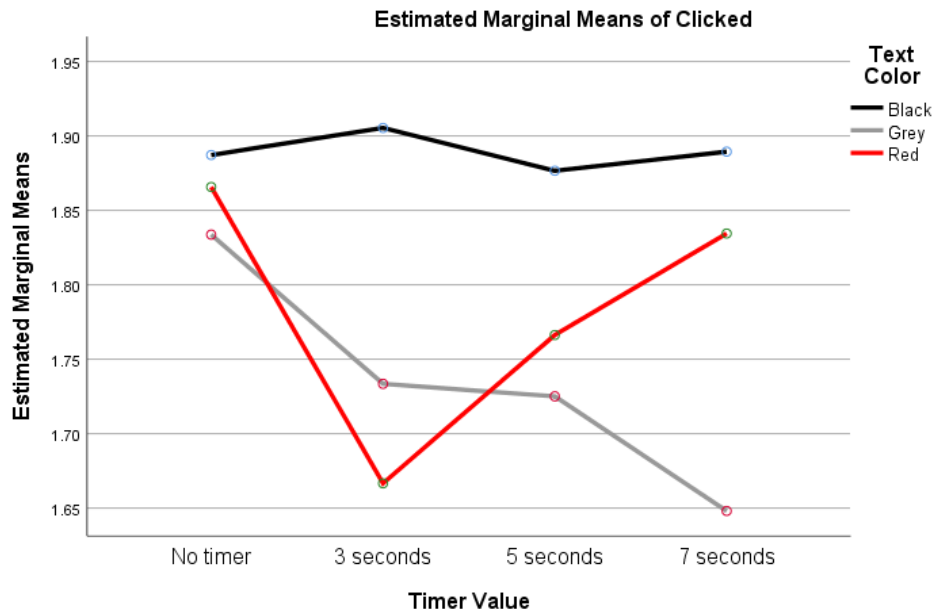
*Profile Plot of Text Color x Timer Value with Email Volume as a Covariate*





**Figure 16**

*Profile Plot of Text Color x Timer Value with Attention Span as a Covariate*



### *Phase III – RQ5b*

Phase III addressed RQ5b: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer based on the categories of: (a) age, (b) gender, (c) education level, (d) the volume of email the user receives in a day, and (e) attention span? To answer RQ5b, the data were filtered to include only email interactions with the simulated phishing emails. ANCOVA was used to test for significant differences between groups with each demographic indicator as a covariate. The results of ANCOVA using all five demographic indicators (age, gender, education level, email volume, and attention span) showed significance. F-value for

Timer Type x Timer Value was  $p < .05$  for all demographic factors. The results of the ANCOVA answering RQ5a are shown in Table 23.

**Table 23**

*ANCOVA Results of Difference in Timer Type and Timer Value in Email Interactions*

*(N=1796)*

Source	Sum of Squares	Df	Mean Square	F	Sig.
<b>Age</b>	0.469	1	0.469	3.162	0.076
Between Treatments	5.641	7	0.806	5.437	<b>.000***</b>
Timer Type	0.035	1	0.035	0.234	0.629
Timer Value	0.642	2	0.321	2.167	0.115
Timer Type x Timer Value	1.04	2	0.52	3.51	<b>.030*</b>
Within Treatments	264.987	1788	0.148		
Total	6188	1796			
<b>Gender</b>	0.011	1	0.011	0.075	0.784
Between Treatments	5.183	7	0.74	4.988	<b>.000***</b>
Timer Type	0.049	1	0.049	0.333	0.564
Timer Value	0.654	2	0.327	2.204	0.111
Timer Type x Timer Value	1.04	2	0.52	3.502	<b>.030*</b>
Within Treatments	265.445	1788	0.148		
<b>Education Level</b>	2.178	1	2.178	14.79	<b>.000***</b>
Between Treatments	7.35	7	1.05	7.131	<b>.000***</b>
Timer Type	0.033	1	0.033	0.226	0.634
Timer Value	0.652	2	0.326	2.213	0.11
Timer Type x Timer Value	1.027	2	0.513	3.486	<b>.031*</b>
Within Treatments	263.278	1788	0.147		
Total	6188	1796			

\*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

**Table 23***ANCOVA Results of Difference in Timer Type and Timer Value in Email Interactions**(N=1796) – (continued)*

Source	Sum of Squares	Df	Mean Square	F	Sig.
<b>Email Volume</b>	0.939	1	0.939	6.348	<b>.012*</b>
Between Treatments	6.111	7	0.873	5.901	<b>.000***</b>
Timer Type	0.048	1	0.048	0.327	0.567
Timer Value	0.679	2	0.339	2.294	0.101
Timer Type x Timer Value	1.041	2	0.52	3.517	<b>.030*</b>
Within Treatments	264.517	1788	0.148		
Total	6188	1796			
<b>Attention Span</b>	0.032	1	0.032	0.214	0.644
Between Treatments	5.204	7	0.743	5.008	<b>.000***</b>
Timer Type	0.049	1	0.049	0.327	0.567
Timer Value	0.654	2	0.327	2.204	0.111
Timer Type x Timer Value	1.036	2	0.518	3.491	<b>.031*</b>
Within Treatments	265.424	1788	0.148		
Total	6188	1796			

\*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$ 

Profile plots of Timer Type x Timer Value with each covariate were performed and appear in Figures 17 through 21. Figure 17 shows the profile plot of Timer Type x Timer Value with age as a covariate. Figure 18 shows the profile plot of Timer Type x Timer Value with gender as a covariate. Figure 19 shows the profile plot of Timer Type x Timer Value with education level as a covariate. Figure 20 shows the profile plot of Timer Type x Timer Value with email volume as a covariate. Figure 21 shows the profile plot of Timer Type x Timer Value with attention span as a covariate.

Figure 17

*Profile Plot of Timer Type x Timer Value with Age as a Covariate*

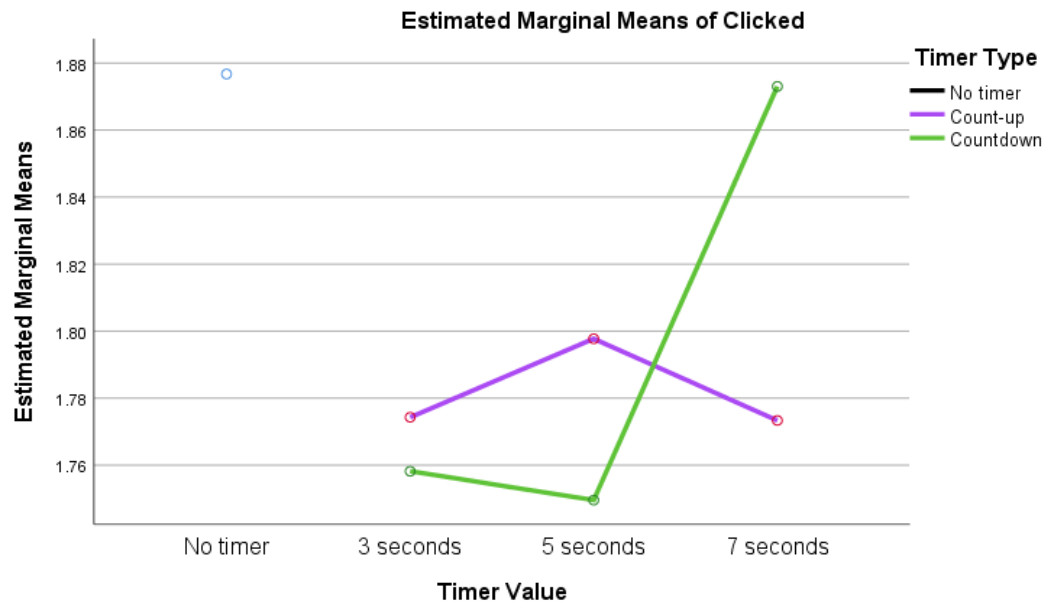


Figure 18

*Profile Plot of Timer Type x Timer Value with Gender as a Covariate*

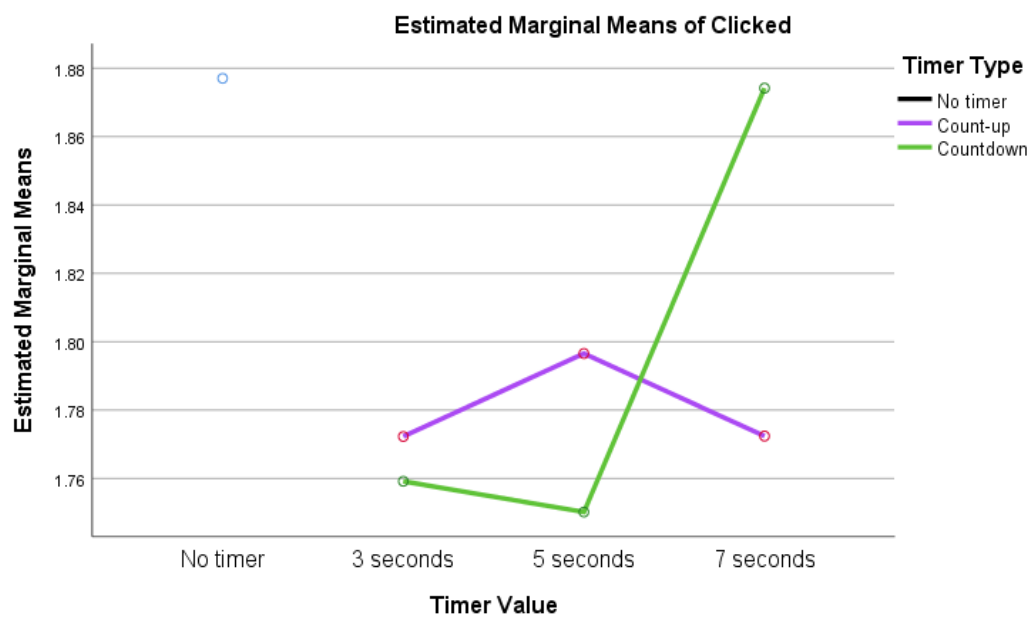


Figure 19

Profile Plot of Timer Type x Timer Value with Education Level as a Covariate

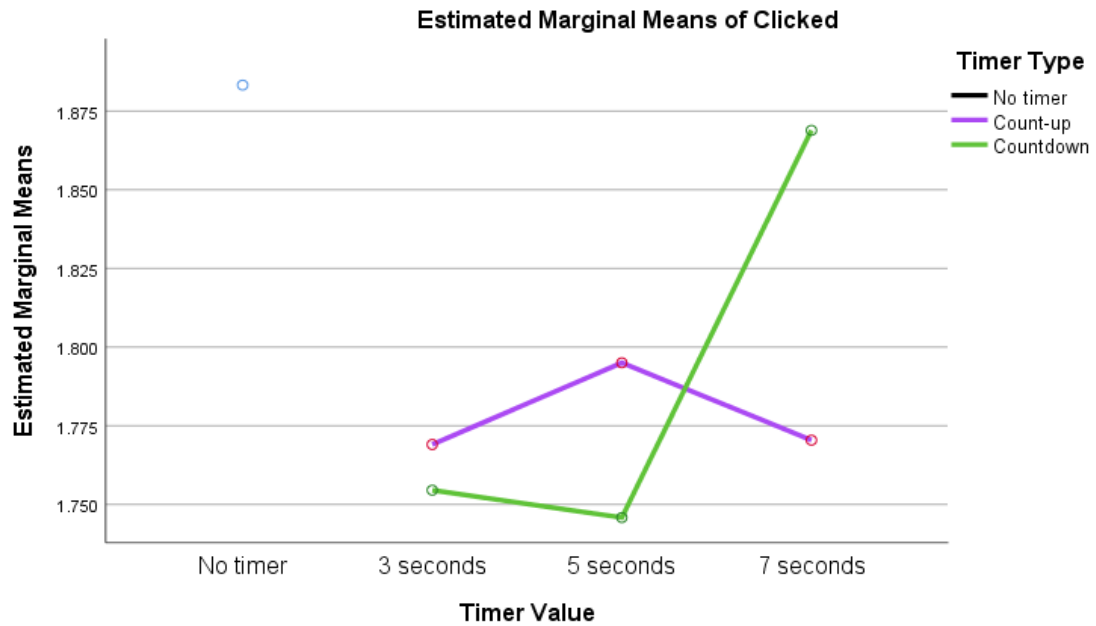
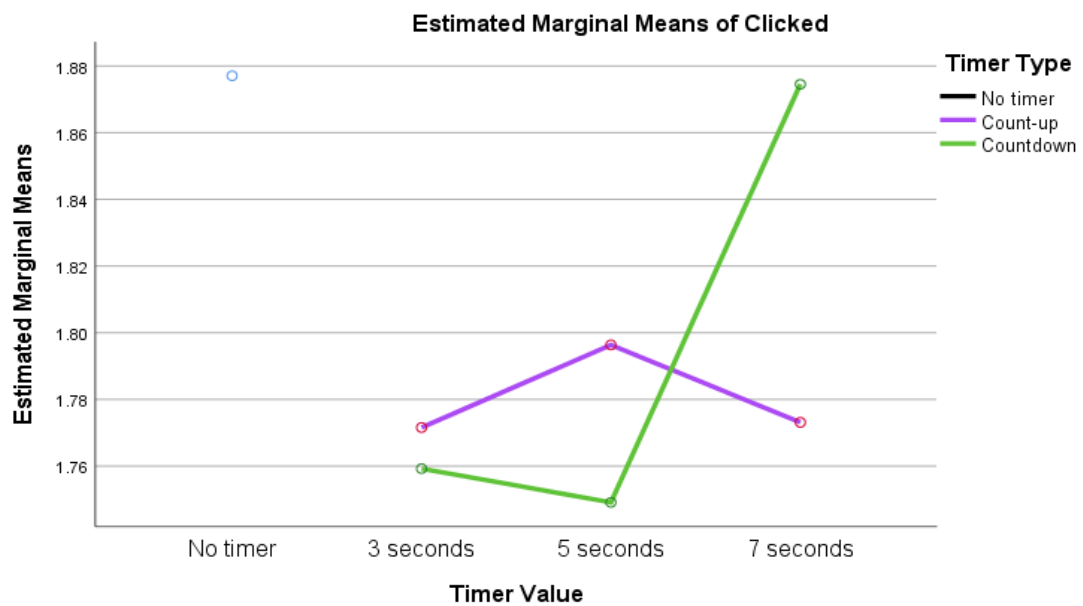


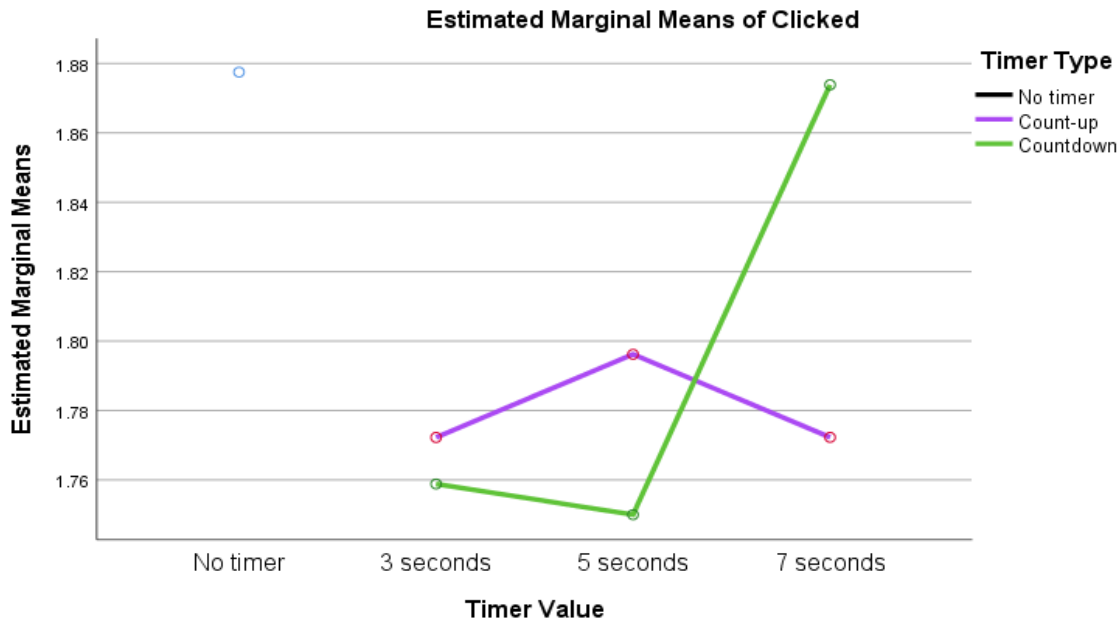
Figure 20

Profile Plot of Timer Type x Timer Value with Email Volume as a Covariate



**Figure 21**

*Profile Plot of Timer Type x Timer Value with Attention Span as a Covariate*



*Phase III – RQ5 – Age Group*

The age demographic was analyzed using the click mean and standard deviation of all the email interactions with the simulated phishing emails. A summary of this data is shown in Table 24 and displayed in Figure 22. The age demographic that performed the best (had the lowest click mean) was 18-25. The age demographic that appeared to perform the worst was Older than 75, although only one participant was in that demographic, so generalization is difficult.

*Phase III – RQ5 – Gender Group*

The gender demographic was analyzed using the click mean and standard deviation of all the email interactions with the simulated phishing emails. A summary of this data is shown in Table 25 and displayed in Figure 23. The click mean for both genders was very

similar, indicating that gender may not be a factor in ability to avoid clicking a malicious link or attachment.

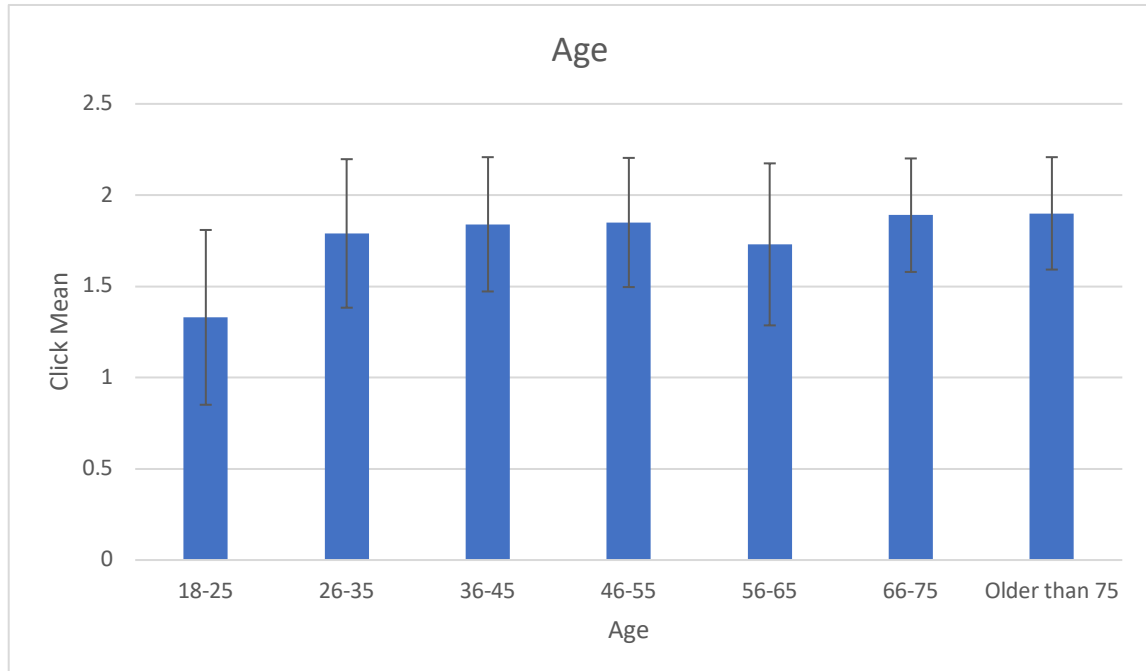
**Table 24**

*Summary of Age Demographic with Respect to Click Mean*

	Click Mean	Std Dev
18-25	1.33	0.479
26-35	1.79	0.407
36-45	1.84	0.368
46-55	1.85	0.354
56-65	1.73	0.444
66-75	1.89	0.311
Older than 75	1.9	0.308

**Figure 22**

*Summary of Age Demographic with Respect to Click Mean*



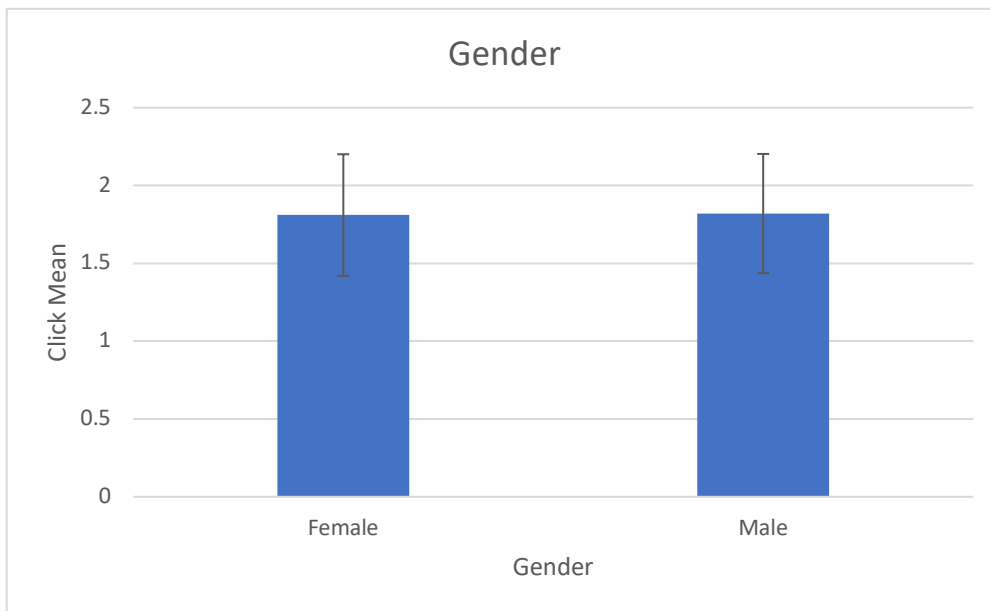
**Table 25**

*Summary of Gender Demographic with Respect to Click Mean*

	Click Mean	Std Dev
Female	1.81	0.391
Male	1.82	0.383

**Figure 23**

*Summary of Gender Demographic with Respect to Click Mean*



### *Phase III – RQ5 – Education Level Group*

The education level demographic was analyzed using the click mean and standard deviation of all the email interactions with the simulated phishing emails. A summary of this data is shown in Table 26 and displayed in Figure 24. The Associates degree demographic performed the worst at a click mean of 1.94, and the High school demographic performed the best at 1.48. This indicates that a higher level of education may not mitigate the user's ability to avoid clicking on a malicious link or attachment.



*Phase III – RQ5 – Volume of Email Group*

The volume of email demographic was analyzed using the click mean and standard deviation of all the email interactions with the simulated phishing emails. A summary of this data is shown in Table 27 and displayed in Figure 25. The 1-10 emails per day demographic performed the best at a click mean of 1.68, and the 121-150 emails per day demographic performed the worst at a click mean of 1.97. This indicates that fewer emails per day help the user to avoid clicking on a malicious email or attachment.

**Table 26**

*Summary of Education Level Demographic with Respect to Click Mean*

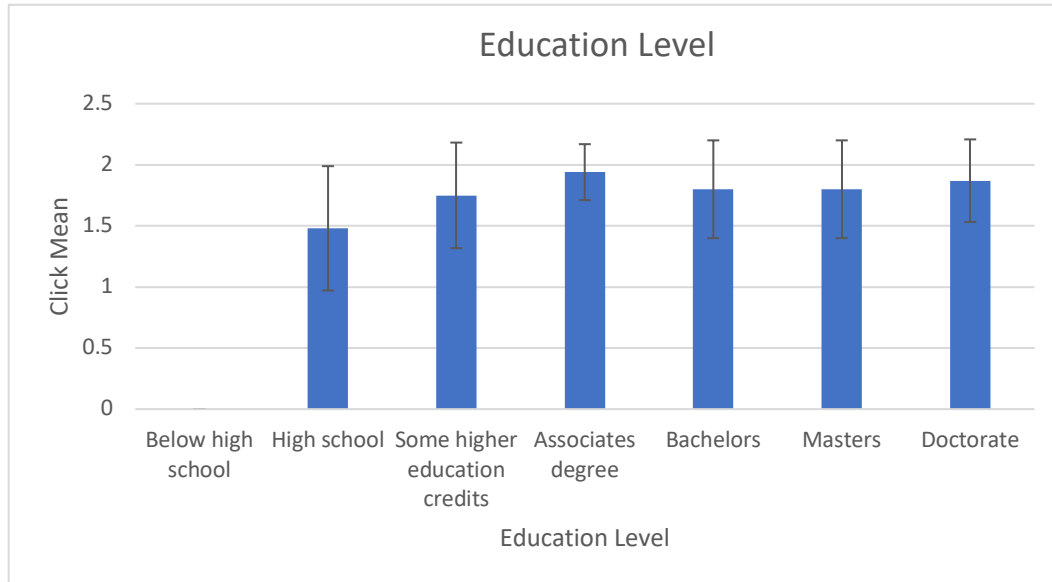
	Click Mean	Std Dev
Below high school	0	0
High school	1.48	0.509
Some higher education credits	1.75	0.432
Associates degree	1.94	0.229
Bachelors	1.8	0.4
Masters	1.8	0.4
Doctorate	1.87	0.338

*Phase III – RQ5 – Attention Span Score Group*

The attention span demographic was analyzed using the click mean and standard deviation of all the email interactions with the simulated phishing emails. A summary of this data is shown in Table 28 and displayed in Figure 26. The Average attention span and Somewhat high attention span demographics performed the best at a click mean of 1.76. The Very high attention span demographic performed the worst at a click mean rate of 1.91. This is counter intuitive as it would be thought that those with a High attention span would be alert to possible phishing attempts.

**Figure 24**

*Summary of Education Level Demographic with Respect to Click Mean*

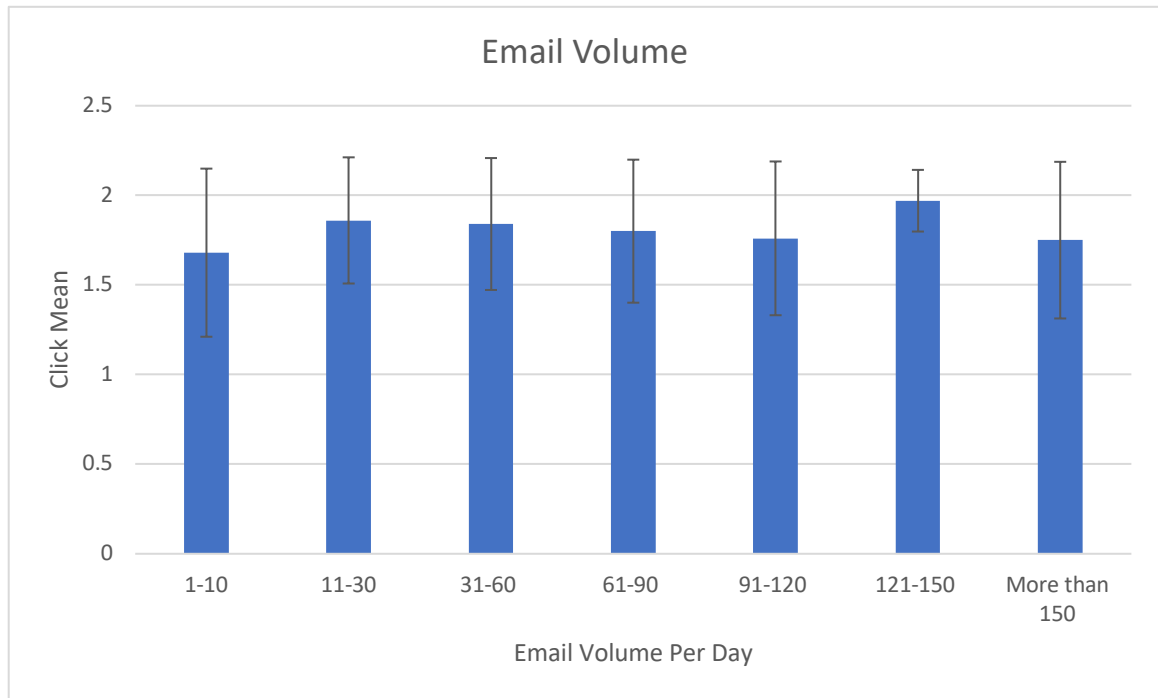
**Table 27**

*Summary of Volume of Email Demographic with Respect to Click Mean*

	Click Mean	Std Dev
1-10 emails per day	1.68	0.469
11-30 emails per day	1.86	0.352
31-60 emails per day	1.84	0.368
61-90 emails per day	1.8	0.399
91-120 emails per day	1.76	0.429
121-150 emails per day	1.97	0.172
More than 150 emails per day	1.75	0.437

**Figure 25**

*Summary of Volume of Email Demographic with Respect to Click Mean*

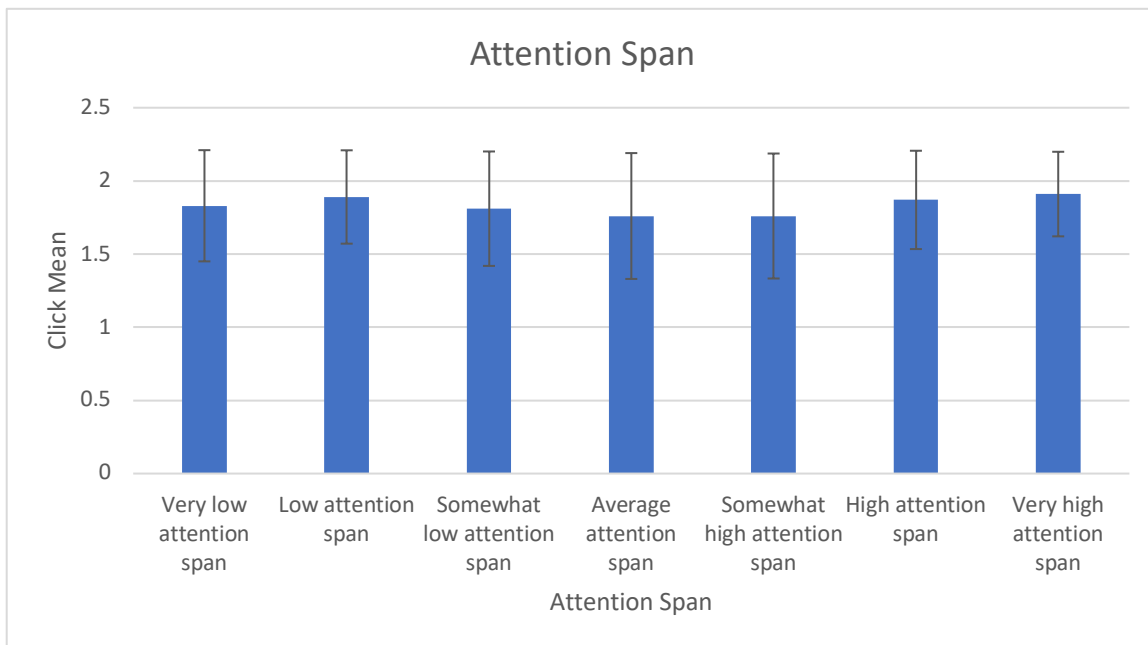
**Table 28**

*Summary of Attention Span Demographic with Respect to Click Mean*

	Click Mean	Std Dev
Very low attention span	1.83	0.38
Low attention span	1.89	0.319
Somewhat low attention span	1.81	0.391
Average attention span	1.76	0.43
Somewhat high attention span	1.76	0.427
High attention span	1.87	0.336
Very high attention span	1.91	0.289

**Figure 26**

*Summary of Attention Span Demographic with Respect to Click Mean*



### Summary

The results and data collection were presented in this chapter. Phase I utilized data from the SME survey to answer RQ1 and RQ2. The PAT mobile app was created and partially tested in Phase II. Pilot testers completed the test of PAT in Phase III. Phase III also included the main study which answered RQs3-5b. An ANOVA was performed on the main study data to answer RQ3 and RQ4. An ANCOVA was performed on the main study data to answer RQ5a and RQ5b.

The results of a two-round Delphi process in Phase I indicated values of 3-seconds, 5-seconds, and 7-seconds as the timer values that should be used in the PAT mobile app. Phase I results also validated the sample emails for use in the PAT mobile app as well as the PAT experimental procedure. These data were used in the creation of the PAT mobile app.

Phase II resulted in the creation of the PAT mobile app. The app was created using data from Phase I, including the timer values, which sample emails to use, and the experimental procedure. The app was tested using pilot testers. Only minor bugs were found and those were fixed before the main study.

Phase III indicated that a countdown timer at 3-seconds with a warning in a text color in red was the most effective in supporting user ability to avoid clicking on a malicious link or attachment. All demographic indicators (age, gender, education level, volume of email per day, and attention span) showed a level of significance.

The age demographic that performed the best (had the lowest click mean) was 18-25. While the age demographic that appeared to perform the worst was Older than 75, there was only one participant in that category, so generalization is difficult. The click mean for both genders was very similar, indicating that gender may not be a factor in ability to avoid clicking a malicious link or attachment. Of education level, the Associates degree demographic performed the worst at a click mean of 1.94, and the High school demographic performed the best at 1.48. This indicates that a higher level of education may not help to mitigate the user's ability to avoid clicking on a malicious email or attachment. The 1-10 emails per day demographic performed the best at a click mean of 1.68, and the 121-150 emails per day demographic performed the worst at a click mean of 1.97. This indicates that fewer emails per day may help to mitigate the user's ability to avoid clicking on a malicious email or attachment. The Average attention span and Somewhat high attention span demographics performed the best at a click mean of 1.76. The Very high attention span demographic performed the worst at a click mean rate of 1.91. This is counter intuitive as it would be thought that those with a High

attention span would be alert to possible phishing attempts. A summary of research question results is shown in Table 29.

**Table 29**

*Summary of Research Question Results*

	RQ	Result
RQ3	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black text?	Grey and red warning text significantly improves a user's ability to avoid clicking on a malicious email when compared to black text
RQ4	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer?	A countdown timer provides the most significant improvement in a user's ability to avoid clicking on a malicious email followed by a count-up timer and no timer
RQ5a	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black text based on the categories of: (a) age, (b) gender, (c) education level, (d) the volume of email the user receives in a day, and (e) attention span?	All five demographic indicators were significant when used as a covariate
RQ5b	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer based on the categories of: (a) age, (b) gender, (c) education level, (d) the volume of email the user receives in a day, and (e) attention span?	All five demographic indicators were significant with respect to Timer Type x Timer Value when used as a covariate

## Chapter 5

### Conclusions, Implications, Recommendations, and Summary

#### **Conclusions**

Red or grey text helps the user's ability to avoid clicking on a malicious link or attachment more than black text does. This seems to follow other studies in which text color was investigated (Nadeem & Junger, 2019; Silver et al., 2002). A countdown timer is better than a count-up timer or no timer with respect to helping the user to avoid clicking on a malicious link or attachment. This follows from studies found in healthcare (Hung et al., 2020; Lindahl et al., 2019; Marto et al., 2016; Uddin et al., 2017), civil engineering (Keegan & O'Mahony, 2003; Kitali et al., 2018), and psychology (Cheong, 2018). Education level appears to have the most positive influence on the user's ability to avoid clicking on a malicious link or attachment both with respect to text warning color and timer value and with respect to timer type and timer value. It appears that less formal education and receiving fewer emails per day helps one's ability to avoid clicking on a malicious link or attachment. This may be because less formally educated users are more careful when responding to an email. This seems to contradict the findings of Ophoff and Robinson (2014) who found formal education to be a positive influence on security behavior. Younger people seem to have a higher ability to avoid clicking on a malicious link or attachment, which agrees with the findings of Koyuncu and Pusatli (2019). There appears to be no difference in gender regarding the ability to avoid clicking on a malicious link or attachment, which seems to contradict Ngoqo and Flowerday (2015)

who found that males have a higher security awareness. It also appears that a high attention span counters one's ability to avoid clicking on a malicious link or attachment. This is counter intuitive, since it is be expected that individuals with a high attention span would be more likely to have the focus required to analyze a possible phish.

The main goal of this research study was to determine through experimental field study whether requiring e-mail users to pause by displaying a colored warning (grey, red, or black text) with a timer (countdown, count-up, or no counter) when they are presented with a potentially malicious link has any effect on the percentage of users falling to phishing attempts. PAT successfully measured user interactions with text warning color and a countdown and count-up timer. The data support the conclusion that a red or grey warning and a timer, specifically a countdown timer, help the user to avoid clicking on a malicious link or attachment.

## **Discussion**

There are several implications for cybersecurity and phishing susceptibility reduction. Warning text color and a timer in the warning dialog may play a significant role in user reaction to a possible phish. In addition, age, gender, education level, volume of email received in a day, and attention span may all affect the user's ability to avoid clicking on a malicious link or attachment.

### *Implications for Practice*

While some corporations already present a colored warning dialog to employees when employees receive an external email, there are no known corporations that employ a timer dialog along with the warning. Corporations could implement a timer dialog to accompany the existing warning text to provide more mitigation against phishing attacks



against their employees. The results show that a countdown timer is more effective than a count-up timer or no timer, lending validation to pedestrian countdown timers.

### *Implications for Research*

Implications for research indicate that both red and grey warning text may be more effective than black text. Timers have not been used in phishing mitigation research previously, and these results show that using timers to mitigate phishing is worthy of further research. The results show that a high attention span negatively effects the ability to avoid clicking on a malicious link which is counter intuitive, and that users with less formal education are more likely to avoid clicking on a malicious link. Future research could investigate these relationships further.

### *Limitations*

This study had several limitations. In Phase I, many invalid responses were received, and this is possibly due to the offering of a \$10 Amazon gift card. It would have been helpful to ask on the SME survey where they found the survey (Facebook or LinkedIn) as this would have helped to track the source of the invalid data. In Phase III, there was a limitation in finding Android users to test the Android version of PAT. A few minor bugs were found, but easily corrected. Loading the email simulations into the app was difficult and time consuming. This can be mitigated in future studies by revising the mechanism in which emails are loaded. As it was, each email with each variable value had to be loaded separately, which meant that 21 versions of each email had to be loaded (two timer types (countdown, count-up) x three colors (black, grey, red) x three timer values (3-seconds, 5-seconds, 7-seconds) + three colors with no timer). During the main study, participants were recruited through Facebook and LinkedIn which created a

limitation of a non-random distribution. In the first few days of the main study data collection, interaction was low. This was mitigated by posting daily reminders on Facebook and LinkedIn. Also, there were a few minor issues with the simulated emails not showing correctly in the app, but these issues were easily fixed. Many participants were confused by what they were to do despite the directions given. It also appeared that many participants did not read the directions as they asked questions that were answered in the directions. Many participants also stated that they would not have clicked on any of the simulated emails if they had been real. This can be mitigated in future studies by modifying the PAT app to use the user's name as a salutation in the simulated emails. Another limitation was the use of the attention span survey from *Psychology Today*. A future research recommendation is to develop a more valid and reliable instrument for attention span.

### **Recommendations and Future Research**

The PAT app could be updated to allow for faster loading of email simulations to make it easier to set up a future study. Many participants stated that they would never respond to an email that was not addressed to them. To address this, PAT could be updated to incorporate the user's name in the simulated emails. Multiple participants indicated that they are used to being able to check the actual email address and/or URL by hovering over the presented value. PAT could also be updated to include these features. PAT could also be updated to allow users to categorize emails by junk or valid by assigning the email to a folder and to validate the sender by simulating a block on the sender email.

Since the app was coded to auto-populate user simulated inboxes at a particular time of day, the PAT app could be used to explore the effect of time of day on the ability to avoid clicking on a malicious link or attachment. While not used in this study, the warning message is able to be changed in the PAT app, so that a future study could investigate word choice in a warning message. The data collected included whether the participant was using an Apple or Android device although that data were not analyzed in this study. A future study could investigate the effect of device usage on the ability to avoid clicking on a malicious link or attachment including a small device such as a phone versus a larger device such as a tablet.

### **Summary**

In summary, a warning in colored text accompanied by a timer helps users to avoid clicking on a malicious link or attachment. This study indicates that a warning in red text accompanied by a countdown timer is the best combination of text and timer. In addition, this study found that the demographic factors of age, gender, education level, email volume, and attention span all influence the user's ability to avoid clicking on a malicious link or attachment.

The main research question that this study addressed is: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values presented with a countdown or count-up timer with a red or grey warning message?

The five specific research questions that this study addressed were:

RQ1: What are the three timer values to require the user to pause that should be

used in this experimental field study to assess users' ability to identify malicious links in e-mail according to cybersecurity SMEs?

RQ2: What level of functional correctness and validity of the custom-designed mobile app is sufficient according to cybersecurity SMEs?

RQ3: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black warning text?

RQ4: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer?

RQ5a: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black warning text based on the categories of: (a) age, (b) gender, (c) education level, (d) attention span, and (e) the volume of email that the user receives in a day?

RQ5b: Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer

values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer based on the categories of: (a) age, (b) gender, (c) education level, (d) attention span, and (e) the volume of email that the user receives in a day?

Phase I answered RQ1 and RQ2. SMEs identified the timer values to use as 3-seconds, 5-seconds, and 7-seconds and gave feedback on the simulated emails to use in the main study as well as the experimental procedures to be used in the main study. Phase II involved the development of PAT, a mobile app that simulates an email inbox capable of displaying a count-up or countdown timer along with specifically colored warning text whenever a link or attachment is part of an email. Phase III answered RQ3-5b and included a pilot study and the main study. The pilot test uncovered a few minor issues that were easily fixed. Analysis of the data from the main study indicated that colored warning text is more effective than black warning text, answering RQ3. A countdown timer was found to be more effective than a count-up timer or no timer, answering RQ4. The demographic indicators of age, gender, education level, email volume, and attention span were all found to influence both text color, answering RQ5a, and timer type, answering RQ5b.

Overall, this study used SME feedback to create a system to investigate whether warning text color or a countdown or count-up timer is effective in helping users to avoid clicking on a malicious link or attachment. The study results showed statistically significant differences among participants presented with red or grey text as compared to black text and presented with a countdown or count-up timer as compared to no timer.

Participants were able to notice phishing emails with the assistance of text warning color and a countdown or count-up timer.

## Appendix A

### Example of SME Demographic Survey

1. Which of the following describes your current job level?

- Owner/Executive/C Level                       Analyst
- Senior Management                               Instructor/Professor
- Middle Management

Other (please specify)

2. How many years of experience do you have in information security?

- Less than one year                               At least 5 years, but less than 10 years
- At least one year, but less than 3 years       10 years or more
- At least three years, but less than 5 years

3. In your opinion, how significant of an issue is phishing?

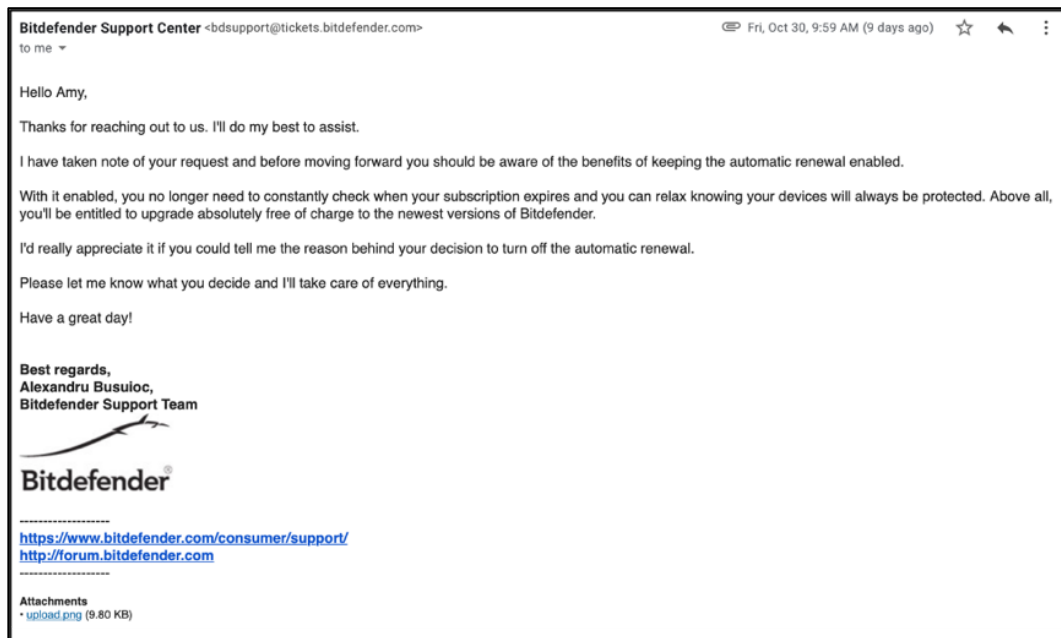
- Quite significant                                   Not very significant
- Very significant                                    Not significant at all
- Somewhat significant

## Appendix B

### Example of SME Sample Email Question

#### 3.1. Sample Email 1:

This is what the participants will see:



3.1.1. Please identify the sample email above as one of the following:

<input type="checkbox"/>	1. Legitimate
<input type="checkbox"/>	2. Phishing
<input type="checkbox"/>	3. Unsure

3.1.2 Please provide your expert opinion about the email sample above by indicating:



<input type="checkbox"/>	1. Keep—the proposed email sample should be included as it is.
<input type="checkbox"/>	2. Adjust—the proposed email sample should be included but with modifications (please provide your feedback on the exact modifications in the short text field in the space provided at the end of this block).
<input type="checkbox"/>	3. Replace —the proposed email sample should be replaced with another one (please provide reasons below why the sample email should be replaced and propose a replacement email, if possible, in the space provided at the end of this block).

3.1.3 If you selected "2. Adjust" and/or "3. Replace" for the sample email above, please provide your recommended adjustments (or write "N/A" if none).

---



---

3.1.4. Please provide additional feedback that you deem fit to be included for sample email above (or write "N/A" if none).

---



---

## Appendix C

### Example of SME Invitation Email

Dear Information Security Subject Matter Expert (SME),

I am a PhD candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy. This work is part of the Levy CyLab Projects (<http://CyLab.nova.edu/>). My research study is seeking to determine if requiring the user to pause can reduce the likelihood of falling for phishing emails.

The goal of the experiment with which I am seeking assistance is to develop an application that will require the user to pause for a certain period of time. The study will be a mobile application that participants download to their mobile device. If the user encounters an email with a link or an attachment, a dialog screen with either a countdown or count-up timer will overlay the email. The user will not be able to interact with the email until the timer has expired.

I am requesting your help to determine what the length of the timer should be.

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personal identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time. As a token of appreciation for your security expert contribution to this research study you will receive a \$10 Amazon digital gift card to your email address upon completing the survey instruments required to initiate this research study.

I appreciate your assistance and contribution to this research study. If you wish to receive the findings of the study, feel free to contact me via email and I will be more than happy to provide you with the information about the academic research publication resulting from this study.

Please let me know if you would like to participate in this SME survey.

## Appendix D

### Example of Participant Recruitment Message for Facebook and LinkedIn

**Seeking Participants**  
**for a cybersecurity research study**

Requirements to participant: Must be 18 or over and a mobile phone user

What you'll do: You will be asked to check a custom mobile app for seven days.

How long it will take: Each day your interaction with the app will take no more than ten minutes

Payment: No payment other than our sincere thanks!

Study title: Pause for a Cybersecurity Cause: Assessing the Influence of a Waiting Period on User Habituation in Mitigation of Phishing Attacks

Questions? Contact:  
Amy E. Antonucci, Principal Investigator  
Nova Southeastern University  
[aa2539@mynsu.nova.edu](mailto:aa2539@mynsu.nova.edu)

or

Dr. Yair Levy  
Nova Southeastern University  
[levyy@nsu.edu](mailto:levyy@nsu.edu)

## Appendix E

### Example of Participant Invitation Email

I am a PhD candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy. This work is part of the Levy Cylab Projects (<http://CyLab.nova.edu/>). I am seeking participants for my dissertation study.

This study will require you to use a custom mobile app for one week. By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personal identifiable information will be collected. You may stop your participation at any time.

If you would like to participate, please go to:  
Pat\_test.com to download the PAT Test App.  
Following download, the test should not take more than 20 minutes.

Best Regards

## Appendix F

### Example of Participant Demographic Survey

#### Participant Demographic Survey

1. Are you completely color blind?

- Yes
- No
- I don't know

2. Do you use an Android or Apple mobile device to check email?

- Yes: Apple
- Yes: Android
- No

3. What is your age?

- 18 - 25
- 26 - 35
- 36 - 45
- 46 - 55
- 56 - 65
- 66 - 75
- Older than 75

4. With which gender do you identify?

- Female
- Male
- Other
- Prefer not to say

## Appendix G

### Example of Participant Attention Span Test

1. Do you get distracted easily (e.g. by background noise, other people's conversations, etc.)? \*

- Yes
- Sometimes
- No

2. How often are you late for work or an appointment? \*

- Quite Often
- Often
- Sometimes
- Rarely
- Almost Never

3. How often do you catch yourself daydreaming at work? \*

- Quite Often
- Often
- Sometimes
- Rarely
- Almost Never

4. Do you jump from task to task because you just can't seem to focus long enough to finish one completely?

- Yes
- Sometimes
- No

5. How do you deal with boring, repetitive tasks? \*

- I'm fine with them; I have very little trouble getting them done.
- I don't mind them, but I may end up needing a break from time to time.
- I can't stand them - they bore me out of my skull.

6. You're on the phone with a friend just as your favorite TV show starts. How difficult would it be for you to pay attention to the conversation? \*

- Extremely Difficult
- Very Difficult
- Somewhat Difficult
- Slightly Difficult
- Not at all Difficult

7. When reading a book or magazine, how often do you find yourself re-reading the same paragraph or skipping ahead? \*

- Quite Often
- Often
- Sometimes
- Rarely
- Almost Never

8. Do you have a knack for noticing details (e.g. typos in a document)? \*

- Yes
- Sometimes
- No

9. Do you lose your patience easily? \*

- Yes
- Sometimes
- No



10. How often do you interrupt people during conversations? \*

- Quite Often
- Very Often
- Sometimes
- Rarely
- Almost Never

Submit

## Appendix H

### Example of Phishing Email

## Security Notice

Dear [berkeley.edu](https://berkeley.edu) member,


As a precautionary measure **we have restricted access to your account until your validate has been changed** . To prevent further irregular activity, you will be unable to send out any emails until this issue has been resolved


To fix security info, click below to validate.


[Click here to validate now](#)

If you usually access your emails via an email or a third-party program, please click above to validate your account via the [berkeley.edu](https://berkeley.edu) homepage. You will then automatically validate your account.

To ensure your account is protected at all times, we ask you to complete the following steps:

 Check that all your computers and mobile devices used to access your account have an up-to-date  
\* virus scanner to detect any possible malware.

 Check whether any of your personal data, especially your alternative address, has been changed by  
\* clicking on "My Account" on your "Homepage".

 Go to your "Email settings" then click on "Filter Rules" to check whether any forwarding rules have  
\* been created. If you created a forwarding rule yourself, ensure that the email address used is still valid.

You can find further information about updating your account security here:

[Help Section](#)

Thank you for your cooperation.

Your [berkeley.edu](https://berkeley.edu) Team

## Appendix I

### Example of Phishing Email with Warning Dialog

# Security Notice

Dear [berkeley.edu](http://berkeley.edu) member,


As a precautionary measure **we have restricted access to your account until your validate has been changed** . To prevent further irregular activity, you will be unable to send out any emails until this issue has been resolved


To fix security info, click below to validate.




If you usually a  
above to va

To ensure your a

 Check that all y  
\* virus scanner to

 Check whether  
\* clicking on "My Account" on your "Homepage".

 Go to your "Email settings" then click on "Filter Rules" to check whether any forwarding rules have  
\* been created. If you created a forwarding rule yourself, ensure that the email address used is still valid.

You can find further information about updating your account security here:  
[Help Section](#)

Thank you for your cooperation.  
Your [berkeley.edu](http://berkeley.edu) Team

## Appendix J


### Example of Phishing Email with Warning Dialog with Timer

# Security Notice

Dear [berkeley.edu](http://berkeley.edu) member,

As a precautionary measure **we have restricted access to your account until your validate has been changed** . To prevent further irregular activity, you will be unable to send out any emails until this issue has been resolved

To fix security info, click below to validate.



**Warning!**  
This e-mail may contain malicious links or attachments. Please pause for the time below to carefully consider if the content is safe before proceeding!

0:27

If you usually a  
above to va

To ensure your e

Check that all y  
\* virus scanner to

Check whether  
\* clicking on "My Account" on your "Homepage".

Go to your "Email settings" then click on "Filter Rules" to check whether any forwarding rules have  
\* been created. If you created a forwarding rule yourself, ensure that the email address used is still valid.

re an up-to-date  
been changed by

You can find further information about updating your account security here:  
[Help Section](#)

Thank you for your cooperation.  
Your [berkeley.edu](http://berkeley.edu) Team

## Appendix K

## Data Collection Detail

No	Research Question	Collection Instrument	Specific Data Collection Question or Screen	Analysis
R Q1	What are the three timer values to require the user to pause that should be used in this experimental field study to assess users' ability to identify malicious links in e-mail according to cybersecurity SMEs?	SME anonymous survey	Question: Please rank the timer values from best to use to worst to use.	Delphi method with Kendall's W values  Three timer values with highest agreement among SMEs will be chosen for Phases II and III
R Q2	What level of functional correctness and validity of the custom-designed mobile app is sufficient according to cybersecurity SMEs?	SME Quantitative Feedback	Please record the actions taken while SME tester is using PAT.	Direct Observation with Delphi method  PAT will be validated and considered functionally correct
R Q3	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in	PAT	PAT main application screen  Data collected for open emails with URL: <ul style="list-style-type: none"> <li>• URL</li> <li>• Whether link or attachment was clicked</li> </ul>	factorial ANOVA

	(a) grey, (b) red, or (c) black text?			
R Q4	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer?	PAT	PAT main application screen  Data collected for open emails with URL: <ul style="list-style-type: none"> <li>• URL</li> <li>• Whether link or attachment was clicked</li> </ul>	factorial ANOVA
R Q5 a	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with a warning in (a) grey, (b) red, or (c) black text based on the categories of: (a) age, (b) gender, (c) education level, (d) attention span, and (e) the volume	PAT	PAT Demographic Survey	factorial ANCOVA

---

	of email that the user receives in a day?			
R	Are there statistically significant mean differences between the ability to avoid clicking on a malicious link of e-mail users who are not required to pause vs. email users who are required to pause at three separate timer values displayed with: (a) countdown timer, (b) count-up timer, or (c) no timer based on the categories of: (a) age, (b) gender, (c) education level, (d) attention span, and (e) the volume of email that the user receives in a day?	PAT	PAT Demographic Survey	factorial ANCOVA

---

## Appendix L

### Institutional Review Board Exemption Letter



#### MEMORANDUM

**To:** Amy E Antonucci, MS  
College of Engineering and Computing

**From:** Ling Wang, Ph.D.  
College Representative, College of Engineering and Computing

**Date:** November 29, 2020

**Subject:** IRB Exempt Initial Approval Memo

**TITLE:** Pause for a Cybersecurity Cause: Assessing the Influence of a Waiting Period on User Habituation in Mitigation of Phishing Attacks– NSU IRB Protocol Number 2020-588

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **November 29, 2020**. You may proceed with your study.

*Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.*

**Level of Review:** Exempt

**Type of Approval:** Initial Approval

**Exempt Review Category:** Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

**Post-Approval Monitoring:** The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

**Annual Status of Research Update:** You are required to notify the IRB Office annually if your

Page 1 of 2



## References

- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., & Sleeper, M. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3), 44. <https://doi.org/10.1145/3054926>
- Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, 3(1), 1-19. <https://doi.org/10.1186/s42400-020-00047-5>
- Alert Logic. (2018, August 22). *Must-know phishing statistics 2018*. <https://blog.alertlogic.com/must-know-phishing-statistics-2018/>
- Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, 26(6), 661-687. <https://doi.org/10.1057/s41303-017-0057-y>
- Alnajim, A., & Munro, M. (2009). An anti-phishing approach that uses training intervention for phishing websites detection. *Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations*, 405-410. <https://doi.org/10.1109/ITNG.2009.109>
- Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS one*, 12(3), e0173284. <https://doi.org/10.1371/journal.pone.0173284.t001>
- Alseadoon, I. M. A. (2014). *The impact of users' characteristics on their ability to detect phishing emails* (Publication No. 72873) [Doctoral thesis, Queensland University of Technology]. QUT ePrints.
- Althobaiti, K., Meng, N., & Vaniea, K. (2021). *I don't need an expert! Making URL phishing features human comprehensible*. Proceedings of the CHI Conference on Human Factors in Computing Systems, Yokohama, Japan.
- Aminuddin, M. M. M., & Nasir, H. M. (2019). Focus loss while driving detection by using prior stage ERP as baseline. *International Journal of Human and Technology Interaction*, 3(1), 39-46.
- Amran, A., Zaaba, Z. F., & Mahinderjit Singh, M. K. (2018). Habituation effects in computer security warning. *Information Security Journal: A Global Perspective*, 27(4), 192-204. <https://doi.org/10.1080/19393555.2018.1505008>

- Amro, B. (2018). Phishing techniques in mobile devices. *Journal of Computer and Communications*, 6, 27-35. <https://doi.org/10.4236/jcc.2018.62003>
- Anderson, B., Kirwan, C., Eargle, D., Jensen, S., & Vance, A. (2015). Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: A neurosecurity study. *Journal of Cybersecurity*, 1(1), 109-120. <https://doi.org/10.1093/cybsec/tyv005>
- Anderson, B., Vance, A., Kirwan, B., Eargle, D., & Howard, S. (2014a). Users aren't (necessarily) lazy: Using neurois to explain habituation to security warnings. *Proceedings of the International Conference on Information Systems*, 1-15.
- Anderson, B., Vance, A., Kirwan, B., Eargle, D., & Howard, S. (2014b). Why users habituate to security warnings: Insights from fMRI. *Proceedings of 2014 IFIP*, 8, 21-41.
- Anderson, B., Vance, A., Kirwan, C., Jenkins, J., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, 33(3), 713-743. <https://doi.org/10.1080/07421222.2016.1243947>
- Anti-Phishing Working Group. (2020). *Phishing activities trends report 1st quarter 2020*. [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2020.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf)
- Arazy, O., Kopak, R., & Hadar, I. (2017). Heuristic principles and differential judgments in the assessment of information quality. *Journal of the Association for Information Systems*, 18(5), 403-432. <https://doi.org/0.17705/1jais.00458>
- Aroyo, A. M., Rea, F., Sandini, G., & Sciutti, A. (2018). Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble? *IEEE Robotics and Automation Letters*, 3(4), 3701-3708. <https://doi.org/10.1109/LRA.2018.2856272>
- Ayyagari, R., & Tyks, J. (2012). Disaster at a university: A case study in information security. *Journal of Information Technology Education*, 11, 85-96.
- Baldwin, C. L., Roberts, D. M., Barragan, D., Lee, J. D., Lerner, N., & Higgins, J. S. (2017). Detecting and quantifying mind wandering during simulated driving. *Frontiers in Human Neuroscience*, 11, 1-15. <https://doi.org/10.3389/fnhum.2017.00406>
- Ball, A. (2012). *A comparison of users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems* (Publication No.

3543920) [Doctoral dissertation, Nova Southeastern University]. ProQuest Dissertations and Theses Global.

- Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management*, 3(1), 180-207.
- Barque-Duran, A., Pothos, E. M., Hampton, J. A., & Yearsley, J. M. (2017). Contemporary morality: Moral judgments in digital contexts. *Computers in Human Behavior*, 75, 184-193.
- Baslyman, M., & Chiasson, S. (2016). "Smells phishy?": An educational game about online phishing scams. *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 1-11. <https://doi.org/10.1109/ECRIME.2016.7487946>
- Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers & Security*. <https://doi.org/10.1016/j.cose.2021.102278>
- Bazilinsky, P., Dodou, D., & De Winter, J. (2019). Survey on eHMI concepts: The effect of text, color, and perspective. *Transportation Research Part F: Traffic Psychology and Behaviour*, 67, 175-194.
- Biros, D. P., George, J. F., & Zmud, R. W. (2002). Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly*, 26(2), 119-144. <https://doi.org/10.2307/4132323>
- Biswas, S., Ghosh, I., & Chandra, S. (2017). Effect of traffic signal countdown timers on pedestrian crossings at signalized intersection. *Transportation in Developing Economies*, 3(1), 2-18. <https://doi.org/10.1007/s40890-016-0032-7>
- Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. *Computers & Security*, 73, 266-293.
- Booth, S., Tompkin, J., Pfister, H., Waldo, J., Gajos, K., & Nagpal, R. (2017). *Piggybacking robots: Human-robot overtrust in university dormitory security*. Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, <https://doi.org/10.1145/2909824.3020211>
- Bottazzi, G., Casalicchio, E., Cingolani, D., Marturana, F., & Piu, M. (2015). MP-shield: A framework for phishing detection in mobile devices. *Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure*

*Computing; Pervasive Intelligence and Computing*, 1977-1983.  
<https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.293>

- Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2), 18-26. <https://doi.org/10.1109/MSP.2010.198>
- Brooks, T. E., Case, B. J., & Young, M. J. (2003). *Timed versus untimed testing conditions and student performance I*. Pearson Education.  
[http://images.pearsonassessments.com/images/tmrs/tmrs\\_rg/TimedUntimed.pdf](http://images.pearsonassessments.com/images/tmrs/tmrs_rg/TimedUntimed.pdf)
- Brustoloni, J. C., & Villamarín-Salomón, R. (2007, 2007, July 18-20). *Improving security decisions with polymorphic and audited dialogs* [Paper presentation]. 3rd Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania.
- Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of experimental criminology*, 11(1), 97-115.  
<https://doi.org/10.1007/s11292-014-9222-7>
- Bulling, A. (2016). Pervasive attentive user interfaces. *Computer*(1), 94-98.  
<https://doi.org/10.1109/MC.2016.32>
- Burns, A., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, 29(1), 24-39.  
<https://doi.org/10.1080/10919392.2019.1552745>
- Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). *Breaching the human firewall: Social engineering in phishing and spear-phishing emails*. Proceedings of the Australasian Conference on Information Systems, Adelaide, Australia.
- Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, 12(1), 28-38. <https://doi.org/10.1109/MSP.2013.106>
- Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills* (Publication No. 10240271) [Doctoral dissertation, Nova Southeastern University]. ProQuest Dissertations and Theses Global.
- Carlton, M., Levy, Y., & Ramim, M. M. (2018). Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool. *Online Journal of Applied*

- Knowledge Management (OJAKM)*, 6(1), 107-118.  
[https://doi.org/10.36965/OJAKM.2018.6\(1\)107-118](https://doi.org/10.36965/OJAKM.2018.6(1)107-118)
- Chang, J., & Chong, M. D. (2021). Cognitive heuristics and risk evaluation in crisis fraud. *Journal of Financial Crime*. <https://doi.org/10.1108/JFC-02-2021-0030>
- Chassidim, H., Perentis, C., Toch, E., & Lepri, B. (2020). Between privacy and security: The factors that drive intentions to use cyber-security applications. *Behaviour & Information Technology*, 1-15. <https://doi.org/10.1080/0144929X.2020.1781259>
- Chatchalermpun, S., & Daengsi, T. (2021). *Improving cybersecurity awareness using phishing attack simulation*. IOP Conference Series: Materials Science and Engineering, Medan, Indonesia. <https://doi.org/10.1088/1757-899X/1088/1/012015>
- Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, 10(1), 247-256. <https://doi.org/10.14257/ijasia.2016.10.1.23>
- Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior. *Information & Computer Security*. <https://doi.org/10.1108/ICS-04-2016-0027>
- Chen, J., Mishler, S., Hu, B., Li, N., & Proctor, R. W. (2018). The description-experience gap in the effect of warning reliability on user trust and performance in a phishing-detection context. *International Journal of Human-Computer Studies*, 119, 35-47. <https://doi.org/10.1016/j.ijhcs.2018.05.010>
- Cheong, L. (2018). *Evaluating visualization for emergency decision-making under uncertainty* [Doctoral thesis, Royal Melbourne Institute of Technology]. RMIT Research Repository. <https://researchbank.rmit.edu.au/view/rmit:162600/Cheong.pdf>
- Cheung, C., Lee, Z. W., & Chan, T. K. (2015). Self-disclosure in social networking sites. *Internet Research*. <https://doi.org/10.1108/IntR-09-2013-0192>
- 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, Washington, D.C., United States. <https://doi.org/10.1145/2335356.2335358>
- Chorghé, S. P., & Shekokar, N. (2016). *A survey on anti-phishing techniques in mobile phones*. Proceedings of the 2016 International Conference on Inventive Computation Technologies, Coimbatore, India. <https://doi.org/10.1109/INVENTIVE.2016.7824819>

- Conteh, N. Y., & Royer, M. D. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer*, 20(1), 1-12.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publication, Inc.
- Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security*, 24(1), 116-134. <https://doi.org/10.1108/ICS-04-2015-0018>
- De Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L., & Zurko, M. E. (2009). *Adaptive security dialogs for improved security behavior of users*. Proceedings of the IFIP Conference on Human-Computer Interaction, Uppsala, Sweden. [https://doi.org/10.1007/978-3-642-03655-2\\_57](https://doi.org/10.1007/978-3-642-03655-2_57)
- Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montréal, Québec, Canada. <https://doi.org/10.1145/1124772.1124861>
- Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, 1-19. <https://doi.org/10.1080/0960085X.2020.1797546>
- Egelman, S., Cranor, L. F., & Hong, J. (2008). *You've been warned: An empirical study of the effectiveness of web browser phishing warnings*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy. <https://doi.org/10.1145/1357054.1357219>
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology*, 6, 323-337.
- FBI. (2018). *Business e-mail compromise the 12 billion dollar scam*. <https://www.ic3.gov/media/2018/180712.aspx>
- Fine, L. (2016). *The presence of timers and their impact on team communications during high-stress scenarios*. Union College.
- 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>
- Fleming, A. (2017). *Exploring Information Security Awareness Training to Reduce Unauthorized Disclosure of Information in Public Schools* (Publication No.



10637293) [Doctoral thesis, Northcentral University]. ProQuest Dissertations & Theses.

- George, J. F., Marett, K., Crews, J., Cao, J., Lin, M., Biros, D., & Burgoon, J. (2004). *Training to detect deception: An experimental investigation*. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, United States. <https://doi.org/10.1109/HICSS.2004.1265082>
- Gerlach, J., Buxmann, P., & Dinev, T. (2019). “They’re all the same!” Stereotypical thinking and systematic errors in users’ privacy-related judgments about online services. *Journal of the Association for Information Systems*, 20(6), 787-823. <https://doi.org/10.17705/1jais.00551>
- Gigerenzer, G. (1991). How to make cognitive illusions disappear: Beyond “heuristics and biases”. *European Review of Social Psychology*, 2(1), 83-115.
- Gigerenzer, G. (1996). On narrow norms and vague heuristics: A reply to Kahneman and Tversky. *Psychological Review*, 103(3), 592-596. <https://doi.org/10.1037/0033-295X.103.3.592>
- Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, 73, 519-544. <https://doi.org/10.1016/j.cose.2017.12.006>
- Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1), 22-44. <https://doi.org/10.17705/1jais.00447>
- Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., & Parkulo, M. (2019). Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Network Open*, 2(3), 1/9-9/9. <https://doi.org/10.1001/jamanetworkopen.2019.0393>
- Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, 26(6), 547-552. <https://doi.org/10.1093/jamia/ocz005>
- Grummon, A. H., Hall, M. G., Taillie, L. S., & Brewer, N. T. (2019). How should sugar-sweetened beverage health warnings be designed? A randomized experiment. *Preventive Medicine*, 121, 158-166. <https://doi.org/10.1016/j.ypmed.2019.02.010>
- Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247-267.

- Hale, M. L., Gamble, R. F., & Gamble, P. (2015). *CyberPhishing: A game-based platform for phishing awareness testing*. Proceedings of the 48th Hawaii International Conference on System Sciences, Kauai, HI, United States. <https://doi.org/10.1109/HICSS.2015.670>
- 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. *Social Science Research Network*. <https://doi.org/10.2139/ssrn.2544742>
- Hall, E. T., Weaver, K. W., Perino, A. C., Elder, A., & Verghese, A. (2018). 'A man walks into a bar': Riddles in the teaching of medicine. *The American Journal of Medicine*, 131(9), 1000-1002. <https://doi.org/10.1016/j.amjmed.2018.03.033>
- Hanus, B., Wu, Y. A., & Parrish, J. (2021). Phish me, phish me not. *Journal of Computer Information Systems*, 1-11. <https://doi.org/10.1080/08874417.2020.1858730>
- Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014). Using personal examples to improve risk communication for security & privacy decisions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2647-2656. <https://doi.org/10.1145/2556288.2556978>
- Harrison, A., Samuel, B., Shan, Z., Cook, M., Zu, T., & Dawani, D. (2019). *Learning to see the hook: Comparing phishing training approaches*. Proceedings of the Fortieth International Conference on Information Systems, Munich, Germany.
- He, J., Becic, E., Lee, Y.-C., & McCarley, J. S. (2011). Mind wandering behind the wheel: Performance and oculomotor correlates. *Human Factors*, 53(1), 13-21. <https://doi.org/10.1177/0018720810391530>
- Hirshleifer, D., Levi, Y., Lourie, B., & Teoh, S. H. (2019). Decision fatigue and heuristic analyst forecasts. *Journal of Financial Economics*, 133(1), 83-98. <https://doi.org/10.1016/j.jfineco.2019.01.005>
- Hung, L. C., Yang, J. Y., Chen, M. C., Chang, H. L., Ku, C. Y., & Hou, T. W. (2020). Design and evaluation of the bed-cleaning mobile application. *Journal of Nursing Management*, 28(4), 771-776. <https://doi.org/10.1111/jonm.12900>
- Imgraben, J., Engelbrecht, A., & Choo, K.-K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, 33(12), 1347-1360. <https://doi.org/10.1080/0144929X.2014.934286>



- Itri, J. N., & Patel, S. H. (2018). Heuristics and cognitive error in medical imaging. *American Journal of Roentgenology*, 210(5), 1097-1105. <https://doi.org/10.2214/AJR.17.18907>
- Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 6(1), 8. <https://doi.org/10.1186/s13673-016-0065-2>
- Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods*, 18(1), 3-20. <https://doi.org/10.1177/1525822X05282260>
- Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., & Kumar, R. (2016). Social engineering: Hacking a human being through technology. *IOSR Journal of Computer Engineering*, 18(5), 94-100. <https://doi.org/10.9790/0661-18050594100>
- Jenkins, J., & Durcikova, A. (2013). What, I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior. *Proceedings of the International Conference on Information Systems*, 1-18.
- Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34(2), 597-626. <https://doi.org/10.1080/07421222.2017.1334499>
- Joo, J. W., Moon, S. Y., Singh, S., & Park, J. H. (2017). S-Detector: An enhanced security model for detecting smishing attack for mobile computing. *Telecommunication Systems*, 66(1), 29-38.
- Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75-87. <https://doi.org/10.1016/j.chb.2016.09.012>
- Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
- Kahneman, D., & Tversky, A. (1973). On the psychology of prediction. *Psychological Review*, 80(4), 237-251. <https://doi.org/10.1037/h0034747>
- Kahneman, D., & Tversky, A. (1996). On the reality of cognitive illusions. *Psychological Review*, 103(3), 582-591. <https://doi.org/10.1037/0033-295X.103.3.582>
- Karegar, F., Pettersson, J. S., & Fischer-Hübner, S. (2020). The dilemma of user engagement in privacy notices: Effects of interaction modes and habituation on user attention. *ACM Transactions on Privacy and Security (TOPS)*, 23(1), 1-38. <https://doi.org/10.1145/3372296>

- Keegan, O., & O'Mahony, M. (2003). Modifying pedestrian behaviour. *Transportation Research Part A: Policy and Practice*, 37(10), 889-901.  
[https://doi.org/10.1016/S0965-8564\(03\)00061-2](https://doi.org/10.1016/S0965-8564(03)00061-2)
- Kim, S., & Wogalter, M. S. (2009). Habituation, dishabituation, and recovery effects in visual warnings. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 53(20), 1612-1616.  
<https://doi.org/10.1177/154193120905302015>
- Kitali, A. E., Sando, T., Castro, A., Kobelo, D., & Mwakalonge, J. (2018). Using crash modification factors to appraise the safety effects of pedestrian countdown signals for drivers. *Journal of Transportation Engineering Part A-Systems*, 144(5), 1-9.  
<https://doi.org/10.1061/JTEPBS.0000130>
- Klein, G. A. (1993). A recognition-primed decision (RPD) model of rapid decision making. *Decision Making in Action: Models and Methods*, 5(4), 138-147.
- Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*, 2019.  
<https://doi.org/10.1155/2019/2786913>
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113-122.  
<https://doi.org/10.1016/j.jisa.2014.09.005>
- Kumar, N., & Chaudhary, P. (2017). Mobile phishing detection using naive Bayesian algorithm. *International Journal of Computer Science and Network Security*, 17(7), 142-147.
- Kumaraguru, P. (2009). *Phishguru: A system for educating users about semantic attacks* (Publication No. 3357586) [Doctoral dissertation, Carnegie Mellon University]. ProQuest Dissertations and Theses Global.
- Lindahl, C., Wagner, S., Uldbjerg, N., Schlütter, J. M., Bertelsen, O., & Sandager, P. (2019). Effects of context-aware patient guidance on blood pressure self-measurement adherence levels. *Health Informatics Journal*, 25(2), 417-428.  
<https://doi.org/10.1177/1460458217717073>
- Lindegren, D., Karegar, F., Kane, B., & Pettersson, J. S. (2021). An evaluation of three designs to engage users when providing their consent on smartphones. *Behaviour & Information Technology*, 40(4), 398-414.  
<https://doi.org/10.1080/0144929X.2019.1697898>

- Liu, Y., Zhu, C., Wu, Y., Xu, H., & Song, J. (2021). MMWD: An efficient mobile malicious webpage detection framework based on deep learning and edge cloud. *Concurrency and Computation: Practice and Experience*, 1-14. <https://doi.org/10.1002/cpe.6191>
- Lo, J. C., Twan, D. C., Karamchedu, S., Lee, X. K., Ong, J. L., Van Rijn, E., Gooley, J. J., & Chee, M. W. (2019). Differential effects of split and continuous sleep on neurobehavioral function and glucose tolerance in sleep-restricted adolescents. *Sleep*, 42(5), 1-10.
- Mansfield-Devine, S. (2018). The ever-changing face of phishing. *Computer Fraud & Security*, 2018(11), 17-19. [https://doi.org/10.1016/S1361-3723\(18\)30111-8](https://doi.org/10.1016/S1361-3723(18)30111-8)
- Mark, T., Bulla, J., Niraj, R., Bulla, I., & Schwarzwäller, W. (2019). Catalogue as a tool for reinforcing habits: Empirical evidence from a multichannel retailer. *International Journal of Research in Marketing*, 36(4), 528-541. <https://doi.org/10.1016/j.ijresmar.2019.01.009>
- Marriott, C. (2018). *Through the net: Investigating how user characteristics influence susceptibility to phishing* [Masters dissertation, Dublin Institute of Technology]. <https://arrow.dit.ie/scschcomdis/140/>
- Martin, N. (2008). *Habit: The 95% of behavior marketers ignore*. Ft Press.
- Martin, N., & Morich, K. (2011). Unconscious mental processes in consumer choice: Toward a new model of consumer behavior. *Journal of Brand Management*, 18(7), 483-505. <https://doi.org/10.1057/bm.2011.10>
- Marto, J. P., Borbinha, C., Calado, S., & Viana-Baptista, M. (2016). The stroke chronometer—A new strategy to reduce door-to-needle time. *Journal of Stroke and Cerebrovascular Diseases*, 25(9), 2305-2307. <https://doi.org/10.1016/j.jstrokecerebrovasdis.2016.05.023>
- Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of US hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security and Privacy*, 2(3), 71-83.
- Mehta, R., Demmers, J., van Dolen, W. M., & Weinberg, C. B. (2017). When red means go: Non-normative effects of red under sensation seeking. *Journal of Consumer Psychology*, 27(1), 91-97. <https://doi.org/10.1016/j.jcps.2016.04.004>
- Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, 14(2), 91-116.

- Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multi-variate statistical methods*. Pyrczak Publishing.
- Mi, T., Gou, M., Zhou, G., Gan, Y., & Schwarzer, R. (2020). Effects of planning and action control on smartphone security behavior. *Computers & Security, 97*, 1-7. <https://doi.org/10.1016/j.cose.2020.101954>
- Mihelič, A., Jevšček, M., Vrhovec, S., & Bernik, I. (2019). Testing the human backdoor: Organizational response to a phishing campaign. *Journal of Universal Computer Science, 25*(11), 1458-1477.
- Minakawa, R., & Takada, T. (2017). Exploring alternative security warning dialog for attracting user attention: Evaluation of “kawaii” effect and its additional stimulus combination. *Proceedings of the 19th International Conference on Information Integration and Web-based Applications & Services*, 582-586. <https://doi.org/10.1145/3151759.3151846>
- Miranda, M. J. (2018). Enhancing cybersecurity awareness training: a comprehensive phishing exercise approach. *International Management Review, 14*(2), 5-10.
- Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
- Molinaro, K. A. (2019). *Understanding the phish: Using judgment analysis to evaluate the human judgment of phishing emails* (Publication No. 13424290) [Doctoral dissertation, State University of New York at Buffalo]. ProQuest Dissertations and Theses Global.
- Mukhopadhyay, S., & Argles, D. (2011). *An anti-phishing mechanism for single sign-on based on QR-code*. Proceedings of the International Conference on Information Society, London, UK. <https://doi.org/10.1109/i-Society18435.2011.5978554>
- Musuva, P., Chepken, C., & Getao, K. (2019). A naturalistic methodology for assessing susceptibility to social engineering through phishing. *The African Journal of Information Systems, 11*(3), 157-182.
- Nadeem, A., & Junger, M. (2019). Laptop theft in a university setting can be avoided with warnings. <https://arxiv.org/abs/1907.08083>
- Nadler, A., & McGuigan, L. (2018, 2018/03/15). An impulse to exploit: The behavioral turn in data-driven marketing. *Critical Studies in Media Communication, 35*(2), 151-165. <https://doi.org/10.1080/15295036.2017.1387279>

- National Eye Institute. (2019). *Types of color blindness*. <https://www.nei.nih.gov/learn-about-eye-health/eye-conditions-and-diseases/color-blindness/types-color-blindness>
- Ndibwile, J. D., Kadobayashi, Y., & Fall, D. (2017). *UnPhishMe: Phishing attack detection by deceptive login simulation through an android mobile app*. Proceedings of the 2017 12th Asia Joint Conference on Information Security, Seoul, South Korea. <https://doi.org/10.1109/AsiaJCIS.2017.19>
- Ndibwile, J. D., Luhanga, E. T., Fall, D., Miyamoto, D., Blanc, G., & Kadobayashi, Y. (2019). An empirical approach to phishing countermeasures through smart glasses and validation agents. *IEEE Access*, 7, 130758-130771. <https://doi.org/10.1109/ACCESS.2019.2940669>
- Newquist, M. H., Dozier, C. L., & Neidert, P. L. (2012). A comparison of the effects of brief rules, a timer, and preferred toys on self control. *Journal of Applied Behavior Analysis*, 45(3), 497-509. <https://doi.org/10.1901/jaba.2012.45-497>
- Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security*, 53, 132-142. <https://doi.org/10.1016/j.cose.2015.05.011>
- Nguyen, C., Jensen, M. L., Durcikova, A., & Wright, R. T. (2021). A comparison of features in a crowdsourced phishing warning system. *Information Systems Journal*, 473-513. <https://doi.org/10.1111/isj.12318>
- Nowitz, J. (2018). *A Modern Perspective on Phishing: An investigation into susceptibility to phishing attacks between mobile and desktop email clients* [Master Thesis, Victoria University of Wellington]. <http://hdl.handle.net/10063/7907>
- Nowrin, S., & Bawden, D. (2018). Information security behaviour of smartphone users. *Information and Learning Science*, 119(7/8), 444-455. <https://doi.org/10.1108/ILS-04-2018-0029>
- Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., & Ebner, N. (2017). *Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing*. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, United States.
- Ophoff, J., & Robinson, M. (2014). *Exploring end-user smartphone security awareness within a South African context*. 2014 Information Security for South Africa, Johannesburg, South Africa. <https://doi.org/10.1109/ISSA.2014.6950500>

- Orunsolu, A. A., Alaran, M. A., Adebayo, A. A., Kareem, S. O., & Oke, A. (2017). A lightweight anti-phishing technique for mobile phone. *Acta Informatica Pragensia*, 6(2), 114-123. <https://doi.org/10.18267/j.aip.104>
- Osman, M. (2020). Overstepping the boundaries of free choice: Folk beliefs on free will and determinism in real world contexts. *Consciousness and Cognition*, 77, 1-15. <https://doi.org/10.1016/j.concog.2019.102860>
- Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, 128, 17-26. <https://doi.org/10.1016/j.ijhcs.2019.02.007>
- Parsons, K., Butavicius, M., Pattinson, M., Calic, D., McCormac, A., & Jerram, C. (2015). *Do users focus on the correct cues to differentiate between phishing and genuine emails?* Proceedings of the Australasian Conference on Information Systems, Adelaide, Australia.
- Phang, I., Zaiton, O., & Cheuk, C. H. (2018). Young adult Malaysian consumers' intention to shop via mobile shopping apps. *Asian Journal of Business Research Volume*, 8(1), 18-37. <https://doi.org/10.14707/ajbr.180041>
- Psychology Today. (n.d.). *Attention span test*. <https://www.psychologytoday.com/us/tests/personality/attention-span-test>
- Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks. *Frontiers in Psychology*, 9, 135-149. <https://doi.org/10.3389/fpsyg.2018.00135>
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A., & Pakrijauskas, K. (2020). E-mail-based phishing attack taxonomy. *Applied Sciences*, 10(7), 1-15. <https://doi.org/10.3390/app10072363>
- Risbey, J. S., & Lewandowsky, S. (2017). Climate science: The 'pause' unpacked. *Nature*, 545(7652), 37-39.
- Rosa, E., Dahlstrom, N., Knez, I., Ljung, R., Cameron, M., & Willander, J. (2021). Dynamic decision-making of airline pilots in low-fidelity simulation. *Theoretical Issues in Ergonomics Science*, 22(1), 83-102. <https://doi.org/10.1080/1463922X.2020.1758830>



- Ross, B., Jung, A., Heisel, J., & Stieglitz, S. (2018). *Fake news on social media: The (in) effectiveness of warning messages*. Proceedings of the Thirty Ninth International Conference on Information Systems, San Francisco, CA, United States.
- Rothman, L., Cloutier, M.-S., Macpherson, A. K., Richmond, S. A., & Howard, A. W. (2019). Spatial distribution of pedestrian-motor vehicle collisions before and after pedestrian countdown signal installation in Toronto, Canada. *Injury Prevention*, 25(2), 110-115. <https://doi.org/10.1136/injuryprev-2017-042378>
- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, 11(4), 89. <https://doi.org/10.3390/fi11040089>
- Schmidt, R. C. (1997). Managing Delphi surveys using nonparametric statistical techniques. *Decision Sciences*, 28(3), 763-774. <https://doi.org/10.1111/j.1540-5915.1997.tb01330.x>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). John Wiley & Sons, Ltd.
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). *Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish*. Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, United States. <https://doi.org/10.1145/1280680.1280692>
- Silver, N. C., Drake, K. L., Niaghi, Z. B., Brim, A. C., & Pedraza, O. (2002). The effects of product, signal word, and color on warning labels: Differences in perceived hazard. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 46(6), 735-739. <https://doi.org/doi/10.1177/154193120204600611>
- Soraghan, C. (2019). *An analysis of nudging as a social marketing technique using Front of Pack nutrition labels: A study of women's perceptions of food labels* (Publication No. 2322032258) [Doctoral, Edinburgh Napier University]. Ann Arbor, MI.
- Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: a Phish Scale. *Journal of Cybersecurity*, 6(1), 1-16. <https://doi.org/10.1093/cybsec/tyaa009>
- Stokes, Y., Vandyk, A., Squires, J., Jacob, J.-D., & Gifford, W. (2019). Using Facebook and LinkedIn to recruit nurses for an online survey. *Western Journal of Nursing Research*, 41(1), 96-110. <https://doi.org/10.1177/0193945917740706>
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169. <https://doi.org/10.2307/248922>

- Sun, J. C.-Y., Kuo, C.-Y., Hou, H.-T., & Lin, Y.-Y. (2017). Exploring learners' sequential behavioral patterns, flow experience, and learning performance in an anti-phishing educational game. *Journal of Educational Technology & Society*, 20(1), 45-60.
- Sunshine, J., Egelman, S., Almuhiemedi, H., Atri, N., & Cranor, L. F. (2009). Crying wolf: An empirical study of SSL warning effectiveness. *USENIX Security Symposium*, 399-416.
- Super, S., Aminuddin, M., & Dom, H. (2016). Comparison of meaningful sound vs no sound for avoiding attention drifting phenomenon while driving. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 8(1), 19-23.
- Tadajewski, M. (2019). Habit as a central concept in marketing. *Marketing Theory*, 19(4), 447-466. <https://doi.org/10.1177/1470593119847251>
- Tang, T., Wang, H., Ma, J., & Zhou, X. (2020, 2020/01/20). Analysis of crossing behavior and violations of electric bikers at signalized intersections. *Journal of Advanced Transportation*, 2020, 1-14. <https://doi.org/10.1155/2020/3594963>
- Terlizzi, M. A., Meirelles, F. d. S., & Viegas Cortez da Cunha, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of Applied Security Research*, 12(2), 224-252. <https://doi.org/10.1080/19361610.2017.1277886>
- Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*, 12(3), 1-23. <https://doi.org/10.5539/10.5539/ijbm.v13n6p1>
- Thompson, H. (2012). The human element of information security. *IEEE Security & Privacy*, 11(1), 32-35. <https://doi.org/10.1109/MSP.2012.161>
- 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>
- Uddin, M., Allen, R., Huynh, N., Vidal, J. M., Taaffe, K. M., Fredendall, L. D., & Greenstein, J. S. (2017). Effectiveness of a countdown timer in reducing OR turnover time. *Journal of Mobile Technology in Medicine*, 6(3), 25-33. <https://doi.org/10.7309/jmtm.6.3.5>
- Vance, A., Jenkins, J. L., Anderson, B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI,



- eye tracking, and field experiments. *MIS Quarterly*, 42(2), 355-380.  
<https://doi.org/10.25300/MISQ/2018/14124>
- Virvilis, N., Tsalis, N., Mylonas, A., & Gritzalis, D. (2014). *Mobile devices: A phisher's paradise*. Proceedings of the 2014 11th International Conference on Security and Cryptography, Vienna, Austria.
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146-1166.  
<https://doi.org/10.1177/0093650215627483>
- Volkamer, M., Renaud, K., Reinheimer, B., Rack, P., Ghiglieri, M., Mayer, P., Kunz, A., & Gerber, N. (2018). *Developing and evaluating a five minute phishing awareness video*. Proceedings of the International Conference on Trust and Privacy in Digital Business, Regensburg, Germany. [https://doi.org/10.1007/978-3-319-98385-1\\_9](https://doi.org/10.1007/978-3-319-98385-1_9)
- Vranas, P. B. (2000). Gigerenzer's normative critique of Kahneman and Tversky. *Cognition*, 76(3), 179-193.
- Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 17(11), 759 – 783.  
<https://doi.org/10.17705/1jais.00442>
- Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9, 11895-11910. <https://doi.org/10.1109/ACCESS.2021.3051633>
- Wash, R., & Cooper, M. M. (2018). *Who provides phishing training? Facts, stories, and people like me*. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montréal, Québec, Canada.  
<https://doi.org/10.1145/3173574.3174066>
- Weanquoi, P., Johnson, J., & Zhang, J. (2018). Using a game to improve phishing awareness. *Journal of Cybersecurity Education, Research and Practice*, 2018(2), 2.
- Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). *What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game*. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, Scotland. <https://doi.org/10.1145/3290605.3300338>
- Wogalter, M. S., Conzola, V. C., & Smith-Jackson, T. L. (2002). Research-based guidelines for warning design and evaluation. *Applied Ergonomics*, 33(3), 219-230. [https://doi.org/10.1016/S0003-6870\(02\)00009-1](https://doi.org/10.1016/S0003-6870(02)00009-1)

- Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, 16(5), 463-483.  
<https://doi.org/10.1108/09685220810920549>
- Wu, L., Du, X., & Wu, J. (2014). *MobiFish: A lightweight anti-phishing scheme for mobile phones*. Proceedings of the 2014 23rd International Conference on Computer Communication and Networks (ICCCN), Shanghai, China.
- Yan, J., Qiao, Y., Yang, J., & Gao, S. (2015). *Mining individual mobile user behavior on location and interests*. Proceedings of the 2015 IEEE International Conference on Data Mining Workshop, Atlantic City, NJ, United States.  
<https://doi.org/10.1109/ICDMW.2015.122>
- Zhang, Y., & Kumada, T. (2017). Relationship between workload and mind-wandering in simulated driving. *PloS one*, 12(5), 1-12.  
<https://doi.org/10.1371/journal.pone.0176962>
- Zweighaft, D. (2017). Business email compromise and executive impersonation: Are financial institutions exposed? *Journal of Investment Compliance*, 18(1), 1-7.  
<https://doi.org/10.1108/JOIC-02-2017-0001>