Scholar Commons
USF University of South Florida

University of South Florida
Scholar Commons

Graduate Theses and Dissertations

Graduate School

March 2019

Phishing in Dark Waters: A Quasi-Experimental Approach with Evaluating Cyber-Security Training for End-Users

Jaclyn Martin
University of South Florida, jaclyn.martin28@gmail.com

Follow this and additional works at: https://scholarcommons.usf.edu/etd

Part of the Cognitive Psychology Commons

Scholar Commons Citation

Martin, Jaclyn, "Phishing in Dark Waters: A Quasi-Experimental Approach with Evaluating Cyber-Security Training for End-Users" (2019). *Graduate Theses and Dissertations.*
https://scholarcommons.usf.edu/etd/8388

This Dissertation is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

المنارة للاستشارات

www.manaraa.com

Phishing in Dark Waters:

A Quasi-Experimental Approach with Evaluating Cyber-Security Training for End-Users

by

Jaclyn Martin

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Psychology
College of Arts and Sciences
University of South Florida

Major Professor: Michael D. Coovert, Ph.D.
Chad Dubé, Ph.D.
Walter C. Borman, Ph.D.
Stephen E. Stark, Ph.D.
Logan M. Steele, Ph.D.

Date of Approval:
March 27, 2019

Keywords: training evaluation, phishing susceptibility, cyber-security, signal detection theory

Copyright © 2019, Jaclyn Martin

www.manaraa.com

DEDICATION

This dissertation is dedicated first and foremost to my incredible parents and first teachers, Susanna Stickle, Ron Martin, and Staci Martin. I want to take this opportunity to sincerely thank you for teaching me what books could not. I would not be where I am today without your constant and endless love and support. I would also like to dedicate this work to Nathan Kowal who has been by my side since my first year of graduate school and was always eager and ready to celebrate every triumph and to motivate me to overcome every challenge. You never complained when I needed to work nights, weekends, and holidays and you never failed to make me smile and help me put everything into perspective. I thank you for your all your understanding and encouragement. Lastly, it is dedicated to my siblings, Ron Martin, Allie Martin, Carter Martin, Emily Chambers, and Carrie Martin, who have supported and inspired me since birth.

www.manaraa.com

ACKNOWLEDGEMENTS

I would like to thank Dr. Michael Coovert, who provided invaluable support and feedback over the past five years of my doctoral study. I greatly appreciate all of his time and effort mentoring me, especially with regard to the countless hours spent ensuring I had opportunities to hone my research skills. Second, I would like to thank Dr. Chad Dubé for answering my endless questions on signal detection theory and providing constant guidance and support throughout my related research efforts in graduate school. Additionally, I would like to thank my committee members, Dr. Stephen Stark, Dr. Walter Borman, and Dr. Logan Steele for their valuable feedback and direction. I would like to thank Dr. Chris Young, from the Texas Department of Transportation (TxDOT) for reaching out to me about collaborating on this work and providing and coordinating the TxDOT workforce as a sample for the research. His dedication to the scientist-practitioner model made this collaboration and this work possible. I also greatly appreciate the time dedicated by those in the TxDOT workforce who participated in the research. Finally, I would like to thank Nikki Stoneley and Steph Boettcher for volunteering their time as research assistants to code the email stimuli used in the surveys in this study for phishing email features.

www.manaraa.com

TABLE OF CONTENTS

LIST OF FIGURES iii

LIST OF TABLES iv

CHAPTER ONE: INTRODUCTION 1
- The Human Element in Cyber-security 2
  - The Quantification of Phishing Susceptibility 10
    - Self-Report 11
    - Simulated Attacks 12
    - Signal Detection Theory 13
- The Current State of End-User Phishing Email Awareness Training 20
  - Rule-Based Training 21
  - Fear Appeals 22
- The Science of Training 25
  - Training Needs Assessment 26
  - Training Design and Delivery 27
  - Training Evaluation 29
  - The Larger Training Context: The Influence of Individual Differences 30
- Hypotheses 32

CHAPTER TWO: METHOD 36
- Participants 36
- Procedure 37
- Measures 39
  - Training Evaluation Measures 39
    - Trainee Learning Outcomes: Phishing Susceptibility 39
    - Trainee Reactions 41
  - Cognitive Ability 41
  - Demographics 41

CHAPTER THREE: RESULTS 43
- SDT Analyses 43
  - Model Fitting 43
  - Calculation of SDT Metrics 52
- Hypothesis Testing 54

CHAPTER FOUR: DISCUSSION 63
- Implications 67
- Limitations and Future Directions 69

www.manaraa.com

Conclusion 74

REFERENCES 75

APPENDICES 88
Appendix A: Recruitment Email 89
Appendix B: Phishing Susceptibility Measure 90
Appendix C: Email Stimuli 91
Appendix D: Scenario Prompt 127
Appendix E: Trainee Reactions and Training-Related Questions 128
Appendix F: Cognitive Ability 130
Appendix G: Demographics 131
Appendix H: Fear Appeals 135
Appendix I: Message Involvement Items 137
Appendix J: Organizational Commitment Letter 138
Appendix K: IRB Approval Letter 139

www.manaraa.com

LIST OF FIGURES

Figure 1 Cyber Trust Taxonomy 7

Figure 2 Example Phishing Email 8

Figure 3 Example Phishing Email Training Slide 9

Figure 4 Signal Detection Theory Model 16

Figure 5 ROC Curve 19

Figure 6 Model 1: Relaxed Model with the Variances Freely Estimated 46

Figure 7 Model 2: EVDST Model 47

Figure 8 zROC of SDT Predicted Model 49

Figure 9 Adjusted Model with Post-Training Responses with No Misses Removed 50

Figure 10 Adjusted zROC with Post-Training Responses with No Misses Removed 51

Figure 11 Scatterplot of Cognitive Ability and Baseline Phishing Detection Ability 60

Figure 12 Scatterplot of Utility Reactions and Training Effectiveness 61

Figure 13 Scatterplot of Affective Reactions and Training Effectiveness 62

www.manaraa.com

LIST OF TABLES

Table 1 Signal Detection Theory Outcomes 14

Table 2 Email Stimuli Pilot Testing Statistics 40

Table 3 Frequency Stimulus-Response Table 44

Table 4 Proportion Stimulus-Response Table 44

Table 5 Hit and False-Alarm Rates: Cumulative Proportions 45

Table 6 Chi-Square Difference Tests of Model Fit: Equal-Variance 48

Table 7 Stimulus-Response Matrix 52

Table 8 Formulas for Calculation of SDT Statistics for Example Participants 53

Table 9 Summary of SDT Metrics 54

Table 10 Descriptive Statistics for Focal Study Variables 55

Table 11 Correlations among Study Variables 56

Table 12 Training Effectiveness T-tests 58

Table 13 Regression Model Cognitive Ability Predicting Pre-Training Phishing 59

Table 14 Regression Model for Utility Reactions Predicting Training Effectiveness 61

Table 15 Regression Model for Affective Reactions Predicting Training Effectiveness 61

www.manaraa.com

ABSTRACT

With the increasing amount of digital storage of personal and organizational data, there has been an increasing number of cyber-attacks, which has spurred much research on how to reduce phishing susceptibility. However, there are several gaps in the current research. There is little research on the effectiveness of different interventions on phishing susceptibility. There is no research on the differential impact of interventions on sensitivity (ability to detect phishing emails) and response bias (propensity to treat emails as threatening) or the influence of individual characteristics on phishing email training success. This study addresses these gaps using a quasi-experimental approach to evaluate a cyber-awareness training using Signal Detection Theory (SDT) to measure phishing susceptibility on an organizational sample at the Texas Department of Transportation (TxDOT). Informational approaches to training were effective in reducing phishing email susceptibility, however fear-appeals were not effective. Sensitivity and response bias were differentially impacted by the informational approach to cyber-awareness training. Cognitive ability predicted starting phishing email susceptibility and affective and utility reactions predicted training success. Implications and directions for future research are discussed.

www.manaraa.com

CHAPTER ONE: INTRODUCTION

As society becomes ever more reliant on technology, it is increasingly important that employees throughout all industries are aware of cyber-security issues. Employees have access to organizational systems and are vulnerable to cyber-attacks that can ultimately cause theft, damage, or disruption to an organizational system's hardware, software, information, or services. An organization's employees have the greatest potential to defend the organization from cyber-attacks. While technological defenses and the teams of cyber-security professionals who implement and manage the systems are necessary to an organization's continued security, those precautions are not sufficient. With ever-evolving threats and the ability for insiders to open up system vulnerabilities (either intentionally or unintentionally), technological defenses cannot completely secure an organization's systems.

Psychological research can provide insights for leveraging the human capabilities needed to improve cyber-security defenses. Social engineering used in phishing scams involves exploiting end-users' trust in order to gain access to a system. An understanding of human cognition and the different influences on human behavior can improve both the evaluation of training programs and the overall effectiveness of the intervention. The evaluation of phishing training programs can be improved with more precise measurement of end-users' phishing susceptibility through the application of a cognitive model for decision-making, signal detection theory (SDT; Green & Swets, 1966). Training effectiveness can be improved through the use of psychological interventions designed to improve end-users' affective, behavioral, and cognitive learning outcomes (Kraiger, Ford, & Salas, 1993).

www.manaraa.com

The current study aims to utilize psychological research to reduce individuals' phishing susceptibility. First, I outline the quasi-experimental study used to evaluate the effectiveness of different interventions on phishing susceptibility. Firstly, I provide background on the human element of cyber-security including susceptibility to social engineering attacks, such as phishing. Secondly, I review the literature on the measurement of phishing susceptibility. Thirdly, I present a summary of the current state of phishing email training as well as the literature on the components of effective employee training. Next, the hypotheses for this work are presented, followed by the method, including details about the Texas Department of Transportation (TxDOT) sample and the quasi-experimental study design. Then, the analyses that were used following data collection are presented. Finally, a discussion section covering the practical and theoretical implications of this work and the limitations and future directions is presented.

The Human Element in Cyber-security

Cyber-security professionals often cite humans as the "weakest link" in an organization's cyber-security chain (e.g., Arce, 2003; Lineberry, 2007; Nohlberg, 2009; Sasse, Brostoff, & Weirich, 2001). Bruce Schneier, an internationally renowned security technologist, wrote on the field of cyber-security;

> "...the mathematics are impeccable, computers are vincible, the networks are lousy and the people are abysmal. I've learned a lot about the problems of securing computers and networks, but none that really helps solve the people problem" (Schneier, 2000).

Since adversaries typically use social engineering tactics to exploit users' trust and gain access to systems, it is easy to understand why cyber-security is a "people problem" rather than merely a technological problem.

www.manaraa.com

A popular phishing training company cofounded by Kevin Mitnick (a famous hacker), called *KnowBe4*, reported that in a sample of over 6 million end-users and across more than 11,000 organizations, the average phish prone percentage (calculated based on end-user behavior during a simulated phishing attack) was 27% (Sjouwerman, 2018). With the average cost of a successful phishing attack to a mid-sized company being $1.6 million (PhishMe, Inc., 2017), having more than one in four employees vulnerable to phishing attacks poses a substantial threat to organizations.

Employee vulnerability statistics are especially alarming given the common security mantra, "it's not *if* you'll be attacked, but *when*." According to Wombat Security's State of the Phish report (Wombat Security Technologies, 2018), which surveys over 10,000 information security professionals, 76% of organizations surveyed said they experienced phishing attacks in 2017. Moreover, on average, 53% of information security professionals reported experiencing spear-phishing, a more targeted form of phishing.

How does phishing work? Social engineers send emails pretending to be someone (e.g., an IT person from your organization) or something (e.g., Gmail) they are not, in order to extract sensitive information out of their target. Their approach is to gain trust from the end-user in order to retrieve the targeted information. Some tactics include attempts to elicit fear, curiosity, or a sense of urgency out of the end-user to bypass or expedite a target's typical decision-making process for determining the legitimacy of emails. Recent surveys suggest the success rate of different tactics has changed in recent years. Specifically, PhishMe reported that the emotional motivators commonly used in phishing emails that previously held the highest end-user response average (i.e., fear, urgency, and curiosity) were outpaced by entertainment, social, and reward motivators (PhishMe, Inc., 2017).

www.manaraa.com

These tactics to elicit the end-user's trust are applied through certain email design features. Staggs and colleagues (2014) proposed a perceptual taxonomy with three types of design features that influence an end-user's cyber trust:1) **content**, 2) **context**, and 3) **contract** (see Figure 1). The **content** features are specific to emails and include: 1) *graphics*, 2) *URL links*, 3) *attachments*, and 4) *signatures*. Email *graphics* can foster suspicion when logos are altered or of poor quality. Alternatively, phishing emails that include logos that are of high quality and appear legitimate can increase a user's trust in the email. *URL* (Universal Resource Locators) *links* included in phishing emails can be obfuscated through the use of tiny URLs, which can make the link appear more legitimate to end-users. URL misdirection is a common tactic for leading users to compromised web pages. For instance, a phishing email may contain a link that appears to be the Facebook login page, when in reality, it takes the user to a phony site that collects the user's information. Social engineers use this approach since URLs that end in a risky domain name may decrease a users' trust in the email. Moreover, URLs that link to immediately download a file or start an executable are also cause for suspicion. Email *attachments* represent a hazardous cue when the logo or file extension is identified as risky. For instance, file attachment logos or extensions that show an executable file (.exe) indicate it is risky to download the attachment. As with the graphics, when visual trickery is used to deceive users into thinking the file is familiar or safe, it can increase a user's trust in the email. Finally, the email *signature* is another design feature that concerns the content of the email. The absence of an email signature may cause suspicion of the email. Further, the presence of an email signature that is unfamiliar or inconsistent with what the user expects can signal the user to suspect malicious intent.

www.manaraa.com

The **context** features identified for emails are: 1) *origin*, 2) *tone*, and 3) *language* (Staggs et al., 2014). *Origin* refers to the sender of the email. Like the URL links in content, the sender address can alert the end-user to malicious intent when the address ends in a risky domain name. *Tone* refers to the way the email is written to address the recipient. For instance, if the greeting were formal, the email would convey a more professional tone. If the greeting was informal, but the sender is unknown, this could cause the end-user to be suspicious of the email. Likewise, a professional tone when it appears to be coming from a familiar address may be suspicious. Another aspect of tone is the sense of urgency conveyed in the message. Often, in phishing emails, social engineers design the email to create a sense of urgency to influence the recipient to reveal sensitive information. For instance, phishing emails that appear to be from IT often claim that the end-user's password will expire in a number of days if action is not taken. *Language* represents another part of the context that can cause suspicion in email communication. When an email is riddled with spelling or grammar errors, it could indicate to an end-user that the email is suspicious. Thus, the context with which the email was sent is an important determinant for the end-user's trust propensity.

The third and final type of features that influence end-user's trust in an email are the **contract** features, which include: 1) *offer*, 2) *consideration*, and 3) action. *Offer* focuses on what the sender is claiming to provide the recipient in exchange for information. Phishing emails often promise large sums of money and/or access to sensitive information. These offers can also alert the end-user to malicious intent. *Consideration* involves the persuasion used to request information from the end-user. For instance, oftentimes phishing emails will request information, such as login credentials. *Action* involves urging the recipient to take some action that will allow the social engineer access to their system. For instance, phishing emails often include urges to

www.manaraa.com

verify credentials, click URLs, or download attachments. Figure 2 displays an example phishing email with several of the reviewed phishing design features included.

Many cyber awareness training programs incorporate informational curriculum on the design features of phishing emails in order to educate employees on how to recognize phishing emails. For instance, the Texas Department of Transportation's (TxDOT) cyber awareness training provides information on how to hover over URLs and identify suspicious links (content: URL links), to check that the signature appears normal (content: signature), to recognize generic salutations (context: origin), to be wary of the use of urgent tone (context: tone), to watch for odd phrasing, bad grammar, or incorrect spelling (context: language), to be wary of emails requiring immediate action (contract: action), and to recognize emails that contain unusual requests (contract: consideration). Thus, the only design features from Staggs et al.'s (2014) taxonomy that are not explicitly covered in the TxDOT training are the content features of suspicious graphics and attachments. Figure 3 provides an example slide from the TxDOT training where the above design features are covered.

www.manaraa.com

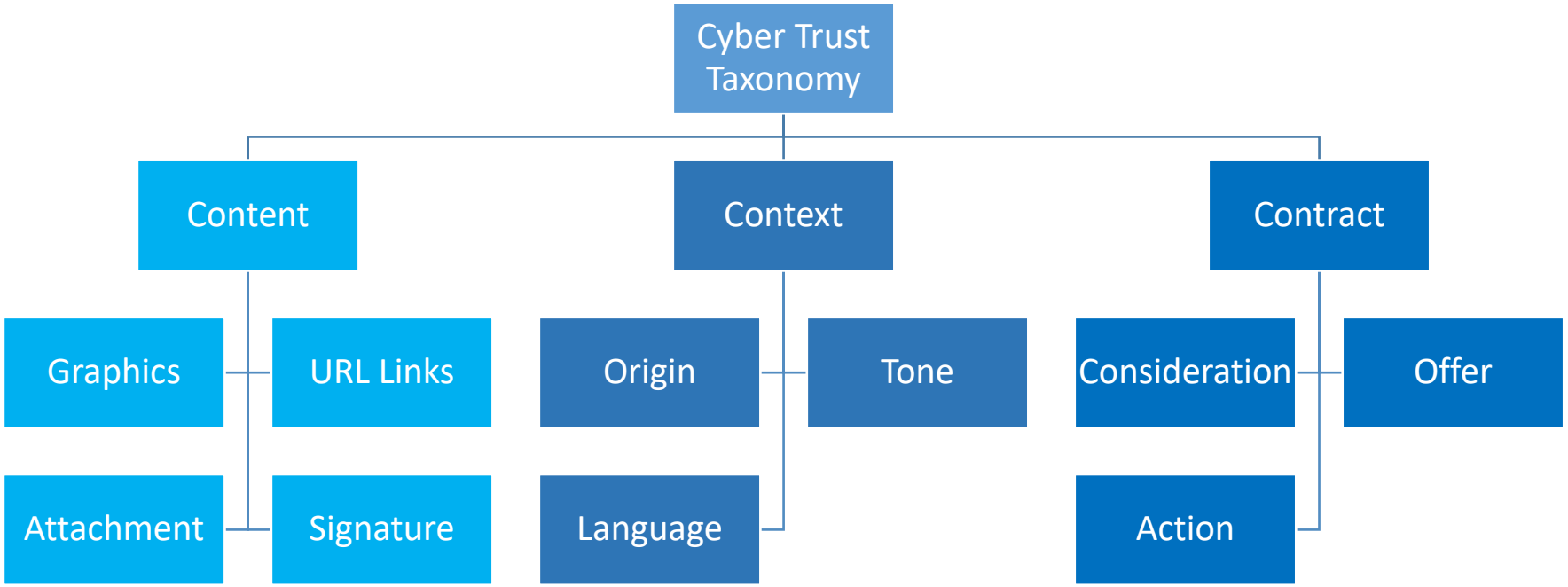


Figure 1. Staggs et al.'s (2014) cyber-trust taxonomy adapted to include only email design features (excludes web or social network specific design features).

www.manaraa.com

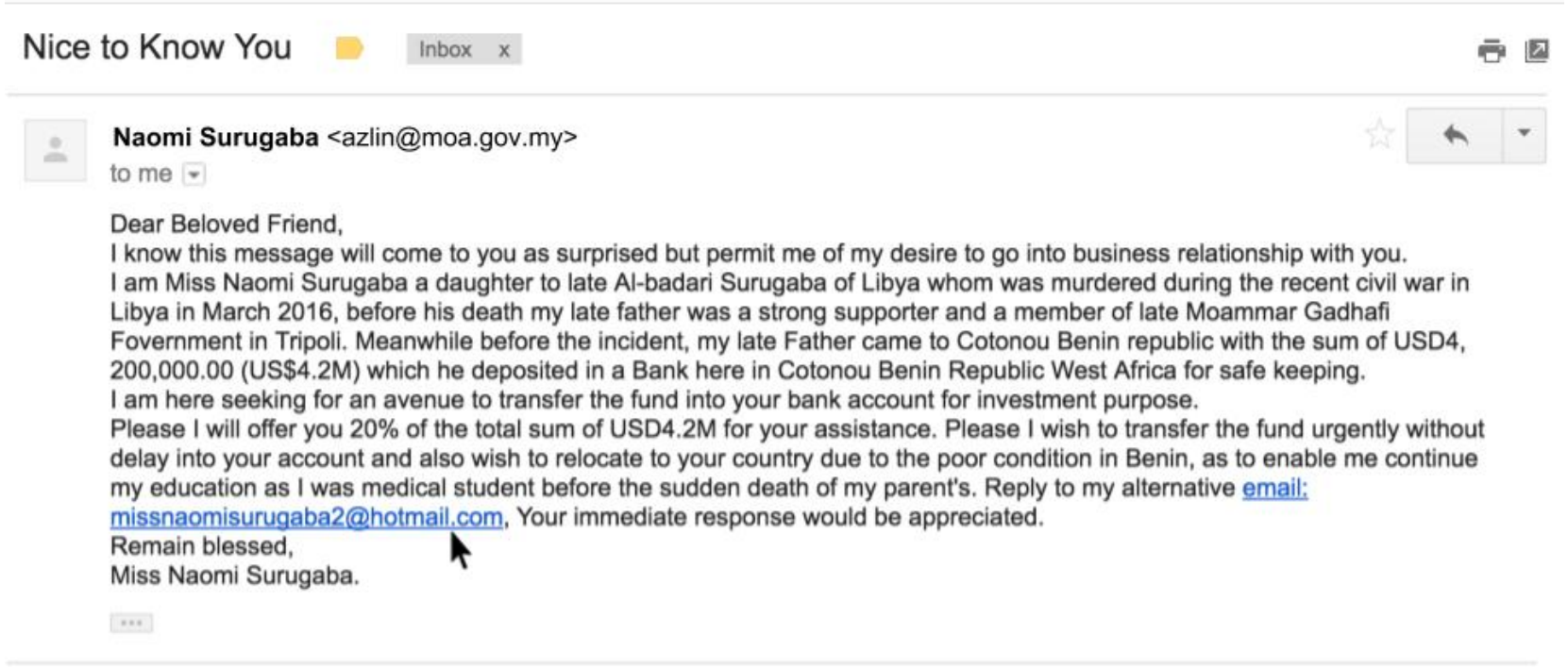


Figure 2. Phishing email with several phishing design features, including; suspicious URL link, origin, tone, language, consideration, offer, and action.

www.manaraa.com

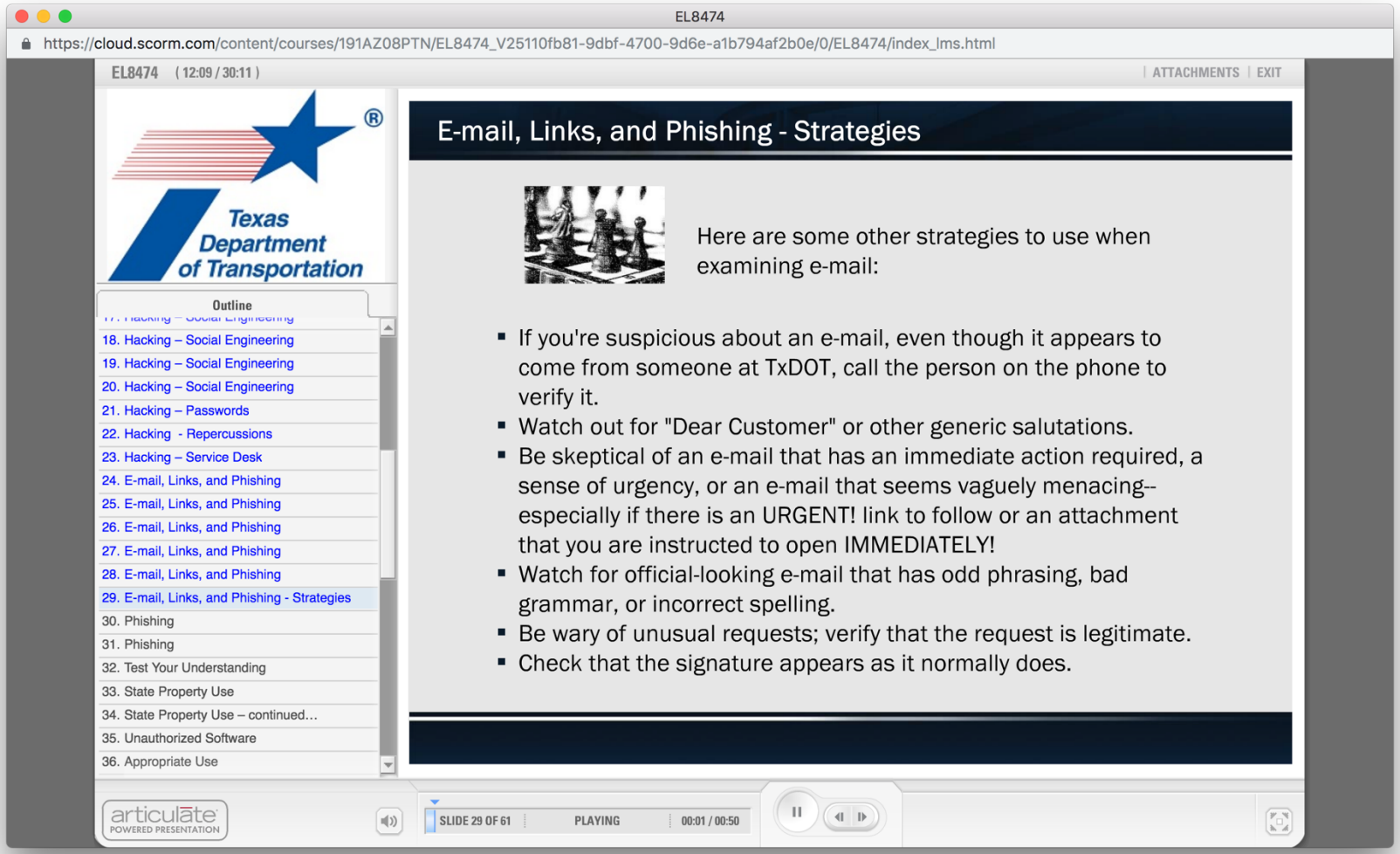


Figure 3. TxDOT Phishing Email Training Slide Covering Email Design Features.

www.manaraa.com

This section provided an overview of the human element in cyber-security and details on how phishing emails are used to exploit end-user trust and gain access to organizational systems. Phishing emails are an effective method for opening vulnerabilities in an organization's systems via social engineering of the organization's employees because phishing is easy and profitable for attackers. Phishing emails are easy and inexpensive to create with virtually no cost to the attacker and as long as one recipient falls for the phishing scam, it provides the attacker with the ability to target the recipient, other employees and/or the organization as a whole. While the design features of phishing emails and the nature of the targeting will likely continue to evolve as attackers become smarter and technology allows for the faster and more effective gathering of target background information and personalization of email content, the basic approach will likely remain the same due to the underlying psychological manipulation.

Social engineering has been used as a tactic to gain target's trust long before technology changed the way we store and safe-guard information. For centuries, Con Artists utilized the same psychological manipulations to gain targets' trust and persuade them to divulge confidential information. The term, "confidence man" (colloquially shortened to con man), dates back to the early 1800s and is used today with great frequency. It follows that the best defense to the psychological tactics used in social engineering involves employing psychological principles to arm the most important link in an organization's cyber-security defense—the humans. The following section will review how the human element of an organization's cyber-security defense is measured in terms of phishing susceptibility.

The Quantification of Phishing Susceptibility

Organizations recognize the importance of a baseline assessment of employee phishing susceptibility. Wombat Security's State of the Phish report states that in 2017, 76% of

www.manaraa.com

organizations surveyed reported they measure their organization's susceptibility to phishing. However, there is no standard assessment for measuring phishing susceptibility. There have been several different measures of phishing susceptibility used both in research and in practice. This section will review different ways to quantify phishing susceptibility.

Self-Report. There have been several self-report scales used to measure phishing susceptibility (e.g., Chuchuen & Chanvarasuth, 2015; Harrison, Vishwanath, & Rao, 2016; James, Boyle, & Bennett, 2014; Sudzina & Pavlicek, 2017). James and colleagues (2014) used the susceptibility to scams scale, a five-item self-report measure where participants rated their agreement to five statements indicating their willingness to trust others and their wariness of scams. Sudzina and Pavlicek (2017) simply measured propensity to click on suspicious links with one question, "Would you click on suspiciously advantageous offer if it led to a deal site?" and Likert scale response options for indicating the likelihood. In another study, researchers looked at a self-reported measure of email trust where respondents were presented with a phishing email and asked on a Likert scale with a single item to rate the extent to which they agreed that they trusted the email (Harrison et al., 2016). Self-report measures of behavioral tendency similar to those described above are limited in that they do not capture a person's ability to detect phishing emails.

Other measures of phishing susceptibility focus on self-reported behavioral intention for given scenarios. For instance, several researchers have created scenarios or simulated email tasks where participants indicate how they would respond to the email in the given scenario (e.g., Albladi & George, 2017; Curtis, Rajivan, Jones, & Gonzalez, 2018; Lawson, Zielinska, Pearson, & Mayhorn, 2017; Martin, Dubé, & Coovert, 2018; McBride, Carter, & Warkentin, 2012; Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2011). Typically, participants were given

www.manaraa.com

a scenario description and several emails to read through and respond to. They were given a variety of safe and unsafe behavioral response options for each simulated email scenario, such as: reply to email, forward the email, click the link in the email, leave the email in the inbox and flag for follow up, leave the email in the inbox, delete the email, or delete the email and block the sender.

Simulated Attacks. Other researchers use actual simulated phishing attacks by sending participants phishing emails to their personal or work email account and recording how many participants open the email, click on the link, and/or provide the information requested in the email (e.g., El-Din, Cairns, & Clark, 2014; Halevi, Lewis, & Memon, 2013; Halevi, Memon, & Nov, 2015). This method involves deception, in that the participants are unaware that the email is related to the study (i.e., the email is sent outside the formal context of the study/experiment). Data obtained in this fashion are likely a more valid reflection of real-life phishing scenarios. Still, there are obvious ethical considerations with the use of this methodology for collecting data on phishing susceptibility and great care should be used when this is used in practice and research settings. Many organizations have their IT departments "self-phish" their employees in order to get a metric for phishing susceptibility. This is the method that KnowBe4 used on the over 11,000 organizations included in their study evaluating the effectiveness of their phishing email training on phishing susceptibility (Sjouwerman, 2018). Some companies even use these methods to publicly reward or reprimand employees based on who reports or falls for the fake phishing attacks (Sjouwerman, 2018). Though some argue these mock phishing attacks offer a safe way to expose vulnerabilities (Beyer & Brummel, 2015), there is no research on the effects self-phishing has on end-users' trust of the IT department, self-efficacy, or other important variables that are likely affected by continuous self-phishing.

www.manaraa.com

There are several ways to quantify the information from the behavioral responses based on scenarios or simulated phishing attacks into a measure of a person's phishing susceptibility. Some researchers have used false positives (the percentage of genuine emails flagged as phishing) and false negatives (the percentage of phishing emails treated as genuine emails) as measures of phishing susceptibility (e.g., Pendleton, Garcia-Lebron, Cho, & Xu, 2016; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). Most researchers simply calculate end-users' accuracy in responding to threatening emails (e.g., percentage of correct responses to phishing emails). The typical accuracy measures are limited in that they ignore the fact that behavior related to phishing emails occurs as part of a cognitive process that is influenced by expectancy factors.

Signal Detection Theory. Recently, several studies have applied the statistical framework provided by Signal Detection Theory (SDT)(Green & Swets, 1966) to measure phishing susceptibility (Canfield et al., 2017; Canfield, Fischhoff, & Davis, 2016; Canfield & Fischhoff, 2018; Martin et al., 2018; Mayhorn & Nyeste, 2012; Nguyen, 2018, 2018; Sheng et al., 2007). SDT allows for the separation of sensitivity and bias as factors explaining behavior (Green & Swets, 1966; Lynn & Barrett, 2014; Macmillan & Creelman, 2004). Sensitivity represents a person's ability to detect phishing emails or their ability to distinguish between phishing emails and legitimate emails. Response bias is the propensity to be liberal or conservative with regard to treating emails as threatening (responding safely versus unsafely). It is important to separate sensitivity and response bias in phishing susceptibility because the two are independent. Sensitivity is influenced by how easily a stimulus can be detected from noise whereas response bias is influenced by expectations of the likelihood and/or costs of different outcomes.

www.manaraa.com

Through the SDT model, if you present a person with a signal (e.g., phishing emails) and noise (e.g., non-threatening or legitimate emails) and collect the person's responses based on the stimulus presented (e.g., click on link in email, forward to IT), the framework can be used to compute a person's sensitivity to the stimuli (i.e., ability to detect phishing emails) and their response bias (i.e., propensity to treat emails as if they are threatening). Based on whether the responses indicated that the individual perceived a stimulus or noise and whether or not a stimulus was present, responses are categorized into one of four different outcomes: respond as if the signal is present when it is present (hit); respond as if the signal is present when it is absent (false alarm); respond as if the signal is absent when it is absent (correct rejection); and respond as if the signal is absent when it is present (miss) (see Table 1). Over several trials with either the stimulus present or absent, responses are collected and the hit rate (*HR*; the probability of detecting a stimulus when it is present) and false alarm rate (*FAR*; the probability of detecting a stimulus when it is absent) are calculated as follows:

$$\text{Eq. 1: } HR = \frac{\#\ of\ hits}{\#\ of\ phishing\ emails\ presented}$$

$$\text{Eq. 2: } FAR = \frac{\#\ of\ false\ alarms}{\#\ of\ legitimate\ emails\ presented}$$

Table 1. Signal Detection Theory Outcomes

	Respond "Absent" (e.g., reply to email)	Respond "Present" (e.g., delete email)
Signal Present (phishing email presented)	Miss	Hit
Signal Absent (legitimate email presented)	Correct rejection	False Alarm

Sensitivity, or d' (d-prime), can then be calculated as the difference between the inverse normal cumulative distribution functions of the HR and FAR (Macmillan & Creelman, 2004). D-

www.manaraa.com

prime is the difference between the means of the signal and noise distributions (see Figure 4). Thus, an individual who has a large sensitivity to the stimulus (e.g., someone who is very good at identifying phishing emails) will have a larger divide between their signal and noise distributions. That is, they can more easily discriminate between a signal and noise and therefore, the signal and noise distributions have less overlap.

Eq. 3: $d' = z(HR) - z(FAR)$

A person's response bias, or decision criterion, represents the cutoff point for the decision to respond as if the signal is present or absent. If the signal strength is great enough to where it is to the right of the criterion in Figure 4, the individual would respond as if the signal were present. In the example in Figure 4, the noise and signal distributions overlap enough to where sometimes the individual would be correct to respond as if the signal were present (hit), but other times, they would be responding to noise (false alarm). Still, as the signal strength increases, it is more likely that responding as if a signal is present will result in a hit. In the measurement of phishing susceptibility, the decision criterion would represent the threat level at which an individual would respond as if the email were a phishing email. For instance, the typical Nigerian Prince email (like the one in Figure 2) has enough phishing design features that the signal strength, or threat level, is great enough to exceed the individual's decision criterion and they would respond as if the email were threatening (e.g., delete the email, notify IT, etc.).

Eq. 4: $c = .5[z(HR) + z(FAR)]$

www.manaraa.com

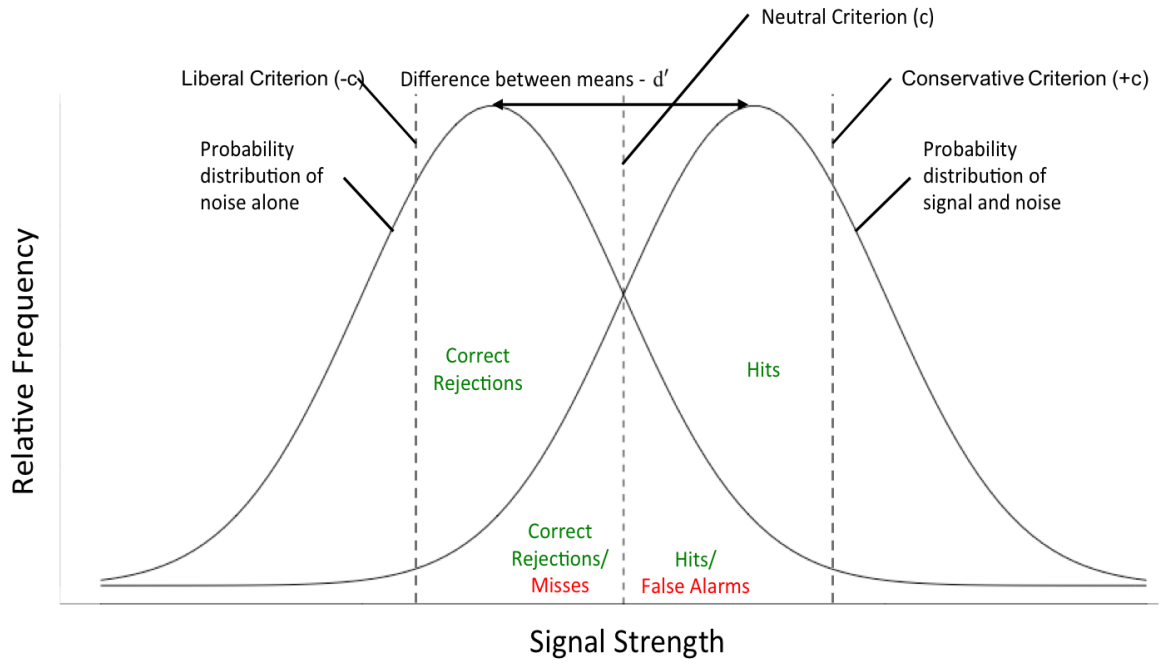


Figure 4. Signal Detection Theory Model.

When a person's criterion shifts from the neutral position, it indicates either a liberal response bias (to the left of the neutral position) or a conservative response bias (to the right of the neutral position). A liberal response bias indicates that the person has a greater propensity to respond as if a signal is present. Thus, response bias is measured as the distance between the criterion and the point at which the signal and noise distributions intersect. In the context of phishing emails, this would reflect a person who is more likely to respond with safe behaviors (forward an email to IT, delete the email, etc.). On the other hand, a conservative response bias indicates a greater propensity to respond as if there is no stimulus. That is, the individual would be more likely to respond with unsafe behaviors (e.g., reply to the sender, download the attachment, click on the link in the email, etc.).

Two variables are known to influence response bias: 1) payoff perceptions, which are an individual's perceptions of the costs and benefits associated with each of four possible decision

www.manaraa.com

outcomes (correct detections, missed detections, false alarms, and correction rejections) and 2) base-rate, which is the probability of targets relative to noise (Green & Swets, 1966; Lynn & Barrett, 2014; Macmillan & Creelman, 2004).

Payoff perceptions influence employees' cyber-security compliance in that an individual's perception that misses (e.g., the threat of cyber-attack) are costly promotes a smaller response bias for judging that a target is present. This bias would make employees more likely to treat emails as if they are threatening or they need to be more alert/vigilant when responding to emails. An extreme example would be a paranoid employee who scrutinizes each email for any indication of a threat. Alternatively, the weightless, abstract nature of data loss through security breaches or excessive trust in their organization's IT security may lead employees to underestimate the cost of misses, resulting in a conservative bias, where employees would be less likely to treat emails as threatening. Similarly, the perception that false alarms (e.g., hindering productivity by spending too much time evaluating and verifying emails) are costly promotes a more conservative response bias.

Typically, due to the volume of legitimate emails and the recent use of automatic screening software, the prevalence rate of phishing emails is very low (<1%) (Canfield et al., 2016). A low base rate of the stimulus typically results in a conservative response bias because people are more likely to identify a stimulus as noise when they know it is unlikely that a stimulus will occur (Lynn & Barrett, 2014). Phishing email base rate cannot realistically be manipulated by organizations unless they were to periodically phish their own employees or allow more legitimate phishing emails past their automatic filters.

In order to optimize performance, organizations need to find a balance and make sure that creating an awareness of the risks does not push employees too far, resulting in increased

www.manaraa.com

vigilance disrupting productivity. For most organizations, they would want employees to be at "relaxed alert" (IBRS adaptation of the Cooper color codes) (Givens, 2004) where the user is aware of their actions and their environment. Text, semantics, nuances of language, sender information from an email that seems wrong will stand out, which can push a user into a higher alert level. This level of readiness keeps employees alert (as opposed to unaware and unprepared) but relaxed so they do not become exhausted from being extra vigilant. Depending on which costs (e.g., employee productivity dollars, cyber-breach dollars) an organization chooses to minimize, companies can calculate an optimal criterion (response bias level) for their cyber-security goals.

Receiver Operating Characteristic (ROC) curves are used to visualize sensitivity and response bias. ROC curves plot the hit rate that would be obtained for every value of false alarm rate, given a certain d' value. When d' is equal to zero, it indicates that performance is at chance level, or the decision-maker has no ability to distinguish between the two signals (see the line labeled "$d' = 0$" in Figure 5). As the ability for the decision-maker to distinguish between signal and noise increases, the curves shift toward the upper left corner, where accuracy is maximized, or the hit rate is always greater than or equal to the false-alarm rate (labeled "$d' = 3$" in Figure 5). ROC points are typically calculated through having participants rate their confidence in their decision for each stimulus (Wixted, 2007, p. 153). Response bias can be visually evaluated by looking at where the ROC points fall along the curve. Points that are further toward the top right corner of the ROC plot indicate a liberal bias where the respondent has both a high hit rate and high false alarm rate, indicating they are more likely to respond as if the signal is present, regardless of the stimulus (see blue points in Figure 5). On the other hand, points that are closer to the bottom left corner of the ROC curve indicate a conservative response where there is both a

www.manaraa.com

low hit rate and low false alarm rate, indicating the respondent was more likely to respond as if the signal was absent regardless of the stimulus (see red points in Figure 5 ROC curves are also used to determine SDT model fit to the observed data. The closer the observed data points are to the SDT generated curve, the better the SDT model fits the data. The fit can be empirically evaluated using a chi-squared test of model fit (see the analysis section for more detail).

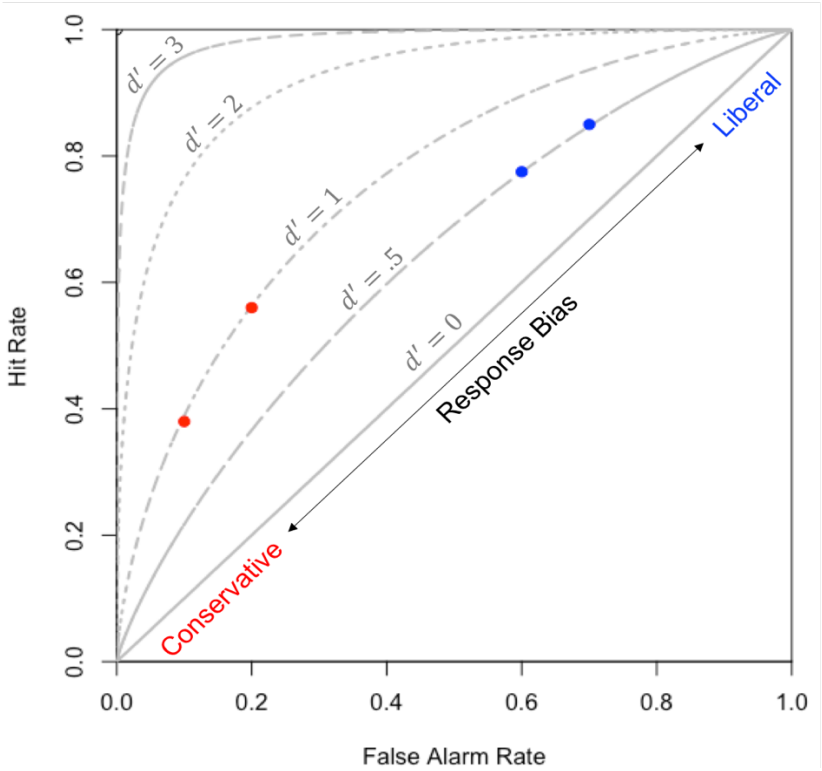


Figure 5. ROC Curve

Overall, SDT is useful for assessing an individual's ability to detect phishing emails (sensitivity) and their propensity to respond safely to emails (response bias). SDT statistics provide a superior quantification of phishing susceptibility because they move beyond the simple calculation of accuracy (e.g., percent correct) by evaluating an individual's perceptual ability to distinguish between threatening and non-threatening emails (sensitivity) and taking into account

www.manaraa.com

other objectives, such as responding to legitimate emails appropriately (i.e., correct rejections) (Canfield et al., 2016). With the calculation of d-prime, "SDT accommodates the inevitable trade-off between hit rates (*H*, correctly identifying a signal) and false-alarm rates (*FA*, incorrectly identifying noise as signals)" (Canfield et al., 2016 p. 1159).

SDT metrics also allow for the incorporation of expectancy factors through the calculation of response bias. Response bias is influenced by a person's perceptions of the costs of different outcomes and their perception of the base rate occurrence of the stimuli. By quantifying performance, SDT offers metrics for analyzing individuals' vulnerability as well as for designing and evaluating interventions to reduce it, such as training and incentives. For instance, a large tech company in Tampa, Florida rewards employees for detecting their IT's phishing emails with a notification congratulating them on finding the phishing email. Moreover, if they find a legitimate phishing email, they are rewarded with $50. SDT could capture the effect these incentives have on employees' response bias.

This section summarized the different measures used for phishing susceptibility and the many benefits and previous research associated with operationalizing phishing susceptibility through SDT. The next section will review how training interventions can be used to reduce phishing susceptibility.

The Current State of End-User Phishing Email Awareness Training

Many organizations recognize that all employees who use the organization's networks must be trained on the knowledge, skills, and policies related to cyber-security (Beyer & Brummel, 2015). The State of the Phish report states that 95% of those surveyed report that their organization trains end-users on how to identify and avoid phishing attacks (Wombat Security Technologies, 2018). Still, only 54% of information security professionals surveyed reported that

www.manaraa.com

they have been able to quantify a reduction in phishing susceptibility based on their training activities (Wombat Security Technologies, 2018).

There are several different types of training that have been studied as interventions to reduce phishing susceptibility. Most training programs include educational elements aimed at reducing phishing susceptibility through teaching end-users how to identify phishing emails and how to respond to them. Additionally, several researchers have evaluated the effects of fear-based elements, which aim to increase end-user motivation to identify and respond safely to phishing emails. Moreover, one study evaluated the effectiveness of incorporating elements of mindfulness training to teach users to take the time to pause and critically evaluate emails before responding (Nguyen, 2018).

Rule-Based Training

One type of training that organizations use to reduce phishing susceptibility includes providing informational training ranging from simple lists of internet tips for users to information on specific design cues to look out for (like with the TxDOT training previously reviewed) to cartoons that help explain tips in a story format (Anti-Phishing Phil; Sheng et al., 2007) to game-based phishing training that sends test emails to individuals, providing feedback for correct and incorrect responses to phishing emails (PhishGuru; Kumaraguru et al., 2007). These educational training programs can be referred to as *rule-based training*, where end-users are instructed to apply sets of rules to received emails in order to identify and correctly respond to the emails (Jansen, 2018; Nguyen, 2018). For instance, the TxDOT training instructs end-users to look out for emails with generic salutations (e.g., “Dear friend,”). If the end-user is suspicious of the email, they are instructed to “Play IT Forward” by forwarding the email to IT to find out if it is safe.

www.manaraa.com

Rule-based training has demonstrated effectiveness in reducing phishing susceptibility in several studies (Alnajim & Munro, 2008, 2009; Kumaraguru et al., 2009, 2007; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010; Mayhorn & Nyeste, 2012; Sheng et al., 2007). Alnajim and Munro (2008, 2009) found certain tips regarding phishing websites (e.g., "Type in your browser the address of the site you intend to go or use a bookmark that you previously created.") resulted in a small increase in the correct decision rate participants had with regard to submitting their information to phishing websites. Kumaraguru and colleagues (2009) found that the percentage of participants who clicked on phishing links and/or gave information was reduced by almost 20% using the Anti-Phishing Phil training and that the knowledge from the training was retained even after 28 days.

Fear Appeals

One successful avenue for training in security research appears to be through the use of *fear appeals*. Research, including two recent meta-analyses (Sheeran, Harris, & Epton, 2014; Tannenbaum et al., 2015), have shown that risk appraisals, which increase individuals' awareness of potential threats and their sense of vulnerability to harm, have a large influence on attitudes, intentions, and behaviors. Fear appeals are intended to arouse fear in their audience by emphasizing the danger in not following the guidelines or recommendations laid out in the message (Tannenbaum et al., 2015). The influence of fear appeals is grounded in protection motivation theory (Maddux & Rogers, 1983), which stipulates that protection motivation, or the intention to act cautiously, is initiated by the threat appraisal process where individuals evaluate their perceived vulnerability and the severity of the consequences of the threat (Jansen & van Schaik, 2018). Thus, fear appeals motivate individuals to change their attitudes, intentions,

www.manaraa.com

and/or behaviors in order to reduce their perceived vulnerability and the perceived threat of harmful consequences.

This effect has been demonstrated in a variety of contexts, including many health-related topics (Anand-Keller, 1999) such as reckless driving (Lewis, Watson, Tay, & White, 2007), dental care (Evans, Rozelle, Lasater, Dembroski, & Allen, 1970), tanning (Cooper, Goldenberg, & Arndt, 2014), and smoking (Thompson, Barnett, & Pearce, 2009). Research demonstrates that fear appeals can also influence energy consumption (Hass, Bagley, & Rogers, 1975) and advertising (Henthorne, LaTour, & Nataraajan, 1993). The use of fear appeals is also pervasive in the area of information security, with studies surrounding the influence of fear appeals on protective security behaviors such as creating stronger passwords, complying with IT procedures, and protecting organizational information assets (Boss, Galletta, Lowry, Moody, & Polak, 2015; Sasse et al., 2001; Vance, Eargle, Ouimet, & Straub, 2013; Wall & Buche, 2017). A recent study used these principles to test the influence of a fear appeal intervention on precautionary internet behavior (Jansen & van Schaik, 2018). These authors found that fear appeals did predict protection motivation and intentions to perform precautionary behavior (Jansen & van Schaik, 2018).

A couple of recent studies evaluated the influence of fear appeals on phishing email susceptibility. One study found that risk level manipulations during cyber awareness training predicted self-reported secure internet behavior a week after the training occurred (Davinson & Sillence, 2010). Another study reported that increasing a participant's general fear level through three news articles after informational training predicted greater training success when compared with a control condition (Zielinska et al., 2014).

www.manaraa.com

The limitation of the above research on the use of fear appeals to reduce phishing susceptibility is that phishing susceptibility is narrowly measured in the studies. It is unexplored whether the use of fear appeals in phishing email training changes cautionary behavior with regard to emails (response bias) and/or phishing email detection performance (sensitivity). It could be that the awareness of perceived vulnerability and threat level caused by fear appeals maps onto the base rate and expectations of costs that have been shown to influence response bias. However, since sensitivity is resistant to the influence of expectancy factors, perhaps fear appeals have no effect on phishing email detection ability.

On the other hand, there is research that suggests that negative mood states, such as anxiety or fear, promote detail-orientation on primary tasks (De Dreu, Baas, & Nijstad, 2008). In this sense, one could argue that fear appeals, to the extent that they bolster fear and anxiety in their audience, may increase performance arousal and therefore increase phishing email detection performance. This relationship between arousal and performance is well researched, with the general psychological principle of the Yerkes-Dodson effect, which stipulates that performance increases with arousal, but only up to a certain arousal level, at which performance starts to decline (Yerkes & Dodson, 1908). It is unlikely that written fear appeals would cause a high enough arousal level to reach the point at which performance decreases, however it is important to consider the possibility of a non-linear relationship between arousal and performance in the context of phishing email detection.

The distinction between effects on response bias versus phishing email detection has important implications, because an organization must consider the tradeoffs associated with manipulating response bias, such that people respond more safely to all emails. On the positive side, applying safe responses to all emails would invariably reduce phishing susceptibility.

www.manaraa.com

However, there are also certain costs to consider with the increase in false alarms (e.g., reduction in employee productivity, overloading IT personnel with reports of phishing emails).

Overall, the available research on phishing email training is relatively new, sparse, and published primarily in technical journals and conference proceedings (e.g., Alnajim & Munro, 2008, 2009; Kumaraguru et al., 2009, 2009, 2007; Sheng et al., 2010, 2007). Both the evaluation and implementation of cyber-awareness training for end-users could be improved through the application of training research from I-O psychology. The next section will review the science of training found in the I-O psychology literature and applications to cyber-awareness training.

The Science of Training

I-O psychology has a long history of science-based training research dating back to the early 1900s (Bell, Tannenbaum, Ford, Noe, & Kraiger, 2017). The research involved developing and validating techniques for designing, conducting, and evaluating training programs. Salas, Tannenbaum, Kraiger, and Smith-Jentsch (2012) summed up training research with the following statement: "the research on training clearly shows two things: (a) training works, and (b) the way training is designed, delivered, and implemented matters" (p. 74). There have been several meta-analyses focused on employee training and development that provide effect sizes that quantify the effectiveness of training and also show the conditions in which training is most effective (e.g., Arthur, Bennett, Edens, & Bell, 2003; Blume, Ford, Baldwin, & Huang, 2010; Colquitt, LePine, & Noe, 2000; Taylor, Russ-Eft, & Chan, 2005). Goldstein's Instructional Systems Design (ISD) model outlined the essential steps to creating an effective training program; training needs assessment, training design, training delivery, and training evaluation (Goldstein & Ford, 2002). This section will review research from the training literature on these

www.manaraa.com

four steps for creating a training program and how the science of training can be used to implement phishing email training.

Training Needs Assessment

The training needs assessment (TNA) allows for the assessment of characteristics of the job and the trainees and organizational goals and constraints. The purpose of TNA is to ensure that training resources are spent on areas of a demonstrated need. TNA involves analyzing training needs at three levels: the person, job and task, and organizational levels (McGehee & Thayer, 1961). At the person level, the employees' KSAOs are evaluated to determine the areas with the greatest potential for training. At the job level, the nature of the tasks involved is assessed through job analysis techniques. This assessment of the tasks involved can help to inform the content of the training. At the organizational level, the company's objectives and goals are assessed to determine the indicators of organizational effectiveness and any potential barriers to training success, such as organizational support and constraints. Ultimately, the TNA informs the design and delivery of the training program by ensuring that training resources are spent in areas of demonstrated need in terms of which employees need the training, which job tasks need to be improved, and which organizational goals need to be met. Research shows that despite the importance of TNA, only 6% of companies report having done a needs assessment prior to implementing training (Arthur et al., 2003).

TNA is an important consideration for cyber-security awareness training. At the person level, organization's need to evaluate employees' KSAOs related to cyber-security performance in order to get an assessment of the potential for improvement through training. At the job level, it is important to understand how the importance of cyber-security defense differs for different positions. For instance, training on effective cyber-security behaviors may be especially

www.manaraa.com

important for Human Resources employees because their logins can be used to access all of the organization's employee data.

Moreover, it is important to understand where cyber-security fits into different employees' job roles. Often, employees are expected to comply with cyber-security policies even though cyber-security is not part of their job description. The extra-role nature of cyber-security performance can lead to motivational challenges with regard to training. At the job level, it is also important to identify and evaluate the specific tasks or critical work functions for cyber-security defense (e.g., forwarding suspicious emails to IT).

There are also TNA considerations at the organizational level. Companies have different postures related to cyber-security policies (offensive, defensive, strong, intentionally weak, etc.). Some companies choose not to defend themselves (minimal legal compliance) because they can get insurance to cover the costs of breaches. Understanding an organization's security posture is important for ensuring that the training goals are aligned with the organizational goals regarding security.

Training Design and Delivery

Training design involves the creation of the training content, while training delivery involves the method and implementation of the training. The TNA provides the foundational blueprint for the design and delivery of training (Salas et al., 2012). For instance, the job-level of the TNA provides information on which tasks to include in the training content, while the person-level of the TNA provides information on the best mode of delivery considering individual characteristics. Specifically, training is shown to be more effective for older workers when the training is self-paced (Kueider, Parisi, Gross, & Rebok, 2012). The organizational-level of the TNA informs training design and delivery through the organizational resources available

www.manaraa.com

for training development. For instance, there may not be organizational resources available to coordinate and implement a two-week in-person training for all staff on cyber-security awareness.

Effective training involves the key elements of instruction, demonstration, practice, and feedback (Salas & Cannon-Bowers, 2001; Salas et al., 2012). An important consideration for the practice element of training is there should be variability among contextual stimuli, practice frequency, and practice method (Baldwin & Ford, 1988). Through effective training design and delivery, trainees will learn targeted knowledge, skills, and attitudes (KSAs), which will result in changes in cognition, behavior, and affect (Kraiger et al., 1993; Salas et al., 2012).

Effective training will set and communicate objectives for the training, including a statement of what you should be able to do/think/feel after the training (Cascio & Aguinis, 2005). For instance, end-user cyber-security training should include an objective similar to, "Be more vigilant with email by using simple and effective techniques to recognize phishing email scams." Research shows that when trainees understand the objectives, purpose, and intended outcomes of training, learning and transfer outcomes are improved (Noe & Colquitt, 2002). Further, training design increases training effectiveness when the content includes meaningful examples and exercises that are relevant to the job (e.g., provides phishing emails that are common and similar to what employee may receive), learning aids to help trainees retain information (e.g., the TxDOT uses the saying "Don't be quick to click" throughout their phishing email training), a safe environment to practice (i.e., there is no penalty for mistakes in training), and feedback for trainees on their learning (e.g., results to quiz responses that include feedback on why responses are incorrect) (Noe & Colquitt, 2002; Salas et al., 2012).

www.manaraa.com

There are several different delivery methods used in training including: computer-assisted instruction, realistic training environments (e.g., simulation), behavior modeling (see Taylor et al., 2005 for a meta-analytic review of behavior modeling traning), serious gaming (see Wilson et al., 2009), and error management (see Keith & Frese, 2008 for a meta-analyitic review of error management training). Choice of an appropriate delivery method for training should be based on the nature of the KSAs to be trained, individual characteristics of trainees, and business goals and organizational resources for training.

Training Evaluation

The development of a new training program should always include training evaluation. Since 1959, Kirkpatrick's four levels of training (reaction, learning, behavior, and results) have been widely used and accepted (Kirkpatrick, 1959a, 1959b, 1960a, 1960b, 1996). Trainee reactions are generally measures of how the trainees feel about various aspects of the trainee program (Kirkpatrick, 1996). Measurement of trainee reactions to the training should include both perceptions of training utility (i.e., was the training useful?) and affective perceptions of the training (i.e., did you like the training?) because utility reactions have been shown to predict training transfer (Alliger, Tannenbaum, Bennett Jr, Traver, & Shotland, 1997). Training reactions are also important because they provide an indirect indication of how motivated trainees were to learn (Kirkpatrick, 1996). Specifically, if a trainee has negative reactions to the training, it is unlikely that the trainee put a lot of effort into learning during the training.

Learning is a measure of the change in KSAs (Knowledge, Skills, and Attitudes) (Kirkpatrick, 1996). That is, the learning evaluation indicated the knowledge acquired, skills improved, and/or attitudes changed due to the training intervention. Typically, learning is evaluated through pre- and posttests of knowledge, skills, and/or attitudes. Knowledge and

www.manaraa.com

attitudes are typically assessed through paper-and-pencil assessments, while skills are assessed through a performance test. Research suggests that learning outcomes are multidimensional, including three components: affective, skill-based (behavioral), and cognitive (Kraiger et al., 1993). Behavior is a measure of the extent to which trainees change their on-the-job behavior as a result of training (Kirkpatrick, 1996). Depending on the targeted KSAs of training, behavior can be evaluated through employee performance reviews. For phishing email training, some organizations evaluate on-the-job behavior though periodic phishing of their employees. Results are an organizational indication of the effectiveness of training (e.g., high productivity, increased profits). For cyber-security training, results could be captured in an organization-wide reduction in successful phishing attacks.

In addition to training needs assessment, training design, training delivery, and training evaluation, there are several other variables that influence training success as part of the larger training context. The influence of training characteristics was previously mentioned in the review of the person analysis as part of the TNA. The work environment in terms of organizational support for training, opportunities to use training, and any work constraints also predict training success (Baldwin & Ford, 1988).

The Larger Training Context: The Influence of Individual Differences

Baldwin and Ford (1988) created the most cited theoretical model of training transfer, which outlines the different variables that influence training success in terms of generalization of the KSAs trained to on-the-job performance. According to their model, training transfer is affected by training inputs (trainee characteristics, training design, and work environment) and training outputs (learning and retention). The trainee characteristics that have the greatest effect on training transfer are learning goal orientation, cognitive ability, negative affect, openness,

www.manaraa.com

self-efficacy, perceived utility, organizational commitment, and pretraining motivation (Baldwin & Ford, 1988). Similarly, trainee characteristics influence training outcomes, such as learning.

The importance of the assessment of individual differences for identifying trainee characteristics that influence training success has been well established through research (see Bell et al., 2017 for a review). Individual differences shown to affect training success include: cognitive ability (Salas & Cannon-Bowers, 2001; Schmidt & Hunter, 1998), personality traits (Barrick & Mount, 1991), motivational constructs (Colquitt et al., 2000; Noe & Schmitt, 1986), goal orientation (Martocchio & Hertenstein, 2003) and values and interests (Gordon & Alf, 1962). Blume, Ford, Baldwin and Huang (2010) conducted a meta-analysis on the transfer of training and found that some of the greatest predictors of training transfer in terms of trainee characteristics were cognitive ability (r = .37), conscientiousness (r = .28), neuroticism (r = -.19), learning goal orientation (r = .16), pretraining self-efficacy (r = .22), and motivation (r = .29).

Cognitive ability, or general mental ability (g), is one of the most consistently strong predictors of training success across job domains, with the commonly cited validity coefficient of r=.56 from Schmidt and Hunter's (1998) meta-analysis of predictors of job performance and training performance. Ree and Earles (1991) found that general ability (g) was the greatest predictor of training grades in a sample of Air Force enlistees.

Despite the research on the importance of cognitive ability for training and employee performance across different jobs, there has been little research on the relationship of cognitive ability to phishing email susceptibility to date. One study found that working memory (as measured by the Alphabet span task) and selective attention (as measured by the Stroop task) were significantly related to phishing susceptibility (measured as the miss rate or identifying phishing emails as trustworthy) (Mayhorn & Nyeste, 2012). Further research is needed to

www.manaraa.com

understand the influence of cognitive ability on phishing susceptibility and on cyber awareness training success.

This section reviewed the science of training, providing evidence-based suggestions for cyber awareness training for end-users. The reviewed theoretical framework for training evaluation and training context will be used to assess the influence of different interventions for improving employee phishing susceptibility in this study. The following section outlines hypotheses based on the review of the literature in the previous sections.

Hypotheses

The previous sections reviewed recent findings related to phishing susceptibility research and the theoretical foundations of training research. In this section, I propose several hypotheses based on previous research and theory to test as part of a phishing email training evaluation for a sample of transportation workers. The proposed study has three primary goals.

The first goal is to evaluate the effectiveness of phishing email training with regard to informational approaches and fear-appeals. To this aim all participants receive phishing email training that is primarily informational in nature. Specifically, the training provides information on the characteristics, or design features, found in phishing emails and how to recognize and response to the threats. Employees will be assessed on phishing susceptibility (sensitivity and bias) using behavioral responses during an email simulation containing several phishing emails both before and after training. Employees will also be randomly assigned to fear appeal conditions to supplement the standard training. One group will receive a strong fear appeal, one will receive a weak fear appeal, and one will receive no fear appeal (control condition).

The second goal is to distinguish between sensitivity and response bias in phishing susceptibility and evaluate the differential impact that training and fear appeals have on each of

www.manaraa.com

the two outcomes. Understanding the differential impact of training on response bias and sensitivity has implications for how organizations should approach training. If training mostly impacts response bias rather than sensitivity, organizations should consider the impact that a greater tendency to treat emails as threatening could have on other aspects of organizational performance (e.g., productivity).

The third goal is to understand the influence of the larger training context on training success. To this aim, employees will answer questions pertaining to training reactions, cognitive ability, and demographics, which will be evaluated for their effects on baseline phishing susceptibility (pretest scores) and training success (changes in phishing sensitivity and response bias between the pretest and posttest). Thus, the following hypotheses will be examined:

First, based on the distinction between sensitivity and response bias in phishing susceptibility, I hypothesize that an employee's sensitivity and bias will be differentially influenced by phishing email training interventions. Response bias is thought to be variable and influenced by environmental and expectancy factors (Lynn & Barrett, 2014). Thus, I hypothesize that:

Hypothesis 1: There will be a significant, negative change in individuals' response bias after training, such that individuals will have a more liberal response bias after training.

Hypothesis 2: The change in response bias between pre- and posttest scores will depend on the fear appeal intervention, such that the strong fear appeal will predict the largest difference in pre- and posttest response bias, the weak fear appeal will predict a smaller difference in response bias, and the control condition will have the smallest impact on response bias.

www.manaraa.com

Alternatively, sensitivity to phishing emails is a perceptual ability that represents a relatively stable individual difference that is unlikely to be influenced by expectancy factors, such as fear appeals. Still, the information provided in training on how to recognize email design features will likely result in some improvement in phishing email sensitivity.

Research Question 1: Are the effects of the training intervention different for the sensitivity and response bias outcomes?

Hypothesis 3: There will be a significant change in individuals' sensitivity to phishing emails after training, such that individuals will have a greater sensitivity to phishing email after training.

Hypothesis 4: The change in sensitivity between pre- and post-test scores will not significantly differ across fear appeal conditions.

Recent research suggests that individual differences may explain an individual's susceptibility to targeting to phishing emails. Thus, I propose that there are stable individual differences, such as cognitive ability, that will influence phishing email sensitivity.

Hypothesis 5: Cognitive ability will positively relate to individuals' phishing sensitivity, such that individuals with higher cognitive ability will have a greater sensitivity to phishing emails pre-training.

Research Question 2: Does the success of training (change in sensitivity scores between pre- and post-training assessments) depend on cognitive ability?

Based on the research on trainee reactions (Alliger et al., 1997; Kirkpatrick, 1996), I predict that trainee reactions to training will influence training success.

Hypothesis 6a: Utility reactions will positively relate to change in phishing sensitivity, such that individuals with higher perceptions of training utility will have a greater

www.manaraa.com

change in pretest and posttest phishing sensitivity than those with lower utility perceptions.

Hypothesis 6b: Utility reactions will positively relate to change in response bias, such that individuals with higher perceptions of training utility will have a greater change in pretest and posttest response bias than those with lower utility perceptions.

Hypothesis 7a: Affective reactions will positively relate to change in phishing sensitivity, such that individuals with higher affective perceptions of training will have a greater change in pretest and posttest phishing sensitivity than those with lower affective perceptions.

Hypothesis 7b: Affective reactions will positively relate to change in response bias, such that individuals with higher affective perceptions of training will have a greater change in pretest and posttest response bias than those with lower affective reactions.

This section detailed the study hypotheses and the accompanying research and theoretical backgrounds. These hypotheses will be tested to address the three goals of the current research: 1) to evaluate the effectiveness of informational cyber awareness training and fear-appeals on phishing susceptibility, 2) to distinguish between sensitivity (phishing email detection ability) and response bias (tendency to response safely or unsafely to emails) in phishing susceptibility, and 3) to understand the influence of the larger training context on phishing email training success. The next chapter will detail the methodology used in this study.

www.manaraa.com

CHAPTER TWO: METHOD

Participants

Participants were recruited via their work email provided by the Workforce Development Director of the TxDOT. There were 1,714 TxDOT employees who were identified as eligible for the study as their annual cyber-security training was due during the data collection period. These employees were emailed through Qualtrics using the Qualtrics mail merge software to assign IDs to each recipient to be used to connect the surveys without the use of any identifiable information (see Appendix A for the recruitment email). A reminder email was sent to all employees identified to participate in the study by the Director of Workforce Development. Employees were encouraged to use company time to complete the survey and responses were anonymous with no penalty for choosing not to participate.

Participants in the present study were 248 TxDOT employees. This sample size was determined as the appropriate recruitment number based on an a priori power analysis. A sample size of 100 was derived from an a priori power analysis using G*power (Faul, Erdfelder, Buchner, & Lang, 2009). This estimate was based on the regression analyses for reactions predicting response bias and sensitivity. For the inputs for the power analysis, an alpha of .05, and a power of .95, and an effect size of .10 was used for reactions predicting response bias and sensitivity, which is similar to what prior research has found for reactions predicting behavioral outcomes in training (see Alliger et al., 1997). Since, the majority of the analyses require the completion of both the pre- and post-training surveys, recruitment continued until at least 100 participants completed both the pre- and post-training surveys. This recruitment strategy resulted

www.manaraa.com

in a sample of 248 respondents who completed the pre-training survey and 174 respondents who completed the post-training survey. Duplicate (N=6) and partial (N=28) responses were removed and responses were screened to remove those that did not take the training in-between the surveys. These participants were identified as those who had a self-reported training completion date prior to the start of data collection (N=26). The final sample of respondents that completed both surveys and met the above inclusion criteria comprised of 139 participants (226 completed at least one survey).

Participants were predominately male (62.3%), with a large proportion of participants holding a bachelor's degree (37.4%) as their highest level of education, and fewer with some college courses (24.6%), a graduate degree (12.8%), associate's degree (13.3%), a high school diploma (11.3%), or less than a high school diploma (0.5%). The majority of the respondents had been at TxDOT between 0 and 5 years (56.9%) and in their current position between 0 and 2 years (57.1%). Only one participant held a cyber certification (0.5%), 23 had cyber education (11.1%), and eight had previously held a job where the primary responsibilities were cyber-security (3.9%). Less than half of participants indicated that they had helped someone fix a computer problem (40.6%). The majority of participants indicated they receive less than 50 emails per day to their work email (81.2%) and spend between 0 and 2 hours per day on email (72.3%). The results of multiple one-way analysis of variances (ANOVAs) indicated there was no significant difference between the randomly assigned fear condition groups on any of the measured demographic variables.

Procedure

During a three-month period, TxDOT employees who were due to take the mandatory annual cyber-security training within the next one to two months were emailed an invitation to

www.manaraa.com

participate in the study and a link to the pre-training assessment and post-training assessments, hosted by Qualtrics. They were instructed that there were two survey links in the email and that they should first take the pre-training assessment (first link), then complete their training as normal, and finally come back to the email to complete the post-training assessment (second link). The Director of Workforce Development also sent a follow-up email to the participants as a reminder to participate if they had not already done so.

The pre-training assessment survey contained an informed consent, a phishing email simulation, and demographics. The informed consent included information on the purpose of the study, risks and benefits to participation, and the study procedures. The phishing email simulation contained 30 emails, 10 of which were legitimate and five of which are phishing emails. After completing the pre-training assessment, participants were instructed to complete their security training through the portal provided by TxDOT. This training is a self-paced course in a slide deck format with an optional audio narration.

After employees took the mandatory training, they were instructed to take the post-training assessment by clicking on the link in their original email, in the end of survey message from the pre-training survey, or in the reminder email. At the start of this survey, they were randomly assigned to one of three conditions for the fear appeal: strong fear-appeal, weak fear appeal, and control. The fear appeals were designed to manipulate employees' perceptions of the consequences of falling for phishing emails and are based on fear-appeals that have been previously used in phishing email training (adapted from Jansen, 2018)(see Appendix H). At the end of the fear appeal message, the respondent answered two message involvement items designed to evaluate how impactful the fear appeal message was to the respondent (see Appendix I). After reading the fear-appeal/control and answering the corresponding items, employees

www.manaraa.com

completed the post-training assessment (contained a parallel phishing email simulation and the training reactions questions). After the completion of the post-training survey, employees were thanked for their participation and closed out of Qualtrics.

Measures

Training Evaluation Measures

Trainee Learning Outcomes: Phishing Susceptibility. Phishing susceptibility was measured through responses to simulated phishing emails. Simulations were administered in both the pre- and posttest assessments. In each of the parallel assessments, participants were prompted with 30 different emails, 10 of which were phishing emails and 20 of which were legitimate emails. For each email, participants were asked to indicate 1) how they would respond to the email and 2) their confidence in their response. An example phishing email stimulus with the behavioral response options and confidence rating is provided in Appendix B. Appendix C includes all email stimuli used in each the pre- and post-training surveys. The majority of the emails were adapted to fit the TxDOT scenario (see Appendix D) from email stimuli used in Martin et al.'s (2018) study. The remaining emails were either created for the purposes of this study or drafted from real phishing emails found online.

First, emails from the pre- and post-training simulations were matched on the proportion of safe responses obtained in Martin et al.'s (2018) study. The stimuli were then pilot-tested on 8 mTurkers with the order of the emails randomized. The stimuli were split into the different surveys (pre and post) to achieve essentially equivalent summary statistics for each survey (see Table 2 below). The number and types of email design features for each email were coded by two research assistants and discussed to consensus. The average number of phishing features per email were also balanced for each assessment. The above design precautions were used to create

www.manaraa.com

email simulations with matching threat levels. The emails in each the pre- and post-training surveys had about 35% of people respond safely on average based on the Martin et al. (2018) data and an average of about 40% based on the pilot data.

Table 2. Email Stimuli Pilot Testing Statistics

Pre-Training Stimuli				Post-Training Stimuli			
Stimulus ID	# of features	Proportion Safe*	Proportion Safe (Pilot)**	Stimulus ID	# of features	Proportion Safe*	Proportion Safe (Pilot)**
L19	0	0.09	0.38	L37	1	0.09	0.38
L10	0	0.09	0.63	L24	0	0.10	0.38
L6	0	0.13	0.75	L34	2	0.10	0.25
L14	0	0.15	0.13	L32	0	0.19	0.13
L15	0	0.16	0.13	L31	0	0.15	0.63
L3	2	0.16	0.38	L33	2	0.16	0.25
L18	0	0.19	0.13	L23	2	0.21	0.25
L16	0	0.21	0.25	L21	0	0.22	0.13
L5	0	0.22	0.13	L25	0	0.23	0.13
L12	0	0.23	0.13	L35	0	0.24	0.25
L17	1	0.24	0.38	L22	0	0.26	0.13
L2	0	0.25	0.75	L29	0	0.27	0.25
L11	0	0.27	0.25	L4	0	0.30	0.13
L26	0	0.31	0.25	L27	1	0.40	0.63
L8	0	0.39	0.75	L28	0	0.47	0.25
L13	0	0.47	0.50	L36	0	0.50	0.38
L9	1	0.48	0.25	L30	1	0.61	0.33
L1	1	0.53	0.88	L38	0	N/A	0.13
L7	0	0.58	0.75	L40	2	N/A	0.13
L20	6	N/A	0.63	L39	0	N/A	0.63
P7	3	0.26	0.13	P20	4	0.15	0.13
P5	4	0.35	0.88	P16	3	0.21	0.50
P2	5	0.37	0.50	P11	4	0.35	0.50
P3	5	0.45	0.88	P14	5	0.36	1.00
P8	6	0.52	0.13	P13	4	0.47	0.63
P1	8	0.66	0.38	P17	5	0.51	1.00
P6	6	0.70	0.63	P18	7	0.60	0.63
P9	6	0.86	0.63	P19	7	0.76	0.63
P10	3	N/A	0.25	P15	6	0.85	0.88
P4	3	N/A	0.38	P12	4	N/A	0.75
Average	**2**	**0.35**	**0.44**	**Average**	**2**	**0.34**	**0.41**
Min	**0**	**0.09**	**0.13**	**Min**	**0**	**0.09**	**0.13**
Max	**8**	**0.86**	**0.88**	**Max**	**7**	**0.85**	**1.00**

Notes. *based on data from Martin et al. (2018), N=207. **Based on pilot data from Mturk respondents, N=8.

www.manaraa.com

SDT was used to evaluate the responses to the email stimuli and to calculate two metrics to quantify phishing susceptibility; phishing detection ability and response bias. Both d-prime and response bias were calculated based on Macmillan and Creelman's (2004) equations. Confidence ratings were collected in order to calculate and Receiver Operating Characteristic (ROC) curve (Macmillan & Creelman, 2004), which allowed for the testing of the equal variance SDT model assumption.

Trainee Reactions. Trainee reactions was measured during the post-training assessment using items adapted from (Tan, Hall, & Boyce, 2003) trainee reactions scale and Kirkpatrick's (1996) comment sheet (see Appendix E). These items include measures of both affective and utility trainee reactions. The 3-item utility reactions scale demonstrated very good reliability (α = .94) and the two affective reactions items correlated .87 with one another.

Cognitive Ability

Items available through a public domain assessment tool for measuring different dimensions of cognitive ability, the International Cognitive Ability Resource (ICAR) 16-item test were used for measuring several cognitive ability dimensions (The International Cognitive Ability Resource Team, 2014) (see Appendix F). The 16-item measure demonstrated good reliability (α = .79) (Condon & Revelle, 2014).

Demographics

Demographic questions relating to gender, age, ethnicity, education, income, tenure, and cyber-security/IT experience were measured at the end of the pre-training assessment. At the beginning of the post-training assessment, participants were asked background questions about the training related to the date they completed the training, the number of attempts they used, and

www.manaraa.com

the number of times they have completed the training (see Appendix G for a list of all the demographic and background questions).

www.manaraa.com

CHAPTER THREE: RESULTS

This section details the results for the present study. First, the suitability of using SDT metrics for the observed data was evaluated using model fitting of generated ROC curves to the observed data. Then, the equal-variance assumption that the noise and signal distributions have equivalent variance was evaluated using chi-square difference tests comparing the freely estimated ROC curve models with those with constrained variances. Next, SDT statistics were computed and the hypotheses were tested.

SDT Analyses

Model Fitting

ROC curves for the pre-training and post-training phishing susceptibility were plotted to evaluate the fit of the SDT model to the observed data. The confidence ratings data was used to add additional criteria and construct the empirical ROC curves (Macmillan & Creelman, 2004). For each participant, the average confidence across all stimuli was computed. Any responses where the participant's confidence rating was above or equal to their average confidence were coded as "sure", while any responses with confidence ratings less than their average confidence were coded as "unsure". For example, if a participant's average confidence rating across all 30 pre-training stimuli was 65% and for one of the phishing email stimuli they endorsed the safe response with a 50% confidence, this response was coded as an "unsure" safe behavior response to a phishing email stimulus.

The coordinates for the ROC curves were computed by first creating a frequency stimulus-response table, which totals the number of responses for each stimulus-response pair

www.manaraa.com

(see Table 3). Next, the proportion of trials on which the stimulus yielded each response is calculated by dividing each cell from the stimulus-response table by the total number of responses for that stimulus type (see Table 4). These values are then cumulated to be used as the ROC coordinates (see Table 5 and Figure 6).

Table 3. Frequency Stimulus-Response Table

		Response				
		Safe Behavior		Unsafe Behavior		
		"Sure"	"Unsure"	"Unsure"	"Sure"	Total
Pre-training	Legitimate Email	642	379	453	826	2300
	Phishing Email	660	252	92	146	1150
Post-training	Legitimate Email	576	304	361	1059	2300
	Phishing Email	789	222	47	92	1150

Note. N = 115. Participants made a binary detection response indicating "Option 1" for safe behaviors and "Option 2" for unsafe behaviors. This response was immediately followed by a confidence judgment. The participants' confidence judgments were coded into sure and unsure based on whether it fell above or below the participants' mean confidence rating. Participants with less than 30 responses for the confidence questions were excluded. The values in each cell represent the number of responses for the stimulus-response pair.

Table 4. Proportion Stimulus-Response Table

		Safe Behavior		Unsafe Behavior		Total
		"Sure"	"Unsure"	"Unsure"	"Sure"	
Pre-training	Legitimate Email	.28	.16	.20	.36	1.00
	Phishing Email	.57	.22	.08	.13	1.00
Post-training	Legitimate Email	.25	.13	.16	.46	1.00
	Phishing Email	.69	.19	.04	.08	1.00

Note. N = 115. The values in each cell represent the proportion of responses for the stimulus-response pair.

www.manaraa.com

Table 5. Hit and False-Alarm Rates: Cumulative Proportions

		Safe Behavior		Unsafe Behavior	
		"Sure"	"Unsure"	"Unsure"	"Sure"
Pre-training	Legitimate Email	.28	.44	.64	1.00
	Phishing Email	.57	.79	.87	1.00
Post-training	Legitimate Email	.25	.38	.54	1.00
	Phishing Email	.69	.88	.92	1.00

Note. N = 115. The values in each cell represent the cumulative frequencies of responses for the stimulus-response pair.

After plotting the points for the observed data on an ROC curve (see Figure 6), Maximum-likelihood was used to generate SDT parameters (Dorfman & Alf, 1969). As is customary in the SDT literature, the mean and standard deviation of the noise distribution were set to 0 and 1, respectively (Macmillan & Creelman, 2004). The generated points according to the best-fitting parameters are plotted with X's in Figure 6. Close correspondence of these points to the observed data indicated that the SDT model fit the data well.

www.manaraa.com

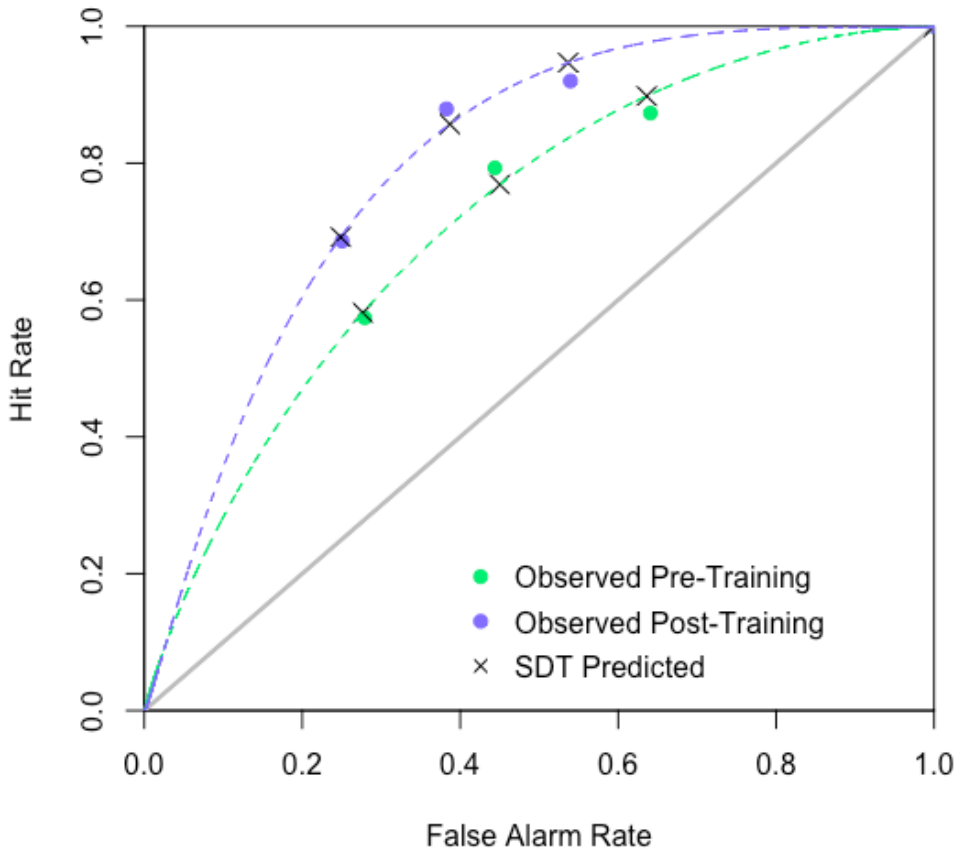


Figure 6. Model 1: Relaxed Model with the Variances Freely Estimated

SDT states that d' is unaffected by response bias only if the assumption that the noise and signal distributions have equal variance is met (Macmillan & Creelman, 2004; Stanislaw & Todorov, 1999). When the equal-variance assumption is not met, d' varies with response bias and alternative measures (i.e., d_a) must be used. This unequal-variance is observable through an asymmetrical ROC curve, whereas equal-variance SDT models have symmetrical implied ROC curves. To evaluate the equal-variance assumption that is required for the calculation of d' and c, the freely-estimated model (Figure 6) was compared to an equal-variance model where the

www.manaraa.com

standard deviation of the signal distribution was constrained to be equal to the standard deviation of the noise distribution. The chi-square difference tests of model fit to evaluate the EVSDT assumption did not show a significant difference between the relaxed model where the variance was freely estimated and the constrained model (see Figure 7) where the variance was fixed to be the same as the noise distribution for either the pre-training assessment ($\chi^2 = .64$, $p = .42$) or the post-training assessment ($\chi^2 = 1.76$, $p = .18$) (see Table 6), indicating the equal-variance assumption was met for both assessments.

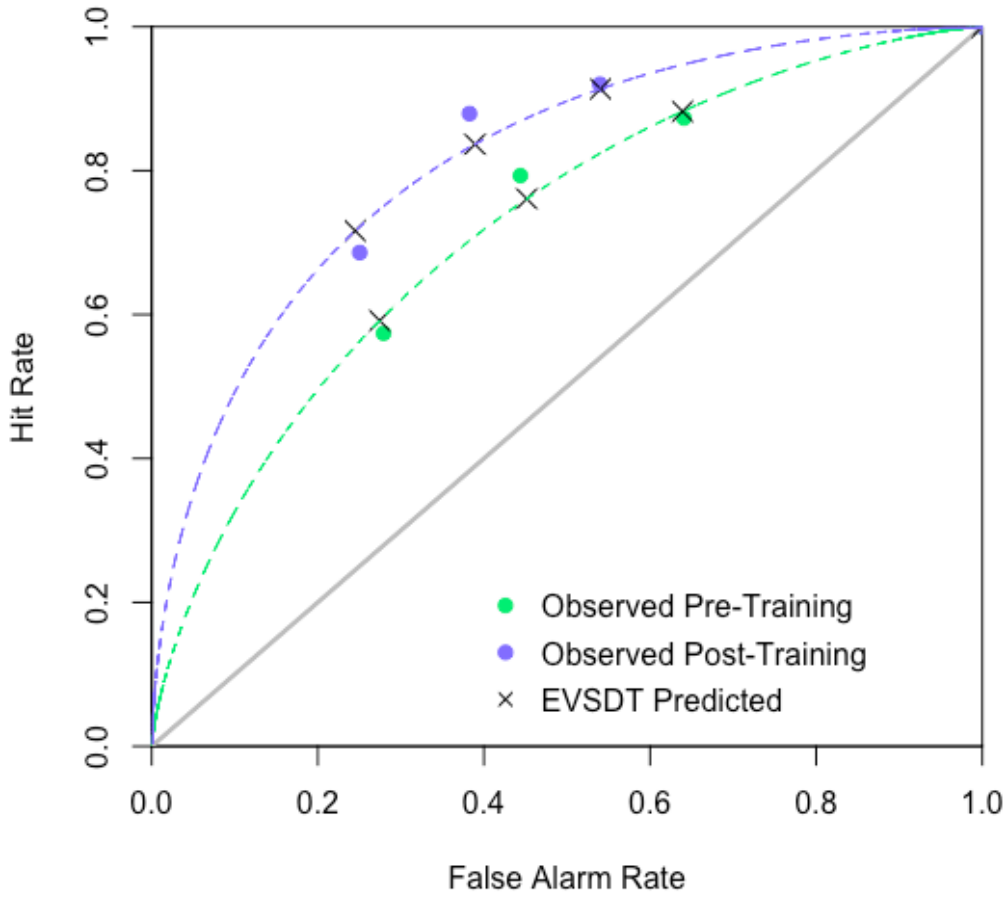


Figure 7. Model 2: Equal Variance SDT Predicted Model with the Variances Constrained

www.manaraa.com

Table 6. Chi-Square Difference Tests of Model Fit: Equal-Variance

	Model	μ	σ	c_1	c_2	c_3	χ^2	df	*p*
Pre	Model 1: Relaxed	.77	.88	.59	.12	-.35	2.13	3	.35
	Model 2: Constrained Equal Variance	.83	1.00	.59	.12	-.36	2.77	4	.25
Post	Model 1: Relaxed	1.03	.69	.68	.29	-.09	1.77	3	.41
	Model 2: Constrained Equal Variance	1.26	1.00	.69	.28	-.10	4.53	4	.10
	Model Comparison Pre (1&2): $\Delta\chi^2$						.64	1	.42
	Model Comparison Post (1&2): $\Delta\chi^2$						1.76	1	.18

Notes. μ = mean of the signal distribution, σ = standard deviation of the signal distribution, $c_{1\text{-}3}$ = confidence criterion

In order to further evaluate the equal-variance assumption, the ROCs were transformed into zROCs (see Figure 8). A zROC with a non-unit slope (or a slope not equal to one) indicates that the equal-variance assumption is not met and computation of an alternative measure of d', d_a is required. d_a is a measure of sensitivity that assumes unequal variance underlying distributions (Simpson & Fitter, 1973; Macmillan & Creelman, 2002). Notably, d_a is equivalent to d' when the ROC slope is 1, so if the underlying distribution for the pre-training assessment is equal variance, d_a will be of the same value as d'.

www.manaraa.com

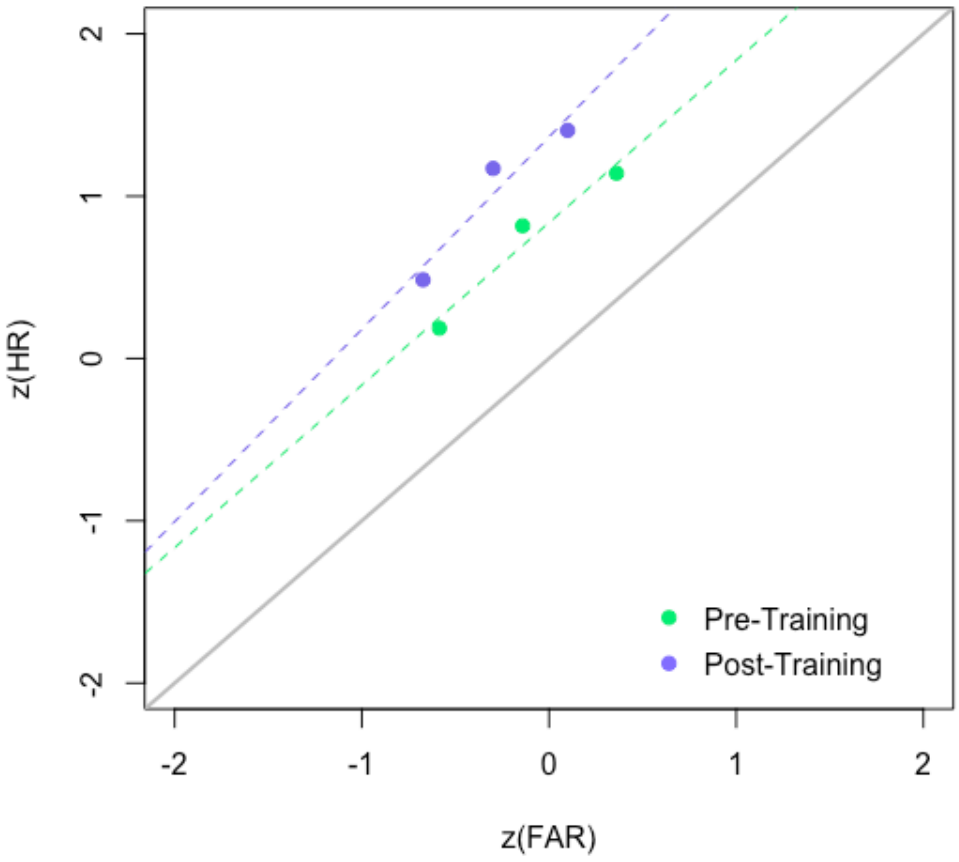


Figure 8. zROC of SDT Predicted Model

From the zROC, it is evident that the post-training line is not a perfectly unit slope, suggesting unequal-variance of the noise and signal distributions in the post-training simulation. Closer examination of the data revealed that there were 48 respondents without any misses (responding unsafely to phishing emails) in the post-training simulation. This means that almost 42% of the respondents had 10 hits in the safe response to the phishing email stimuli cells of the stimulus-response matrix (between the "sure" and "unsure" confidence levels). This contributes to the asymmetry of the ROC curve because for the second and third ROC points, these participants had a hit rate of 1.00, which would draw those points toward the top of the ROC plot, as is evidenced in Figure 6. To evaluate whether this was the main contributing factor to the

www.manaraa.com

asymmetry of the ROC plot, ROC curves were generated with the 48 identified respondents removed (see Figure 9). A zROC was also generated for this sample (see Figure 10). These plots reflect an equal-variance underlying distribution, as evidenced by the symmetry (in Figure 9) and unit slope (in Figure 10).

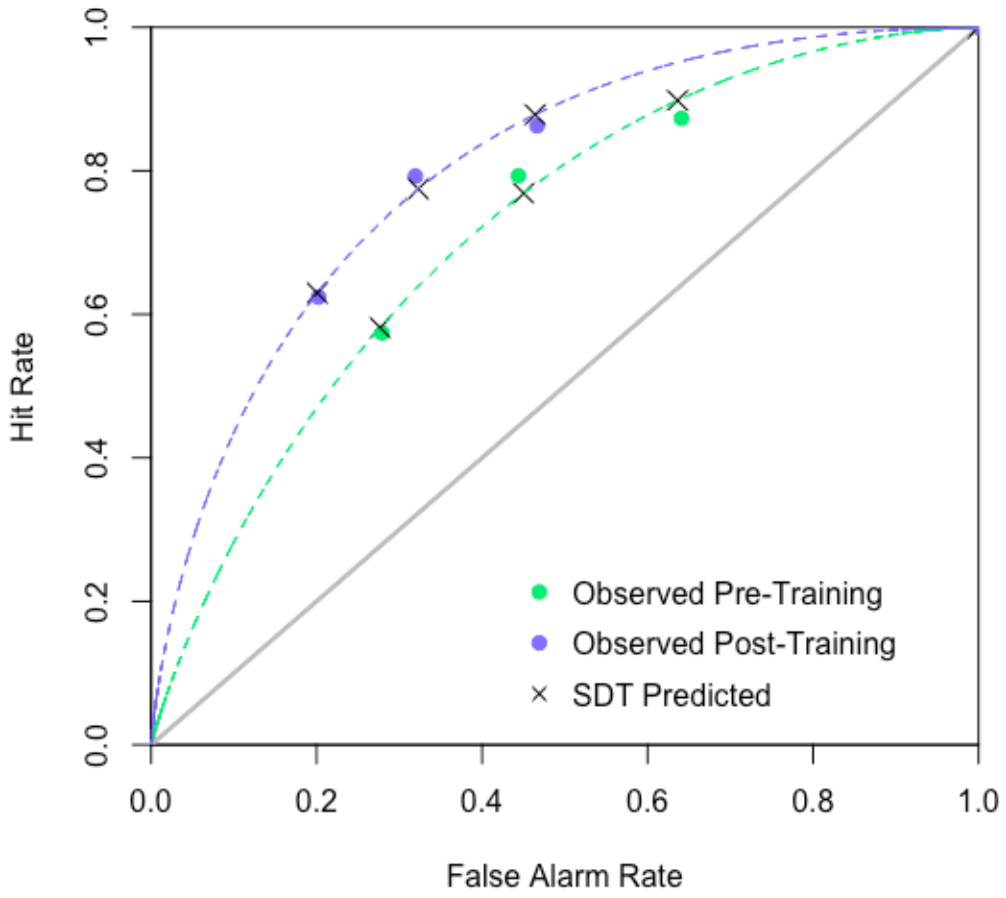


Figure 9. Adjusted Model with Post-Training Responses with No Misses Removed

www.manaraa.com

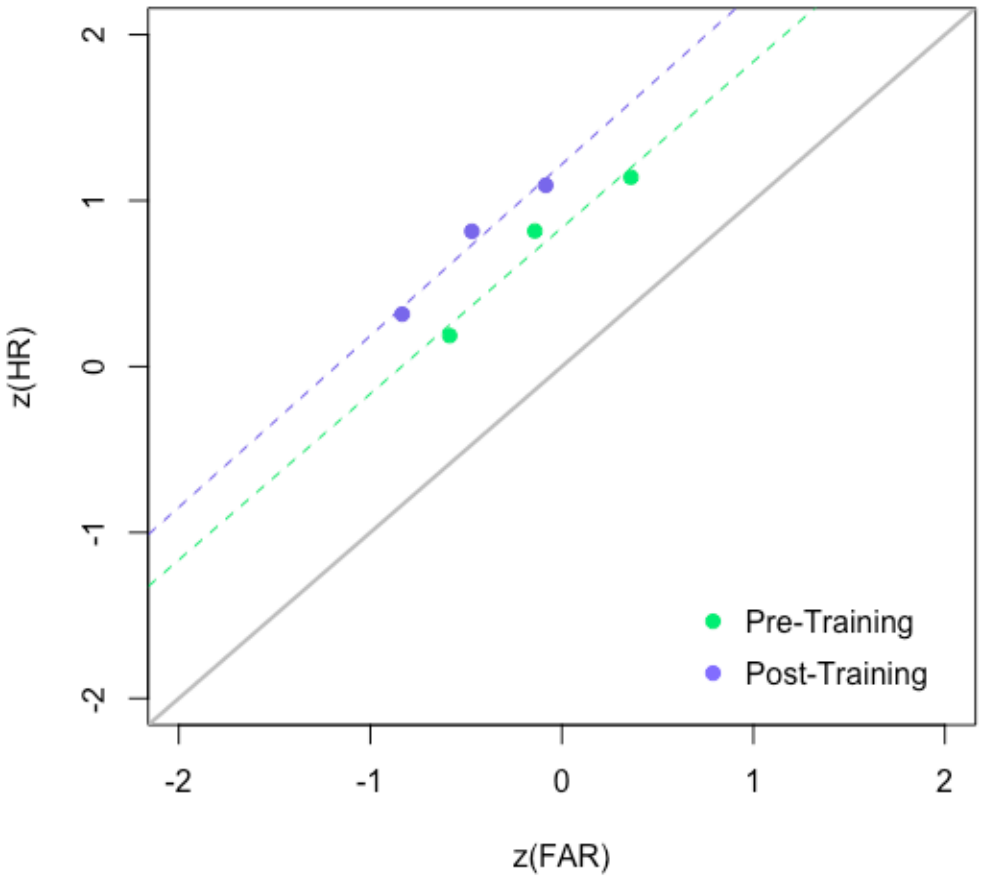


Figure 10. Adjusted zROC with Post-Training Responses with No Misses Removed

From this, it can be inferred that the equal-variance assumption would hold for all the data if there had been a greater number of signals (phishing emails) to reduce the chances that so many participants would have 100% hit rate. This combined with the evidence from the chi-squared difference test of model fit that the fit was not significantly worse for the equal-variance model than the freely-estimated model (Table 6) justify the use of equal-variance SDT metrics (d', c) to test the study hypotheses.

www.manaraa.com

Calculation of SDT Metrics

Two equal-variance SDT statistics were used to test the hypotheses regarding phishing email detection ability (d') and response bias (c). A pre- and post-training sensitivity (d'), or phishing email detection ability, was computed for each participant through the following calculation: 1) computed the number of hits, misses, false alarms, and correct rejections based on the stimulus-response pairings (30 in each simulation); 2) computed the hit and false alarm rates (see Table 7 for the averaged hit and false alarm rates); 3) computed d' by taking the difference between the inverse normal cumulative distribution functions (cdf) of the hit and false alarm rates.

Table 7. Stimulus-Response Matrix

Stimulus	*Response to prompt ("How would you handle this email?")*			
	Pre-Training		Post-Training	
	Safe Behavior	Unsafe Behavior	Safe Behavior	Unsafe Behavior
S_1 = Legitimate email	False alarms (44.4)	Correct rejections (55.6)	False alarms (38.0)	Correct rejections (62.0)
S_2 = Phishing email	Hits (78.0)	Misses (22.0)	Hits (86.0)	Misses (14.0)

Note. N=115. Values are in percentages and reflect the aggregate of responses across participants.

There were respondents who detected every signal (responded cautiously/safely to all 10 phishing emails), detected no signals (responded normally/unsafely to all 10 phishing emails), had zero false alarms (respond normally/unsafely to all 20 legitimate emails), or had a 100% false alarm rate (responded safely to all 20 legitimate emails). Hit and false alarm rates of either 0 or 1 pose a problem for computing d' because a probability value of 1 corresponds to an inverse normal cdf value of negative infinity while a probability value of 0 corresponds to an inverse normal cdf value of positive infinity. The conventional adjustment for this issue in SDT is to set the minimum probability to one divided by two times the number of trials used (1/2N).

www.manaraa.com

For instance, the minimum value for the false alarm rate in this study with the adjustment is 1/(2*20) or .025. Similarly, the adjustment for the maximum probability value is one minus one divided by two times the number of trials used (i.e., for the hit rate in this study: 1-1/(2*10) = .95). This adjustment was applied when the number of misses or the number of false alarms was zero so that d' could still be calculated. This process, including the adjustment is reproduced for two example participants in Table 8.

Table 8. Formulas for Calculation of SDT Statistics for Example Participants

	A (Labels Only)	*Formula (for Column B; Then copy to all other columns)*	*B (Part. 1)*	*C (Part. 2)*
1	# hits		7	10
2	# misses		3	0
3	# false alarms		10	9
4	# correct rejections		10	11
5	*HR* (hit rate)	=IF(B2>0, B1 / 10, .95)	0.7	0.90
6	*FAR* (false alarm rate)	=IF(B3>0, B3 / 20, .025)	0.5	0.45
7	*z*(*HR*)	=NORMSINV(B5)	0.524	1.645
8	*z*(*FAR*)	=NORMSINV(B6)	0.000	-0.126
9	d'	=B7-B8	0.524	1.407
10	*c*	= -.5*SUM(B7:B8)	-0.262	-0.760

Note. This process was completed twice for each participant to compute the pre- and post-training d' values. A higher value indicates higher sensitivity, or a greater ability to distinguish between phishing and legitimate emails.

Table 9 provides a summary of the SDT statistics used in this study, including the calculation, typical range, and interpretation within the context of this study.

www.manaraa.com

Table 9. Summary of SDT Metrics

SDT Metric	*Formula*	*Typical Min.*	*Typical Max.*	*Interpretation*
Hit Rate	$HR = \frac{\#\ of\ hits}{\#\ of\ phishing\ emails\ presented}$	0	1	Values closer to 1 indicate a higher proportion of phishing emails were treated as if they were threatening
False Alarm Rate	$FAR = \frac{\#\ of\ false\ alarms}{\#\ of\ legitimate\ emails\ presented}$	0	1	Values closer to 1 indicate a higher proportion of legitimate emails were treated as if they were threatening
D-prime	$d' = z(HR) - z(FAR)$	0*	3	Values closer to 3 indicate a greater ability to detect phishing emails
Response Bias	$c = .5[z(HR) + z(FAR)]$	-3	3	Positive values indicate a tendency to treat emails as if they are legitimate. Negative values indicate a tendency to treat emails as if they are threatening.

Note. *Negative d' values can occur through response confusion (e.g., responding "Option 1" when intending to respond "Option 2")(Stanislaw & Todorov, 1999).

Hypothesis Testing

SPSS 24 was used to compute the SDT statistics, d' and c, and to test the study hypotheses. Before proceeding with the analyses, the focal study variables were evaluated for normality and outliers. There were no concerns with any of the data. Descriptive statistics were computed for the focal study variables (see Table 10). Then, correlational analyses were computed for all study variables (see Table 11). Through initial examination of the correlation analyses, it is evident that the study variables are related in the expected directions. Both utility reactions (M = 4.01, SD = .96) and affective reactions (M = 3.82, SD = .94) were positively and significantly related to training effectiveness (M = .46, SD = .69), as measured by the difference in d' between the pre- and post-training assessments; $r(115) = .28$, $p < .01$ and $r(114) = .23$, $p < .05$. Cognitive ability (M = .51, SD = .27) and training effectiveness, measured by the difference in d' did not have a significant negative correlation; $r(115) = .04$, $p = .69$. However, cognitive ability was significantly related to both pre-training (M = 1.04, SD = .61) and post-training

www.manaraa.com

phishing email detection ability (M = 1.51, SD = .72); $r(120) = .18$, $p < .05$ and $r(121) = .20$, $p < .05$.

Table 10. Descriptive Statistics for Focal Study Variables

	N	*M*	*SD*	*Skewness*	*Kurtosis*
HR (pre-training)	120	0.78	0.16	-1.24	2.26
HR (post-training)	121	0.86	0.12	-1.40	1.15
d' (pre-training)	120	1.04	0.61	0.14	0.24
d' (post-training)	121	1.51	0.72	-0.84	0.72
c (pre-training)	120	-0.37	0.57	0.07	1.48
c (post-training)	121	-0.44	0.50	-0.52	0.89
d' (difference)	115	0.46	0.69	-0.34	0.35
c (difference)	115	-0.08	0.48	0.06	4.46
Cognitive Ability	126	0.51	0.27	-0.15	-0.94
Reaction: Utility	126	4.01	0.96	-1.37	1.92
Reaction: Affective	125	3.82	0.94	-1.07	1.36

www.manaraa.com

Table 11. Correlations among Study Variables

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1. d' (difference)	-									
2. *c* (difference)	-.09	-								
3. d' (pre-training)	-.39**	.01	-							
4. *c* (pre-training)	.24**	-.59**	.16	-						
5. d' (post-training)	.62**	-.08	.48**	.40**	-					
6. *c* (post-training)	.18	.33**	.24*	.60**	.38**	-				
7. Reaction: Utility	.28**	-.12	-.04	.08	.18*	-.02	-			
8. Reaction: Affective	.23*	-.08	-.14	.05	.06	-.05	.88**	-		
9. Cognitive Ability	.04	.00	.18*	.04	.20*	.06	.02	.00	-	
10. Income	-.15	-.01	-.10	-.19*	-.26**	-.19*	-.03	.05	-.05	-
11. Tenure (position)	-.06	.01	.05	-.04	-.05	-.02	-.04	-.06	-.08	-.09
12. Tenure (TxDOT)	-.08	.04	.05	-.15	-.07	-.12	-.06	.00	.11	-.09
13. Gender	-.03	-.09	-.08	-.14	-.14	-.23*	-.13	-.11	.12	.15
14. Education	.26**	.08	-.06	.19*	.22*	.27**	.07	.05	.15	-.17
15. Age	.09	.04	-.04	-.19*	-.03	-.19*	-.02	-.07	-.15	.14
16. Cyber Education	-.16	-.06	.12	.10	-.04	-.04	.01	-.01	.02	-.03
17. Computer Fix	-.01	.03	.19*	.00	.20*	.01	-.09	-.12	.28**	-.14
18. # of emails per day	.13	.12	-.01	.00	.10	.10	.07	.10	.00	.03
19. Time spent on emails	-.07	.16	.11	.00	.01	.12	.01	.04	.06	.01
20. # of completed trainings	-.08	.07	.07	-.08	-.05	.01	-.07	-.06	.14	-.02
21. # of attempts to pass final training quiz	-.10	.07	.02	.07	-.06	.11	.05	.04	-.15	.01

Notes. N = 112-126. *p<.05, **p<.01

www.manaraa.com

Table 11, continued. Correlations among Study Variables.

	11	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*
11. Tenure (position)	-									
12. Tenure (TxDOT)	.63**	-								
13. Gender	.19*	.30**	-							
14. Education	-.05	-.01	-.04	-						
15. Age	.26**	.36**	.18	.05	-					
16. Cyber Education	-.04	-.08	.01	-.12	-.08	-				
17. Computer Fix	-.16	.00	.14	.09	-.09	.03	-			
18. # of emails per day	.13	.13	-.01	.28**	.18*	.01	.18*	-		
19. Time spent on emails	.06	.11	-.02	.29**	.10	-.02	.17	.43**	-	
20. # of completed trainings	.53**	.62**	.15	-.07	.30**	-.14	-.02	.09	.11	-
21. # of attempts to pass final training quiz	-.12	-.09	.03	-.08	-.24**	.11	-.04	-.07	.08	-.09

Notes. N = 81-179. *p<.05, **p<.01

www.manaraa.com

Research question 1 and hypotheses 1 and 3 concerned the effect of training on phishing detection ability (d') and response bias (c). These hypotheses were assessed with two paired-sample t-tests comparing pre-test and post-test scores. The mean pre-training response bias was -.37 (*SD* = .50) and the mean post-test response bias was -.45 (*SD* = .56). A paired-samples t-test showed that the post-test response bias was not significantly different than the pre-test response bias at $t(114) = -1.68$, $p = .10$ (see also Table 12). Thus, hypothesis 1 was not supported. The mean pre-test sensitivity (d') was 1.05 (*SD* = .62) and the mean post-test sensitivity was 1.51 (*SD* = .72). A paired-samples t-test showed that the post-test detection ability was significantly higher than the pre-test detection ability at $t(114) = 7.19$, $p < .001$, Cohen's $d = .67$ (see also Table 12), supporting hypothesis 3.

Table 12. Training Effectiveness T-tests

		N	*M*	*SD*	*SEM*	*t*	df	p-value
Sensitivity (d')	Pre-test	115	1.05	.62	.06			
	Post-test	115	1.51	.72	.07			
	Between posttest-pretest	115	.46	.69	.06	7.19	114	<.001
Response bias (c)	Pre-test	115	-.37	.56	.05			
	Post-test	115	-.45	.50	.05			
	Between posttest-pretest	115	-.08	.48	.04	-1.68	114	.095

The influence of fear appeals on the two different outcomes (hypotheses 2 & 4) was tested with two one-way ANOVAs. A one-way ANOVA revealed no significant difference in response bias between the control group (*M* = -.04, *SD* = .60, N=38), weak fear appeal group (*M* = -.06, *SD* = .45, N=36), and strong fear appeal group (*M* = -.12, *SD* = .38, N=41), $F(2, 114) = .27$, $p = .77$. Thus, hypothesis 2 was not supported. The one-way ANOVA for phishing email detection ability also revealed no significant difference between the control group (*M* = .41, *SD* =

www.manaraa.com

.71), weak fear appeal group (M = .60, SD = .54), and strong fear appeal group (M = .38, SD = .77), $F(2, 114) = 1.16$, $p = .32$, supporting hypothesis 4.

Regression analyses were used to test the remaining hypotheses concerning the influence of cognitive ability and trainee reactions on phishing detection ability and training effectiveness (Research Question 2 and Hypothesis 5-7b). Cognitive ability scores (M = .51, SD = .27) significantly predicted pre-training phishing detection ability; $t(118) = 2.03$, $p < .05$ (see Table 13 for the regression model and Figure 11 for a scatterplot of the relationship). In answer to research question 1, regarding the influence of cognitive ability on the effectiveness of training, there was no significant effect of cognitive ability on training effectiveness ($\Delta d'$); $t(114) = .41$, $p = .57$.

Table 13. Regression Model for Cognitive Ability Predicting Pre-Training Phishing Detection

Predictor	**B**	**SE(B)**	***B***	***95% CI***
Constant	.83*	.12		
Cognitive Ability	.42*	.21	.18*	0.10, 0.82

Note. N=119. *$p < .05$. *B=standardized beta*

www.manaraa.com

Figure 11. Scatterplot of Pre-Training Phishing Detection Ability and Cognitive Ability Scores

A linear regression revealed that utility reactions significantly predicted training effectiveness ($\Delta d'$), $t(114) = 3.15$, $p < .01$ (see Table 14 and Figure 12). Another regression analysis showed that affective reactions also significantly predicted training effectiveness ($\Delta d'$), $t(112) = 2.52$, $p < .05$ (see Table 15 and Figure 13). Thus, hypotheses 6a and 7a were supported.

www.manaraa.com

Table 14. Regression Model for Utility Reactions Predicting Training Effectiveness ($\Delta d'$)

Predictor	B	SE(B)	*B*	*95% CI*
Constant	-.35	.27		
Utility Reactions	.20*	.06	.28*	0.08, 0.33

Note. N=102. *$p < .05$. *B=standardized beta*

Table 15. Regression Model for Affective Reactions Predicting Training Effectiveness ($\Delta d'$)

Predictor	B	SE(B)	*B*	95% CI
Constant	-.18	.26		
Affective Reactions	.17*	.07	.23*	0.10, 0.38

Note. N=102. *$p < .05$. *B=standardized beta*

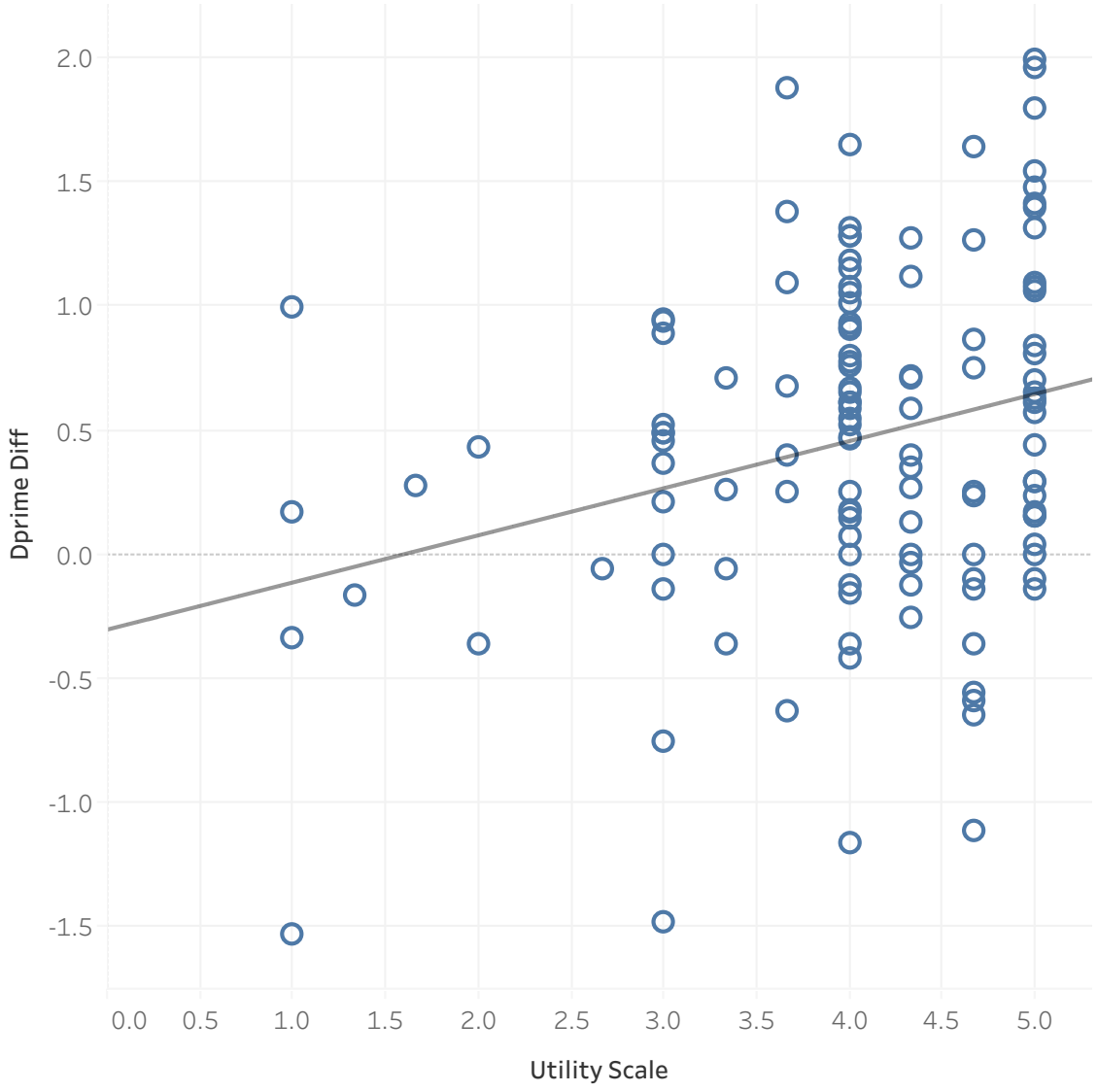


Figure 12. Scatterplot of Utility Reactions and Training Effectiveness ($\Delta d'$)

www.manaraa.com

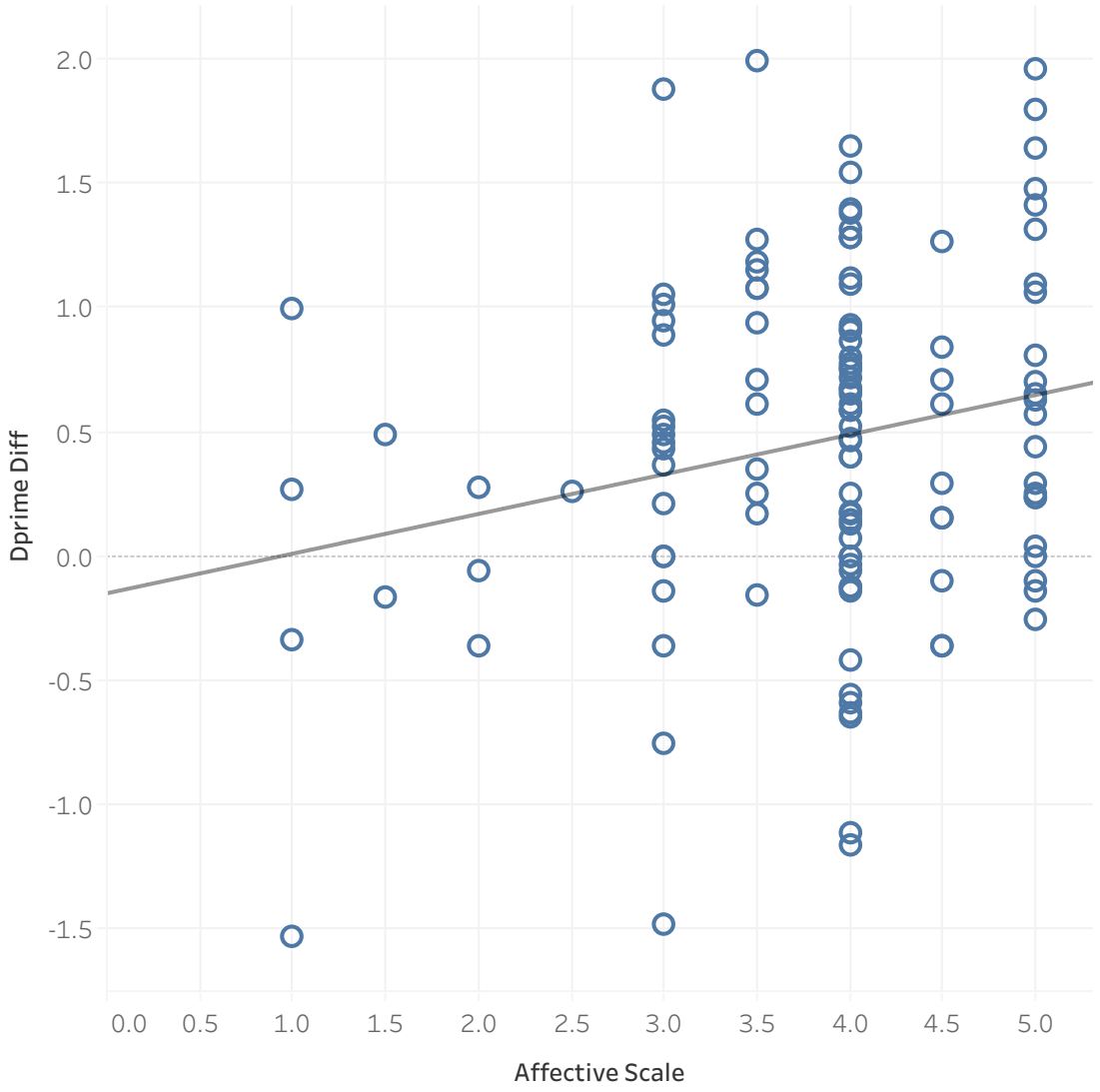


Figure 13. Scatterplot of Affective Reactions and Training Effectiveness ($\Delta d'$)

Linear regressions revealed that neither utility nor affective reactions significantly predicted the difference in response bias (M = -.08, SD = .48) between the pre-training and post-training assessments; $t(113) = -1.25$, $p = .21$ and $t(112) = -.83$, $p = .41$, respectively. Thus, hypotheses 6b and 7b were not supported.

www.manaraa.com

CHAPTER FOUR: DISCUSSION

The purpose of this study was to investigate the influence of cyber-awareness training and fear appeals on phishing susceptibility, as measured by SDT metrics. Overall, the training intervention did not result in a significant difference between pre- and post-training response bias, as measured by *c* (hypothesis 1). However, training did result in a significant difference between pre-training detection ability and post-training detection ability, as measured by d' (hypothesis 3). The fear appeal conditions were not significantly different for response bias or phishing email detection ability (hypotheses 2 and 4). As predicted, both utility and affective reactions to training predicted training success in terms of the change in phishing email detection ability (hypotheses 6a and 7a). However, neither utility nor affective reactions predicted change in response bias between pre- and post-training assessments. Next, these specific results are reviewed in greater detail. Then, the theoretical and practical implications, limitations, future directions, and conclusions are discussed.

Hypothesis 1 was not supported since there was no significant difference in response bias between pre- and post-training assessment. However, the observed difference was in the hypothesized direction (a greater tendency to respond as if the stimulus was threatening) and was approaching significance ($p < .10$). Thus, it is possible that this effect would be detected with greater power. Still, the average difference between groups was small (-.08), which may not indicate a meaningful shift in response bias. It could be that the training intervention did not change individual's payoff perceptions in terms of their perceived costs associated with misses

www.manaraa.com

and false alarms since the training primarily concerned recognizing characteristics of phishing emails.

Perhaps the artificial nature of the email simulations precluded a change in response bias because the perceived costs to false alarms were lower within this simulated email detection task than they would be in reality. It would be interesting to evaluate whether there is a change in response bias for actual, on-the-job behavior regarding evaluating emails. It is worth noting that participants averaged a negative response bias (c_{pre} = -0.37 and c_{post} = -0.44), indicating a tendency to respond as if an email is threatening. One explanation for this liberal response bias could be a perceived low cost for false alarms. Specifically, in the email simulation, there is virtually no cost to participants responding safely to emails, as opposed to in reality where there could be a time and productivity cost for responding safely (e.g., forwarding the email to IT, deleting the email) to legitimate emails.

Hypothesis 2, which predicted that change in response bias would differ between fear appeal conditions, was not supported. The conditions did not significantly differ on response bias. It is possible that the fear appeal intervention was not a salient enough intervention to manipulate response bias. The fear appeals were at the start of the post-training assessment and participants did not spend very much time reading the appeals, with an average of 105 seconds (*SD* = 150) on the strong fear appeal and an average of 68 seconds (*SD* = 35) on the weak fear appeal. Still, only a minority of respondents (N=3) did not favorably rate the message involvement items after the fear appeals, indicating that most participants reported they read the text carefully and perceived the text as having relevant information.

Jansen (2018) found significant differences between fear appeal conditions (using the same fear appeals used in this study) for protection motivation and intentions to perform online

www.manaraa.com

cautionary behavior, but the effect sizes were very small. It could be that the small effect the fear appeals have on individual's behavioral intentions is diminished when it comes to actual response behavior as measured in this study. Other recent studies that evaluated the influence of fear appeals on cyber awareness training effectiveness also found small effects, even when using different fear manipulations, such as new articles (Zielinska et al., 2014) or a generated individual risk level (Davinson & Sillence, 2010).

Hypothesis 3, which predicted that training would significantly increase phishing email detection ability was supported. This demonstrates that an informational approach to training that provides details on email characteristics related to phishing emails is effective for improving individual's phishing email detection ability. This finding is consistent with other studies that have found rule-based training is effective for reducing phishing email susceptibility (e.g., Alnajim & Munro, 2008, 2009; Kumaraguru et al., 2009, 2007, 2010; Mayhorn & Nyeste, 2012; Sheng et al., 2007).

As hypothesized, the three different fear appeal conditions (strong, weak, and control) did not significantly differ on phishing email detection ability (hypothesis 4). In contrast to the informational approach to training, the fear-based approach was not found to have an effect. As detailed above with regard to the lack of effect of fear appeals on response bias, this null result could also be due to the lack of strength of the fear appeal intervention. It could also reflect the SDT paradigm that stipulates that sensitivity is resistant to the influence of expectancy factors, such as payoff perceptions. That is, sensitivity is separate from response bias, such that payoff perceptions do not influence a person's ability to distinguish between signal and noise. In the context of phishing email detection, it makes sense that manipulating the perceptions of the costs

www.manaraa.com

of different outcomes (e.g., the cost of a false alarm for a legitimate email) would not influence one's ability to differentiate between a legitimate email and a phishing email.

Hypothesis 5, regarding the influence of cognitive ability on phishing email detection ability was supported. This finding is consistent with previous research that found working memory and selective attention were related to phishing susceptibility (Mayhorn & Nyeste, 2012). It also supports the notion that phishing email detection ability or sensitivity is a perceptual ability that is influenced by stable individual characteristics, such as cognitive ability.

Hypotheses 6 and 7 were partially supported. Affective and utility reactions both significantly predicted training success in terms of a change in sensitivity (hypotheses 6a and 7a), however they did not predict a change in response bias (hypotheses 6b and 7b). As discussed above, the lack of change in response bias could be an artifact of the simulated environment resulting in skewed payoff perceptions. Alternatively, it could be that training reactions differentially impact phishing email detection ability and response bias.

Favorable affective and utility reactions provide an indication that employees were motivated to learn during the training. For instance, employees who response favorably to liking the training and finding it useful likely were more motivated to internalize the training and use it on-the-job. Since the training was primarily informational in nature and emphasized learning the distinguishing features of phishing emails, a heightened motivation to internalize training would more likely influence phishing email detection ability rather than response bias.

Generally, the finding that affective and utility reactions influenced training success is consistent with previous research across training domains (Blume et al., 2010). Particularly, consistent with the present research, previous research has found that utility reactions have a

www.manaraa.com

stronger effect on training success than affective reactions (Alliger et al., 1997). These results underscore the importance of communicating the utility of training to employees.

Implications

Practically speaking, the finding that training is effective for phishing email detection ability is helpful to organizations, not only because it supports previous research demonstrating the effectiveness of informational training in this domain, but also because the methods used in this study to evaluate training could be adopted by organizations. As previously stated, only 54% of information security professional surveyed in the State of the Phish Report reported being able to quantify phishing susceptibility based on their training activities (Wombat Security Technologies, 2018).

This study has several implications for practice regarding training evaluation. In terms of Kirkpatrick's four levels, organizations should consider including each of the levels: reactions, learning, behavior and results. When evaluating training interventions for phishing email susceptibility, organizations should include affective and utility reactions since they predict training effectiveness. Training reactions are an important metric to gauge trainee's impressions of the training as well as their motivation for learning during the training. Learning is often assessed with pre- and post-training assessments that evaluate the change in the knowledge, skills, and/or attitudes that were a focus of the training. Learning could be assessed with an email simulation, such as the one used in the present study. Behavior and results are more difficult to measure in this context. Behavior could be assessed through periodic phishing of employees, though as previously discussed there are ethical considerations with this method. Results could be assessed through tracking both the number of breaches due to employees falling for phishing

www.manaraa.com

emails as well as reported instances where employees fell for a phishing email, but it did not result in a breach due to IT intervention.

Since both prior research and findings from this study found fear appeals have little or no effect on employee intentions and behavior with regard to phishing emails, organizations should consider the usefulness of the fear approach to reducing phishing susceptibility before implementation. Organizations should turn instead to different approaches with research supporting the effectiveness, such as informational approaches. This consideration is also important given the distinction between the influence of training on phishing email detection ability and response bias. According to the present research, informational training impacts sensitivity, but not response bias. This is an important finding for organizations because it demonstrates that informational training does actually improve individuals' ability to recognize phishing emails rather than unilaterally changing their tendency to respond safely to emails.

There are implications for selection based on the result demonstrating that there is a relationship between cognitive ability and phishing susceptibility. Cognitive ability is a known, consistent predictor of job performance and is often used as part of selection assessment batteries. Organizations may want to consider the extension of this trend to the narrow piece of job performance assessed in this study, phishing email detection performance. It could also be worth investigating whether there are more specific abilities that are strong predictors of phishing email detection performance. With such a narrow performance space, it could make sense to investigate more narrow cognitive ability predictors, such as selective attention. Further, this information could be used to select individuals to target with phishing email training. Interestingly, whether or not participants had experience helping someone fix a computer was also related to phishing email detection performance on both the pre- and post-training

www.manaraa.com

assessment. Perhaps this background information could also be used to identify those who need training.

Limitations and Future Directions

One major limitation of this study is the pretest-posttest no control design to test for improvement of sensitivity attributable to training. The strongest case for causality, in terms of the phishing email training resulting in improved phishing email detection, would be made with a true experimental design with a control group that did not receive training, random assignment to groups, and pre- and post-testing. However, for this field study, organizational constraints prevented a true experimental design from being feasible. At TxDOT, all employees are required to complete the phishing email training within 90 days of employment and then annually after that date. TxDOT also cannot allow new employees to all be used as the control group because they have too many onboarding tasks to be burdened with the survey. Moreover, there would likely be significant selection bias introduced if only new employees were in the control group compared with higher tenured employees in the training groups.

Still, quasi-experimental designs are commonly used in organizational setting because of similar constraints (Condon & Revelle, 2014). Sackett and Mullen (1993) argued in their article on design alternatives to the formal experimental design that a pretest-posttest no control design paired with careful investigation into the plausibility of various threats to internal validity does still permit the computation of a measure of change. One potential threat is that the phishing simulation before the training introduced testing effects that resulted in the increased performance on the post-training assessment. The use of parallel forms for the phishing email simulation likely reduced the influence practice effects to some extent, however without a control group, there is no way to directly test for these practice effects.

www.manaraa.com

Another threat to the internal validity of the study is that the lack of a control group increases risk that there are potential alternative explanations for the change in phishing detection ability, other than the training itself. The risk of potential alternative explanations outside of training was evaluated to the extent possible. The Director of Workforce Development was asked whether there were any other alternative explanations (e.g., history threats due to other experiences that occurred during training) for the observed change in phishing detection ability after training and did not disclose any concerns. Moreover, the design of the current study where employees took the self-paced training at different times on their own (spread out over the course of two to three months), reduces the likelihood of history threats to internal validity.

Another limitation worth noting that the design constraints required for using SDT metrics impose considerable tradeoffs with regard to participant reactions and participant fatigue. Specifically, testing of the equal-variance assumption requires the inclusion of confidence ratings. Including confidence ratings adds an extra item for each stimulus, which meant 30 extra items for each the pre- and post-training assessments in this study. Another design constraint for using SDT metrics is including a large number of stimuli with varied signal strength to ensure that there are not too many participants who get a 100% hit rate (correctly identify all phishing emails) or 0% false alarm rate (correctly identify all legitimate emails). In this study, 10 phishing emails and 20 legitimate emails were included in each assessment. Although the stimuli were carefully designed and pilot tested, there were still a large proportion of participants who achieved a 100% hit rate, particularly in the post-training assessment.

This high proportion of participants with a perfect hit rate is in contrast to previous work with these same phishing email stimuli where less than 10% of the participants (N=19) attained a 100% hit rate (Martin, 2017). This difference is likely due in part to the different samples. The

www.manaraa.com

present study used TxDOT employees who were encouraged by their organization to take the email simulations, whereas the previous study used mTurk workers who likely had less vested interest in performing well on the email simulation.

With 30 emails and 30 confidence ratings in each simulation, there was much negative feedback from participants regarding the length of the simulations. This negative feedback was evident in participant comments (e.g., in a comment regarding the post-training survey a participant said, "By the time I got to it, I'd had enough. The first "survey" was grueling, the training was long and dull. And now I have to answer ANOTHER 30 QUESTIONS and rate my confidence on my answers again? It's just too much."). Further, it could be inferred that the high attrition rate between pre- and post-training surveys (46%) is in part due to negative reactions to the pre-training survey. Future researchers who use a simulation email inbox and SDT metrics for evaluating phishing email susceptibility should consider ways to achieve a better balance between the design constraints and participant reactions. Perhaps gamifying the email simulations by providing a superior user interface and feedback would reduce participant fatigue and negative reactions by keeping participants engaged in the task.

Another future direction for research would be investigating ways to manipulate response bias in phishing email tasks. Response bias did not significantly differ across any of the conditions assessed in this study. It would be interesting to investigate under which conditions response bias does differ. Incentives (e.g., rewards for identifying and forwarding phishing emails to IT) would likely be influential in changing response bias. Particularly, finding which manipulations are successful for changing response bias would be important for organizations that wish to achieve an optimal response criterion in order to maximize or minimize certain outcomes. For instance, if a company wanted to minimize the chance of a "miss", or employees

www.manaraa.com

falling for phishing emails, they would want a liberal criterion like those observed in this study where employees are more cautious and vigilant in their responses.

Another way to manipulate response bias through attitudinal change could be through applications of social psychology research. Exploring how the fear appeal message could be changed to maximize persuasion through the use of the central route to persuasion (Petty & Cacioppo, 1986). Using the central route to persuasion to provide critical information about the dangers of phishing emails would hopefully result in attitudinal change through careful scrutiny of the message. Other features of the message, such as the likeability, credibility, and emotional appeals.

Another area for future research is evaluating the effectiveness of the training intervention over time. This study did not have a time measure of the time between the training was completed and the post-training survey was completed. It would be useful to evaluate how much the effect of the training diminishes over time. Blume et al. (2010) found that the effects of learning outcomes (post-training knowledge and post-training self-efficacy) decreased over time. It is likely that most participants took the post-training survey soon after completing the training, so the large observed effect of the training may only be so large because of the small time lag between training and the post-training learning measure.

A substantial area for future research concerns the refinement of the performance space for phishing email detection performance and the further evaluation of predictors for this area of performance. Overall, research conducted over the last 10 years shows largely mixed results for predicting phishing susceptibility. Though it stands to reason that conscientious individuals who tend to be dutiful in terms of following procedures and have high attention to detail would be less susceptible to phishing emails (Darwish, Zarka, & Aloul, 2012; Parrish, Bailey, & Courtney,

www.manaraa.com

2009), several studies have found a null effect of conscientiousness on phishing susceptibility (Halevi et al., 2013; Lawson et al., 2017; Martin et al., 2018; Pattinson et al., 2011; Schrammel, Köffel, & Tscheligi, 2009; Sudzina & Pavlicek, 2017). Still, there was one study that found that high levels of conscientiousness predicted low levels of cyber-attack victimization based on a self-reported behavioral intention measure (based on four social network and social engineering attack scenarios) in a sample of 316 faculty and students at two universities in Saudi Arabia (Albladi & George, 2017). However, in a small sample (N=40) of employees in India Halevi, Memon, & Nov (2015) found that individuals high in conscientious were *more* likely to click on a link in a simulated phishing email ($r = .32$, $p < .05$). Thus, the existing research suggests that more research is needed to clarify the relationship between conscientiousness and phishing susceptibility.

In addition to conscientiousness, some researchers hypothesized that high levels of agreeableness would predict security risks in terms of individuals more susceptible to phishing emails (Darwish et al., 2012). Agreeable individuals tend to be more trusting, which could lead them to be more easily influenced my social engineering tactics used in phishing emails. However, research shows mixed results for agreeableness with the majority of studies reporting non-significant results (Halevi et al., 2013, 2015; Lawson et al., 2017; McBride et al., 2012; Pattinson et al., 2011; Schrammel et al., 2009; Sudzina & Pavlicek, 2017) and only one study demonstrating a small effect where individuals high in agreeableness were more susceptible to cyber-attack victimization (Albladi & George, 2017).

One explanation for these mixed results is that the bandwidth-fidelity dilemma needs to be taken into consideration in these relationships. Since the criterion of interest (phishing susceptibility) is a small facet of job performance, construct correspondence would suggest that

www.manaraa.com

lower order traits (facets of personality traits) would better predict phishing susceptibility (Judge, Rodell, Klinger, Simon, & Crawford, 2013). For instance, instead of predicting phishing susceptibility with agreeableness and conscientiousness, one could examine facets of these constructs, such as trust (a facet of agreeableness) and dutifulness (a facet of conscientiousness).

Conclusion

The present study had three primary goals. The first goal was to evaluate the effectiveness of phishing email training with regard to informational approaches and fear-appeals. Two email simulations were developed to assess phishing email susceptibility before and after the training and fear appeal interventions. While the informational training was effective at improving participants' phishing email detection ability, the fear-appeals did not influence the phishing email susceptibility outcomes. The second goal was to distinguish between sensitivity and response bias in phishing susceptibility and evaluate the differential impact that training has on each of the two outcomes. The informational approach to training improved phishing email detection ability but did not significantly change response bias. The third goal was to understand the influence of the larger training context on training success. To this aim, employees answered questions pertaining to training reactions, cognitive ability, and demographics, which were evaluated for their effects on baseline phishing susceptibility (pretest scores) and training success (changes in phishing sensitivity and response bias between the pretest and posttest). Training reactions were found to predict training success, while cognitive ability predicted baseline phishing susceptibility. By using psychological models, such as SDT, to evaluate phishing susceptibility in a training context, the present findings yield novel insights into the increasingly important role all employees play in an organization's cyber-security.

www.manaraa.com

REFERENCES

Albladi, S. M., & George, R. S. (2017). Personality traits and cyber-attack victimisation: Multiple mediation analysis. *Internet of Things Business Models, Users, and Networks, 2017*, 1–6. IEEE.

Alliger, G. M., Tannenbaum, S. I., Bennett Jr, W., Traver, H., & Shotland, A. (1997). A meta-analysis of the relations among training criteria. *Personnel Psychology*, *50*(2), 341–358. https://doi.org/10/dn84s7

Alnajim, A., & Munro, M. (2008). An evaluation of users' tips effectiveness for Phishing websites detection. *2008 Third International Conference on Digital Information Management*, 63–68. https://doi.org/10.1109/ICDIM.2008.4746717

Alnajim, A., & Munro, M. (2009). An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection. *2009 Sixth International Conference on Information Technology: New Generations*, 405–410. https://doi.org/10.1109/ITNG.2009.109

Anand-Keller, P. (1999). Converting the Unconverted: The Effect of Inclination and Opportunity to Discount Health-Related Fear Appeals. *Journal of Applied Psychology*, *84*(3), 403–415. https://doi.org/10/c9hcjn

Arce, I. (2003). The weakest link revisited [information security]. *IEEE Security & Privacy*, *99*(2), 72–76. https://doi.org/10/bn4755

Arthur, W., Bennett, W., Edens, P. S., & Bell, S. T. (2003). Effectiveness of training in organizations: A meta-analysis of design and evaluation features. *Journal of Applied Psychology*, *88*(2), 234–245. https://doi.org/10/dgwh7m

www.manaraa.com

Baldwin, T. T., & Ford, J. K. (1988). TRANSFER OF TRAINING: A REVIEW AND DIRECTIONS FOR FUTURE RESEARCH. *Personnel Psychology*, *41*(1), 63–105. https://doi.org/10/cq3btj

Barrick, M. R., & Mount, M. K. (1991). THE BIG FIVE PERSONALITY DIMENSIONS AND JOB PERFORMANCE: A META-ANALYSIS. *Personnel Psychology*, *44*(1), 1–26. https://doi.org/10/hjv

Bell, B. S., Tannenbaum, S. I., Ford, J. K., Noe, R. A., & Kraiger, K. (2017). 100 years of training and development research: What we know and where we should go. *Journal of Applied Psychology*, *102*(3), 305–323. https://doi.org/10/f9xt5j

Beyer, R. E., & Brummel, B. J. (2015). *Implementing Effective Cyber Security Training for End Users of Computer Networks*. 1–22.

Blume, B. D., Ford, J. K., Baldwin, T. T., & Huang, J. L. (2010). Transfer of Training: A Meta-Analytic Review. *Journal of Management*, *36*(4), 1065–1105. https://doi.org/10/ftwgxk

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). *What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors*. https://doi.org/10/gfc89c

Canfield, C. I., Davis, A., Fischhoff, B., Forget, A., Pearman, S., & Thomas, J. (2017). Replication: Challenges in using data logs to validate phishing detection ability metrics. *Symposium on Usable Privacy and Security (SOUPS)*, *12*.

Canfield, C. I., & Fischhoff, B. (2018). Setting Priorities in Behavioral Interventions: An Application to Reducing Phishing Risk: Setting Priorities in Behavioral Interventions. *Risk Analysis*, *38*(4), 826–838. https://doi.org/10/gfgzbn

www.manaraa.com

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *58*(8), 1158–1172. https://doi.org/10/f9bv4t

Cascio, W. F., & Aguinis, H. (2005). *Applied psychology in human resource management*.

Chuchuen, C., & Chanvarasuth, P. (2015). *Relationship between Phishing Techniques and User Personality Model of Bangkok Internet Users*.

Colquitt, J. A., LePine, J. A., & Noe, R. A. (2000). Toward an integrative theory of training motivation: A meta-analytic path analysis of 20 years of research. *Journal of Applied Psychology*, *85*(5), 678–707. https://doi.org/10/b368fq

Condon, D. M., & Revelle, W. (2014). The international cognitive ability resource: Development and initial validation of a public-domain measure. *Intelligence*, *43*, 52–64. https://doi.org/10/f5xfj8

Cooper, D. P., Goldenberg, J. L., & Arndt, J. (2014). Perceived efficacy, conscious fear of death and intentions to tan: Not all fear appeals are created equal. *British Journal of Health Psychology*, *19*(1), 1–15. https://doi.org/10/f5r9tn

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, *87*, 174–182. https://doi.org/10/gd5htc

Darwish, A., Zarka, A. E., & Aloul, F. (2012). Towards understanding phishing victims' profile. *2012 International Conference on Computer Systems and Industrial Informatics*, 1–5. https://doi.org/10.1109/ICCSII.2012.6454454

www.manaraa.com

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739–1747. https://doi.org/10/fxg9gb

De Dreu, C. K. W., Baas, M., & Nijstad, B. A. (2008). Hedonic tone and activation level in the mood-creativity link: Toward a dual pathway to creativity model. *Journal of Personality and Social Psychology*, *94*(5), 739–756. https://doi.org/10/ft2m72

Dorfman, D. D., & Alf, E. (1969). Maximum-likelihood estimation of parameters of signal-detection theory and determination of confidence intervals—rating-method data. *Journal of Mathematical Psychology*, *6*(3), 487–496. https://doi.org/10/ffkr64

El-Din, R. S., Cairns, P., & Clark, J. (2014). *It's all about me! The Influence of Personality on Susceptibility to Mobile Security Attacks*.

Evans, R. I., Rozelle, R. M., Lasater, T. M., Dembroski, T. M., & Allen, B. P. (1970). Fear arousal, persuasion, and actual versus implied behavioral change: new perspective utilizing a real-life dental hygiene program. *Journal of Personality and Social Psychology*, *16*(2), 220. https://doi.org/10/brvqjx

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. https://doi.org/10/b22kn7

Givens, T. (2004). States of Awareness, the Cooper Color Codes. *Sharpen the Blade*, *5*.

Goldstein, I. L., & Ford, J. K. (2002). *Training in organizations: Needs assessment, development, and evaluation*. Wadsworth/Thomson Learning.

Gordon, L. V., & Alf, E. F. (1962). The predictive validity of measured interest for Navy vocational training. *Journal of Applied Psychology*, *46*(3), 212. https://doi.org/10/c46qtj

www.manaraa.com

Green, D. M., & Swets, J. A. (1966). Signal detection theory and psychophysics. 1966. *New York*.

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. *ArXiv Preprint ArXiv:1301.7643*.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal*. https://doi.org/10/gfgzb8

Harrison, B., Vishwanath, A., & Rao, R. (2016). A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing. *System Sciences (HICSS), 2016 49th Hawaii International Conference On*, 5628–5634. IEEE.

Hass, J. W., Bagley, G. S., & Rogers, R. W. (1975). Coping with the Energy Crisis: Effects of Fear Appeals upon Attitudes Toward Energy Consumption. *Journal of Applied Psychology*, *60*(6), 754–756. https://doi.org/10/b7vpqc

Henthorne, T. L., LaTour, M. S., & Nataraajan, R. (1993). Fear appeals in print advertising: An analysis of arousal and ad response. *Journal of Advertising*, *22*(2), 59–69. https://doi.org/10/gfj766

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of Susceptibility to Scams in Older Adults Without Dementia. *Journal of Elder Abuse & Neglect*, *26*(2), 107–122. https://doi.org/10/gfgzb9

Jansen, J. (2018). *Do you bend or break?: preventing online banking fraud victimization through online resilience*.

www.manaraa.com

Jansen, J., & van Schaik, P. (2018). Persuading end users to act cautiously online: a fear appeals study on phishing. *Information and Computer Security*, *26*(3), 264–276. https://doi.org/10/gfgzcb

Jex, S. M., & Britt, T. W. (2014). *Organizational psychology: A scientist-practitioner approach*. John Wiley & Sons.

Judge, T. A., Rodell, J. B., Klinger, R. L., Simon, L. S., & Crawford, E. R. (2013). Hierarchical representations of the five-factor model of personality in predicting job performance: Integrating three organizing frameworks with two theoretical perspectives. *Journal of Applied Psychology*, *98*(6), 875–925. https://doi.org/10/bdbb

Keith, N., & Frese, M. (2008). Effectiveness of error management training: a meta-analysis. *Journal of Applied Psychology*, *93*(1), 59. https://doi.org/10/fbksqf

Kirkpatrick, D. L. (1959a). Techniques for evaluating training programs. *Journal of ASTD*, (13), 3–9.

Kirkpatrick, D. L. (1959b). Techniques for evaluating training programs: Part 2-Learning. *Journal OfASTD*, (13), 21–26.

Kirkpatrick, D. L. (1960a). Techniques for evaluating training programs: Part 3-Behavior. *Journal of ASTD*, (14), 13–18.

Kirkpatrick, D. L. (1960b). Techniques for evaluating training programs: Part 4-Results. *Journal of ASTD*, (14), 28–32.

Kirkpatrick, D. L. (1996). Great ideas revisited. *Training & Development*, (1), 54.

Kraiger, K., Ford, J. K., & Salas, E. (1993). Application of Cognitive, Skill-Based, and Affective Theories of Learning Outcomes to New Methods of Training Evaluation. *Journal of Applied Psychology*, 18. https://doi.org/10/db8xgf

www.manaraa.com

Kueider, A. M., Parisi, J. M., Gross, A. L., & Rebok, G. W. (2012). Computerized cognitive training with older adults: a systematic review. *PloS One*, *7*(7), e40588. https://doi.org/10/9ph

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: a real-word evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 1. https://doi.org/10.1145/1572532.1572536

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, 70–81. ACM.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 1–31. https://doi.org/10/ctgptw

Lawson, P., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *61*, 1331–1333. SAGE Publications Sage CA: Los Angeles, CA.

Lewis, I., Watson, B., Tay, R., & White, K. M. (2007). The role of fear appeals in improving driver safety: A review of the effectiveness of fear-arousing (threat) appeals in road safety advertising. *International Journal of Behavioral Consultation and Therapy*, *3*(2), 203. https://doi.org/10/gfj767

www.manaraa.com

Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy*, *204*(5), 44.

Lynn, S. K., & Barrett, L. F. (2014). "Utilizing" Signal Detection Theory. *Psychological Science*, *25*(9), 1663–1673. https://doi.org/10/f6kg9s

Macmillan, N. A., & Creelman, C. D. (2004). *Detection theory: A user's guide*. Psychology press.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10/cbzjj7

Martin, J. (2017). *Something Looks Phishy Here: Applications of Signal Detection Theory to Cyber-Security Behaviors in the Workplace*. University of South Florida, Tampa, FL.

Martin, J., Dubé, C., & Coovert, M. D. (2018). Signal Detection Theory (SDT) Is Effective for Modeling User Behavior Toward Phishing and Spear-Phishing Attacks. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *60*(8), 1179–1191. https://doi.org/10/gfgzch

Martocchio, J. J., & Hertenstein, E. J. (2003). Learning orientation and goal orientation context: Relationships with cognitive and affective learning outcomes. *Human Resource Development Quarterly*, *14*(4), 413–434. https://doi.org/10/b9vg7q

Mayhorn, C., & Nyeste, P. (2012). Training users to counteract phishing. *Work*, (Supplement 1), 3549–3552. https://doi.org/10/gfgzcj

McBride, M., Carter, L., & Warkentin, M. (2012). *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies*. RTI International – Institute for Homeland Security Solutions.

www.manaraa.com

McGehee, W., & Thayer, P. W. (1961). *Training in business and industry.*

Nguyen, C. (2018). *Learning not to take the bait - An examination of training methods and overlearning on phishing susceptibility*. University of Oklahoma.

Noe, R. A., & Colquitt, J. A. (2002). Planning for training impact: Principles of training effectiveness. *Creating, Implementing, and Managing Effective Training and Development*, 53–79.

Noe, R. A., & Schmitt, N. (1986). THE INFLUENCE OF TRAINEE ATTITUDES ON TRAINING EFFECTIVENESS: TEST OF A MODEL. *Personnel Psychology*, *39*(3), 497–523. https://doi.org/10/dr4k2m

Nohlberg, M. (2009). Why humans are the weakest link. In *Social and Human Elements of Information Security: Emerging Trends and Countermeasures* (pp. 15–26). IGI Global.

Parrish, J. L., Bailey, J. L., & Courtney, J. F. (2009). *A Personality Based Model for Determining Susceptibility to Phishing Attacks*. 285–296.

Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. A. (2011). Managing Phishing Emails: A Scenario-Based Experiment. *HAISA*, 74–85.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016). A Survey on Systems Security Metrics. *ACM Computing Surveys*, *49*(4), 1–35. https://doi.org/10/gc2hkj

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In *Communication and persuasion* (pp. 1–24). Springer.

PhishMe, Inc. (2017). *Enterprise Phishing Resiliency and Defense Report: Analysis of Susceptibility, Resiliency and Defense against Simulated and Real Phishing Attacks*.

Ree, M. J., & Earles, J. A. (1991). Predicting training success: Not much more than g. *Personnel Psychology*, *44*(2), 321–332. https://doi.org/10/dbpvhc

www.manaraa.com

Sackett, P. R., & Mullen, E. J. (1993). Beyond formal experimental design: Towards an expanded view of the training evaluation process. *Personnel Psychology*, *46*(3), 613–627. https://doi.org/10/c58zv9

Salas, E., & Cannon-Bowers, J. A. (2001). The Science of Training: A Decade of Progress. *Annual Review of Psychology*, *52*(1), 471–499. https://doi.org/10/crnpv5

Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The Science of Training and Development in Organizations: What Matters in Practice. *Psychological Science in the Public Interest*, *13*(2), 74–101. https://doi.org/10/gc2htd

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131. https://doi.org/10/cj5hm4

Schmidt, F. L., & Hunter, J. E. (1998). The Validity and Utility of Selection Methods in Personnel Psychology: Practical and Theoretical Implications of 85 Years of Research Findings. *Psychological Bulletin*, *124*(2), 162–174. https://doi.org/10/fd8vxp

Schneier, B. (2000). Secret and Lies. *Digital Security in a Networked World*.

Schrammel, J., Köffel, C., & Tscheligi, M. (2009). Personality traits, usage patterns and information disclosure in online communities. *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, 169–174. British Computer Society.

Sheeran, P., Harris, P. R., & Epton, T. (2014). Does heightening risk appraisals change people's intentions and behavior? A meta-analysis of experimental studies. *Psychological Bulletin*, *140*(2), 511–543. https://doi.org/10/f5tssq

www.manaraa.com

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, 373. https://doi.org/10.1145/1753326.1753383

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 - SOUPS '07*, 88. https://doi.org/10.1145/1280680.1280692

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. https://doi.org/10/f7b43g

Sjouwerman, S. (2018, October). *Levers of Human Deception: The Science & Methodology of Social Engineering*. Presented at the Florida Cyber Conference 2018, Tampa, FL.

Staggs, J., Beyer, R., Mol, M., Fisher, M., Brummel, B., & Hale, J. (2014). A perceptual taxonomy of contextual cues for cyber trust. *Journal for The Colloquium for Information System Security Education (CISSE)*, *2*, 152–169.

Stanislaw, H., & Todorov, N. (1999). Calculation of signal detection theory measures. *Behavior Research Methods, Instruments, & Computers*, *31*(1), 137–149. https://doi.org/10/ffg6rj

Sudzina, F., & Pavlicek, A. (2017). Propensity to Click on Suspicious Links: Impact of Gender, of Age, and of Personality Traits. *30th Bled EConference Digital TransformationBled EConference*, 593–601. University of Maribor.

www.manaraa.com

Tan, J. A., Hall, R. J., & Boyce, C. (2003). The role of employee reactions in predicting training effectiveness. *Human Resource Development Quarterly*, *14*(4), 397–411. https://doi.org/10/bsckcx

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, *141*(6), 1178–1204. https://doi.org/10/f7wvhw

Taylor, P. J., Russ-Eft, D. F., & Chan, D. W. L. (2005). A Meta-Analytic Review of Behavior Modeling Training. *Journal of Applied Psychology*, *90*(4), 692–709. https://doi.org/10/ctnmnw

The International Cognitive Ability Resource Team. (2014). Retrieved from https://icar-project.com/

Thompson, L. E., Barnett, J. R., & Pearce, J. R. (2009). Scared straight? Fear-appeal anti-smoking campaigns, risk, self-efficacy and addiction. *Health, Risk & Society*, *11*(2), 181–196. https://doi.org/10/d47k73

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing password security through interactive fear appeals: A web-based field experiment. *System Sciences (HICSS), 2013 46th Hawaii International Conference On*, 2988–2997. IEEE.

Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, *41*(1), 13.

Wilson, K. A., Bedwell, W. L., Lazzara, E. H., Salas, E., Burke, C. S., Estock, J. L., … Conkey, C. (2009). Relationships Between Game Attributes and Learning Outcomes: Review and Research Proposals. *Simulation & Gaming*, *40*(2), 217–266. https://doi.org/10/cjpdrz

www.manaraa.com

Wixted, J. T. (2007). Dual-process theory and signal-detection theory of recognition memory. *Psychological Review*, *114*(1), 152. https://doi.org/10/bf3ssr

Wombat Security Technologies. (2018). *State of the Phish*.

Yerkes, R. M., & Dodson, J. D. (1908). The relation of strength of stimulus to rapidity of habit-formation. *Journal of Comparative Neurology and Psychology*, *18*(5), 459–482. https://doi.org/10/cfnwhw

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*, 1466–1470. SAGE Publications Sage CA: Los Angeles, CA.

www.manaraa.com

APPENDICES

www.manaraa.com

Appendix A: Recruitment Email

Gmail

Jaclyn Martin <jaclyn.martin28@gmail.com>

EL8474 – Securing the Human – Request for Feedback

1 message

Jaclyn Martin <QualtricsMailer@usf.edu> Sat, Jan 12, 2019 at 10:40 AM
Reply-To: Jaclyn Martin <jmartin85@mail.usf.edu>
To: test <jaclyn.martin28@gmail.com>

Dear TxDOT Team Member,

Our training records indicate you're coming due for your annual "Securing the Human" training (EL8474).

TxDOT's Workforce Development team is looking for your help in evaluating this training. If you can spare the time, then I would like you to complete two online surveys – one before you take EL8474 and one after you take your annual training. We estimate taking the two surveys and the training will take a total of about *2 hours* to complete.

Step 1: Complete *pre-training* survey – https://usf.az1.qualtrics.com/jfe/form/SV_1QX9pIK59c0y1iB?Q_DL=eQGJVbXtjkGmD65_1QX9pIK59c0y1iB_MLRP_b8EoxTJFuLuzMS9&Q_CHL=email

- Please copy and paste the pre-training survey link into your browser
- The first page of the survey will ask you for your respondent ID number. Please enter the ID number (10003) into the form
- This survey will take approximately **40 minutes** to complete

Step 2: Take the training - Securing the Human (EL8474) - which should take **30 minutes to 1 hour**

Step 3: Complete *post-training* survey - https://usf.az1.qualtrics.com/jfe/form/SV_7aHB0vFnkNphC3b?Q_DL=4T10Z30Ce1SIE3b_7aHB0vFnkNphC3b_MLRP_0wx1HJgQXFWzlgd&Q_CHL=gl?Survey=PostTraining

- Please copy and paste the post-training survey link into your browser
- The first page of the survey will ask you for your respondent ID number. Please enter the ID number (10003) into the form
- This survey will take approximately **20 minutes** to complete

Thank you for your help in making the training better for the future.

Sincerely,
Jackie Martin (University of South Florida) and Chris Young, Director of Workfore Development, HRD

Participation in this survey is voluntary. With that being said, I would like to emphasize that your voice, opinions, and beliefs are very important for making positive change in the training program. The post-training assessment includes several questions regarding your evaluation of the training and includes space for you to include comments and/or suggestions.

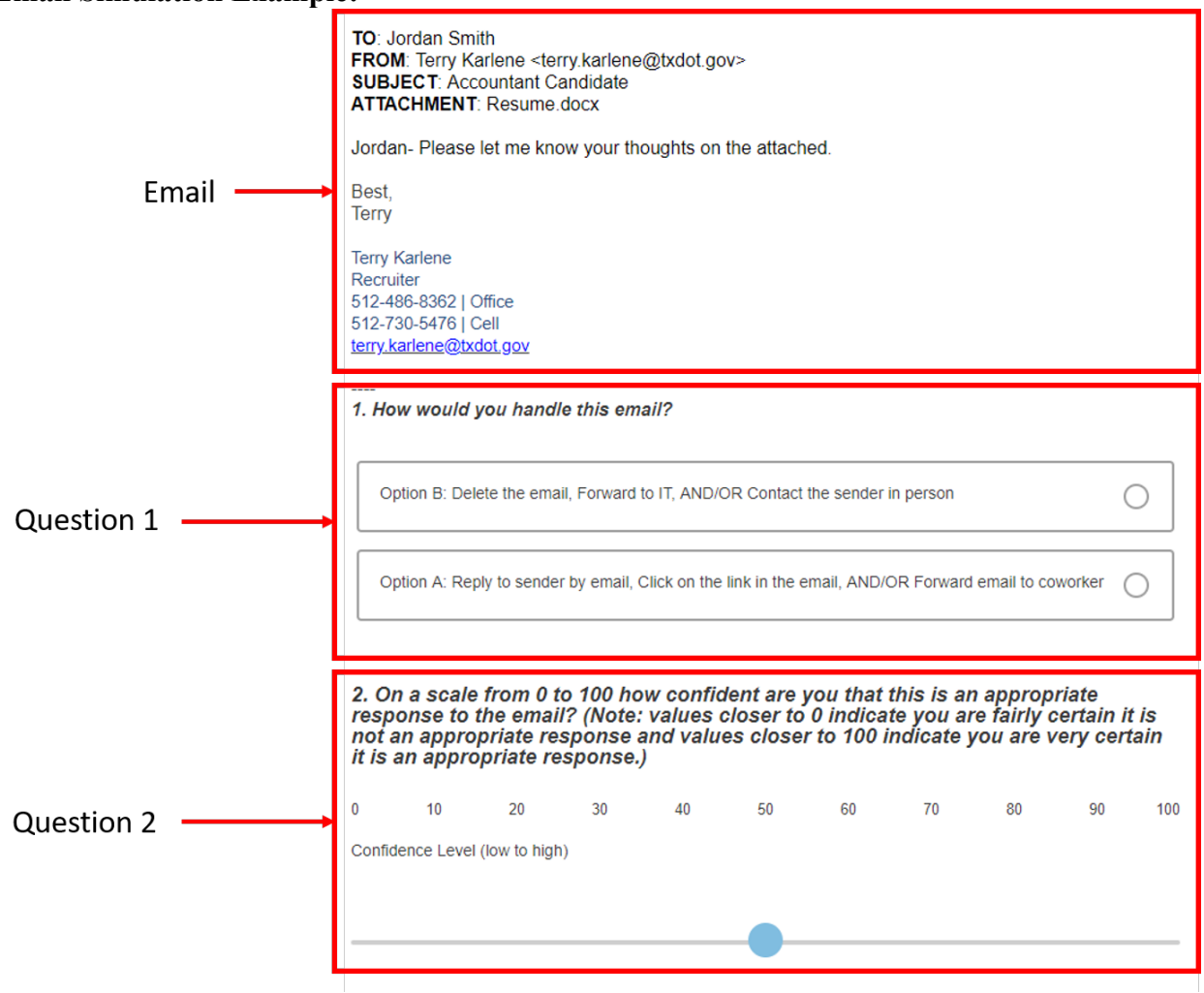
The University of South Florida has donated their time to create and analyze the survey data collected. All survey responses are anonymous and will not be connected to you by name. Your pre-training and post-training survey will be connected by a unique respondent ID number (10003). All results will be reported to TxDOT at the group level. Should you have any questions about the survey, please contact Jackie Martin from the USF research team at jmartin85@mail.usf.edu. If you have any questions about your rights as a research participant, please contact the University of South Florida IRB at (813) 974-5638 or contact by email at RSCH-IRB@usf.edu (Pro00038255).

To opt out of future emails click the following link: https://usf.az1.qualtrics.com/CP/Register.php?OptOut=true&RID=MLRP_b8EoxTJFuLuzMS9&LID=UR_6Fh5lu44UCztlPf&BT=dXNm&_=1

www.manaraa.com

Appendix B: Phishing Susceptibility Measure

Email Simulation Example:



Participants were prompted with 30 emails, presented one email at a time (see example above). There were two questions to answer with each email.

Question 1 asked how they would handle the email and gives two response options (Option A and Option B). *Option A* details actions someone may take to immediately address the sender's email (reply to the sender by email, click on the link in the email, forward the email to a coworker) while *Option B* details actions someone may take to get rid of or vet a suspicious email (delete the email, forward to IT, contact the sender in person).

Question 2 asked respondents to indicate how confident they are that the action they chose is appropriate for the email.

www.manaraa.com

Appendix C: Email Stimuli

Pre-Training Stimuli:

L1

TO: Jordan Smith
FROM: Jeff Pratt <jeff.pratt@happie.com>
SUBJECT: Working for TxDOT

Jordan-

Wanted to follow up on my previous messages introducing you to Happie. We run exclusive, highly effective online events where employers meet carefully-selected candidates in a fun 60 minute speed dating format.

Let me know if you have 5 minutes to connect over the phone.

Jeff

Jeff Pratt
Sr. Business Development Specialist
(216) 570-2458 | Happie
@GetHappie | @happie_jeff

L2

TO: Jordan Smith
FROM: Marje Darren <mdarren@goscoutgo.com>
SUBJECT: Pending candidates in Scout for Sr. Accountant

Hi Jordan,

I wanted to follow up and let you know that you still have 2 candidates pending feedback in Scout for the Sr. Accountant role. Let me know if you have any questions about reviewing or taking action!

Thanks,

Marje Darren
Account Manager
mdarren@goscoutgo.com
goscout***go***.com

Notice: This e-mail may contain confidential and/or privileged information and is intended solely for the person or entity to which it is addressed. Any unauthorized review, dissemination, copying, disclosure or distribution or other use of this e-mail by persons or entities other than the addressee is prohibited. If you are not the intended recipient please notify the sender immediately and destroy this e-mail.

www.manaraa.com

L3

TO: Jordan Smith
FROM: Monster <route@monster.com>
SUBJECT: Monster Resume #gygas9znvakbjhj9 Sr. Accountant 492 163188873
ATTACHMENT: MitalResume2019.docx

Hello,

Great news! This candidate has just applied for your Sr. Accountant position. For your convenience, we have stored this resume in the posting user's account on Monster.

Please do not reply to this email. All replies to this email go to a system email account at monster and are not forwarded to the job candidate.

Attachment format is according with the document provided by the applicant and checked for viruses.

Candidate Contact Information

Candidate Name:
Clara Mital

Candidate Location:
Austin , TX , 78701

Mobile:
241-575-1134

Home:
N/A

Email:
claramital@gmail.com

Contact Preference:
Email

Application Summary

Job Title:
Sr. Accountant

Job ID:
163188873

Application Date:
02/04/19

Resume Updated:
02/04/19

Career Level:
Experienced (Non-Manager)

Relocation:
Will Not Relocate

Rating:
Not Rated

Highest Education:
Bachelor's Degree

Work Status:
US - I am authorized to work in this country for any employer.

Screening Score:
no specified

Work Experience:
More than - years

Login to your account to access this resume.
Login to your account to access all resumes for the Sr. Accountant position.

If you have any questions, a Customer Service Representative is available to assist you at 1-800-MONSTER (666-7837), Monday - Friday from 8:30am - 5:30pm EST.

Sincerely,

The Monster Service Team

www.manaraa.com

L5

TO: Jordan Smith
FROM: John Pop <john.pop@gmail.com>
SUBJECT: Job Application for Senior Accountant

Hi Jordan,

As per the open job position at your company, I am applying for the Senior Accountant position. I have 7+ years of working experience in the field of finance. I have attached my resume with the following link:https://www.dropbox.com/s/uvp

I look forward to your response.

Thanks,
John Pop

L6

TO: Jordan Smith
FROM: Jeff Gordon <jeff.gordon@etgjobs.com>
SUBJECT: Resume for Consideration - Brent Larrie/Senior Accountant
ATTACHMENT: Larrie_Resume.docx

Hi Jordan,

Please find the resume of Brent Larrie for your Senior Accountant position, Brenthas his Master of Science Degree in Accounting and his Bachelor's Degree in Business Administration with 5+ years of overall experience.
He has solid communication skills and is extremely motivated.

He lives in Allendale, Tx. And can phone interview in the afternoons, though it is better for him to personally interview after 3 cst.

All-inclusive hourly rate - $80.30
Salary expectations: 100-115K

Please note that he has other positions that he is actively interviewing for, If you have interest, we need to move quickly.

Thanks!

Jeff Gordon
National Accounts Manager
Engineering Technical Group/ETG
1-888-256-4346
www.linkedin.com/in/jeffgordon/
www.etgjobs.com

www.manaraa.com

L7

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Automatic Reply: Out of Office

Greetings,

I am out of the office from today until 3/8. Please contact Jordan Smith, jordan.smith@txdot.gov, if needed.

Thanks,

Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

L8

TO: Jordan Smith
FROM: Jeff Pratt <jeff.pratt@happie.com>
SUBJECT: Growing the TxDOT Team

Jordan - touching base on my previous note. Are you looking to hire finance talent?

Happie is a fast, fun and innovative way to interview candidates. Our time-saving speed dating format allows you to meet 6 top tier candidates within an hour.

Shoot me back a note if you're interested in filling the candidate pipeline for TxDOT.

Happie hiring!

Jeff

Jeff Pratt
Sr. Business Development Specialist
(216) 570-2458 | Happie
@GetHappie | @happie_jeff

www.manaraa.com

L9

TO: Jordan Smith
FROM: Wren Buffet <invitations@linkedin.com>
SUBJECT: Jordan, please add me to your LinkedIn network

Jordan Smith

Hi Jordan, I'd like to join your LinkedIn network.

Wren Buffet

Accountant at Infosoft, Inc.
San Francisco Bay Area

Accept View profile

Unsubscribe | Help

You are receiving Invitation emails.

This email was intended for Jordan Smith.
Learn why we included this.

LinkedIn

© 2018 LinkedIn Corporation, 1000 West Maude Avenue, Sunnyvale, CA 94085. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

www.manaraa.com

L10

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Offer Letter - Accountant D. Marshall
ATTACHMENT: Offer Letter Marshall.docx

Jordan,

I should've copied you on this when I sent it out but I forgot. I sent out an offer letter to Beacon Hill this morning for David Marshall for the Accountant role. I have attached a copy of the offer letter. Hopefully you will be getting it back by Friday.

Thanks,
Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell

terry.karlene@txdot.gov

L11

TO: Jordan Smith
FROM: Amanda Caro <acaro1245@gmail.com>
SUBJECT: Accountant Position

Hi,

Thursday anytime from 10am to 5 pm cst would be suitable for me.

Thanks
Amanda

<jordan.smith@txdot.gov> wrote:

Thank you for submitting your resume. Our hiring team has reviewed your resume and would like to speak with you in more detail concerning an opportunity. Please reply and indicate when you can be available for a 5-10 minute phone screen. For reference, I have attached the position description. I look forward to speaking with you.

Best,

TxDOT Recruiting Team

Powered by Taleo
www.taleo.com

www.manaraa.com

L12

TO: Jordan Smith
FROM: Anita Mullen <anita.mullen@experthiring.net>
SUBJECT: Appropriate Person

Hi Jordan -

I was informed that you are the appropriate person to contact in regards to any recruitment efforts on behalf of TxDOT. I've had my recruitment team work on a role for you through Scout however I see that the job (Senior Accountant) has been taken down so I'm assuming it is filled? Also, I don't see any other openings on Scout anymore, are you no longer using this portal?

Do you have any openings that you would like to have us recruit for? I can get my recruitment team started on any opening you need to see good resumes for.

Looking forward to hearing from you soon!

Sincerely,

Anita Mullen
Business Development Account Manager
(732) 582 - 0457 Direct
(732) 298 - 6347 EXT 125 Office
mailto:anita.mullen@experthiring.net
http://www.ExpertHiring.com/
Connect on Linked in

www.manaraa.com

L13

TO: Jordan Smith

FROM: Amanda Caro <acaro1245@gmail.com>

SUBJECT: Accountant Opportunity

Good Afternoon Jordan,

Thank you again for the opportunity. I look forward to speaking with you on Thursday, March 31st at 10:30a.m.

Best Regards,

Amanda Caro

On Tuesday, Mar 29 at 8:24 AM, Jordan Smith

<jordan.smith@txdot.gov> wrote:

Good morning Amanda,

Thursday at 10:30am EST works best for me. I will call you then. I look forward to speaking with you!

My best,

Jordan

Jordan Smith

Business Services Coordinator

512-486-3892 | Office

512-730-2378 | Cell

jordan.smith@txdot.gov

www.manaraa.com

L14

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Candidates for Accountant Positions

Hi Jordan,

Are you free at all today to discuss the candidates for the Senior Accountant Position?

Thank you!
Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

L15

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Updates

So far all 3 of the positions I am recruiting for have been more difficult than expected. For the Sr. Financial Specialist – the issue has been salary – over 10 candidates identified – not one will accept less than $100K to $145K. For the Senior Accountant salary and clearance have been the show stopper – those that have been identified with clearance want more than $100K. For the Junior Accountant – salary has been the road block – all candidates screened want over $80K and higher.

The ad on NortonNet has not produced any viable candidates. I continue to search Dice & Monster each day and network though my connections.

Let me know how you want to proceed. Thanks

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

www.manaraa.com

L16

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Marshall - Offer Letter

Hi Jordan,

I just wanted to update you that I still haven't heard anything back since we sent the offer letter. Do you think I should follow up at this point?

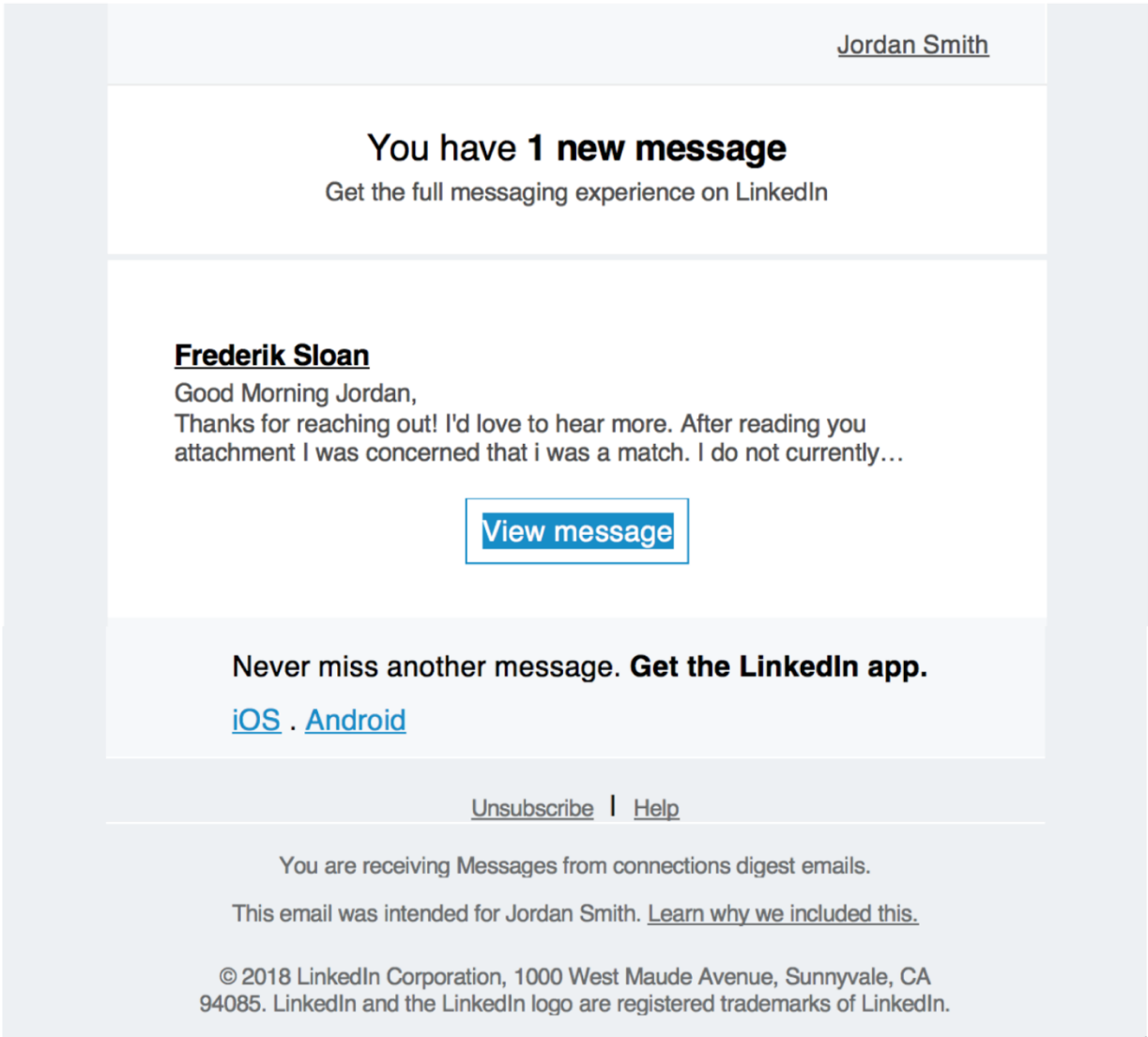
Best,
Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

www.manaraa.com

L17

TO: Jordan Smith
FROM: Frederik Sloan via LinkedIn <650c558c-1fa6-4c42-8520-46669f0814a3@reply.linkedin.com>
SUBJECT: Frederik sent you a new message



www.manaraa.com

L18

TO: Jordan Smith
FROM: Brent Larrie <brent.larrie@icloud.com>
SUBJECT: Interview

Jordan,

I had a family emergency in the wee hours of the morning so unfortunately I'm unable to meet with the interviewer.

Brent Larrie

Today, at 08:40 AM, Jordan Smith <jordan.smith@txdot.gov> wrote:

Good morning Brent,

This email is to confirm your face to face interview with Casey Johnson at 1:30pm today. The exact address is listed below. I look forward to hearing how it goes.

200 E Riverside Drive Austin TX 78704

My best,
Jordan Smith

Jordan Smith
Business Services Coordinator
512-486-3892 | Office
512-730-2378 | Cell
jordan.smith@txdot.gov

www.manaraa.com

L19

TO: Jordan Smith
FROM: Casey Johnson <cjohnson@txdot.gov>
SUBJECT: accountant
ATTACHMENT: Agenda.docx

Jordan,

Terry let me know that you two are meeting to discuss the candidates for the Accountant position. I'd like you to brief me on the updates this week. Please take a look at the attached for an agenda of key points I'd like to discuss.

Casey

Casey Johnson
Human Resources Manager
512-486-3287 | Office
512-730-4398 | Cell
cjohnson@txdot.gov

L20

TO: Jordan Smith
FROM: <no-reply@sharepointonline.com>
SUBJECT: Administrator has responded to your request for 'Accountant Candidates'

Good news. You now have access to 'Accountant Candidates'.

Go to the site

www.manaraa.com

L26

TO: Jordan Smith
FROM: Brent Larrie <oeu19@msc.com>
SUBJECT: Senior Accountant (Key Position) job opening - Brent

Brent Larrie's resume with contact details:
http://www.indeed.com/r/24e66f7are349ee4a0a1

Good morning Jordan,

Please share more details. I have some time to talk between 2:00 - 3pm.

Best regards,

Brent Larrie
(202) 650-2392

From: jordanviaindeed2_bop@indeedemail.com
To: oeu19@msn.com
Subject: Senior Accountant (Key Position) job opening - Brent

Hi Brent,

I found your resume on Indeed. Please reply to this email if you are interested in discussing the following Key Position on a proposal we are pursuing.

B-st,
Jordan

Jordan Smith
TxDOT
Business Services Coordinator
jordan.smith@txdot.gov

Message from Jordan at TxDOT.
Interested? Reply to this email to contact Jordan. Your contact details will be shared when you reply.
Not interested? Decline - Your contact details will not be shared.
Report Spam - This message is suspicious or fraudulent.

www.manaraa.com

P1

TO: Jordan Smith
FROM: Monster <protectone@monster.com>
SUBJECT: Monster Security

Dear Monster member,

We would like to remind you that we offer a number of tools to make finding a job easier and less stressful. While we do this, we need you to help us maintain this whole process secure. That's why we have come up with Monster ProtectOne Program.

Monster ProtectOne is a plan we have managed to develop while looking for a way to keep your information secure. Monster ProtectOne has at its base, a small utility that you need to install on the computer you use (most of the time) to access your Monster job seeker account. The utility will verify that the information you send to our server (username, password etc.) is safe.

Monster ProtectOne must be downloaded from:

http://www.monster.com/texis/jobseeker/Monster-ProtectOne.exe

P2

TO: Jordan Smith
FROM: IT Department <ithelp@txdot.gov>
SUBJECT: Account Expiration Notice

Dear User,

Your account profile will expire today.
Kindly Click Here to validate.

Sincerely,
IT Department

www.manaraa.com

P3

TO: Jordan Smith
FROM: web master <webmaster@beyond.com>
SUBJECT: 2019 Recruitment Plan
ATTACHMENT: 2019 Recruitment Plan.xls

Jordan-
I forward this file to you for review. Please open and view it.

P4

TO: Jordan Smith
FROM: HR <no-reply@hr-ad.com>
SUBJECT: Announcement: Change in Holiday Schedule

Colleagues,

The holiday schedule was adjusted with 2 extra days. You can see the new holiday schedule here.
Print it out and keep it handy.

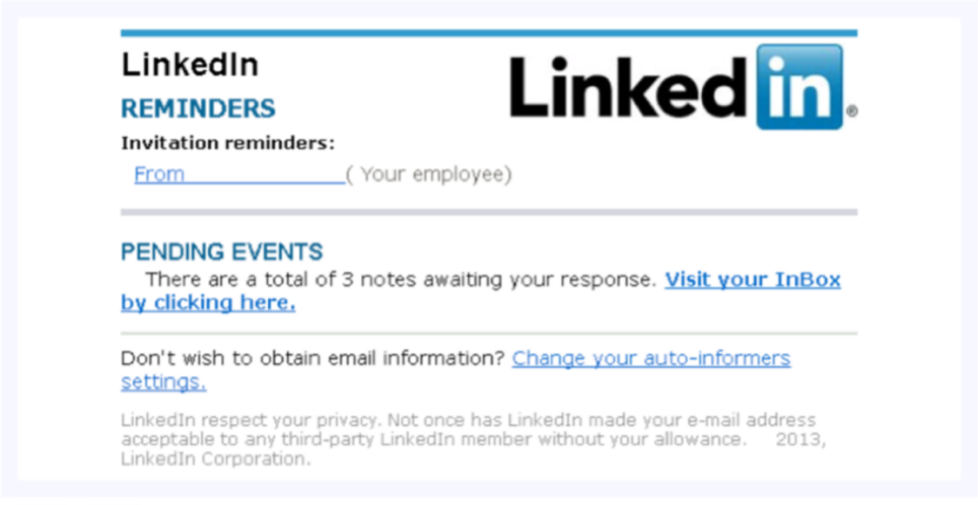
For any questions about the changes please contact your manager.
Enjoy the extra days!

Thank you,

HR Team

P5

TO: Jordan Smith
FROM: Linkedin <noreply@linkedin.com>
SUBJECT: Pending Invitations



www.manaraa.com

P6

TO: Jordan Smith
FROM: Verizon Services <verizonsupport@webmail.net>
SUBJECT: Email Notification:WARNING

It looks like somene is trying to acess your email account from an unrecognized device in (Netherlands).If you haven't recently signed in from an unrecognized device and believe someone may have accessed your account, please click on the below link to verify your account.

http://webmail.secured.net.verify.webmail.accountwebmail.net

Thank you,

webmail Account

Webmail respects your privacy. To learn more, please read our online privacy statement:

http://www.webmail.net/help/accounts/

P7

TO: Jordan Smith
FROM: Casey Johnson <cjohnson@txdot.gov>
SUBJECT: Documents

Please view important document below.

https://docs.google.com/document/d/1ymKBY-6-5OunMQFildGA7zj-2satkQK_n6Ct838EKA/edit

www.manaraa.com

P8

TO: Jordan Smith
FROM: <donotreply@adp.com>
SUBJECT: Account Confirmation Procedure Alert (IMPORTANT)

Dear EasyPayNet Customer,

As trusted custodian of our clients' payroll interests, we are committed to protecting our clients' entrusted information through ADP EasyPayNet Secure Access. As part of our ongoing effort to improve online security, we have decided to put an extra verification process to ensure only you have access to your access. It is all about your security.

Please click on **CONTINUE**

Sign in to continue the activation process to ensure your account security.

Thank you.

Sincerely,
Automated Data Processing, Inc.
Support Service

P9

TO: Jordan Smith
FROM: <srf3958@aol.com>
SUBJECT: Beat the clock

Not able to show full message.

You can view it by clicking here

www.manaraa.com

P10

TO: Jordan Smith
FROM: Casey Johnson <cjohnson@txdot.gov>
SUBJECT: Hi Jordan

Hi Jordan

Are you in the office? Kindly let me know because i need you to send out an important payment for me today.

Thank you.
Casey

Sent from my iPhone

www.manaraa.com

Post-Training Stimuli:

L4

TO: Jordan Smith
FROM: Casey Johnson <cjohnson@txdot.gov>
SUBJECT: Team Picnic

Hi all!

I know it's early, but I wanted to send out a heads up that our annual team picnic will be held on Saturday, June 29 (location TBD). All employees and their families are invited.

Last year's picnic provided an excellent chance to unwind after the busiest time of the year, and we all returned to work rejuvenated. We plan again to feature volleyball, softball, swimming and water-skiing (with at least three boats in the water!). Of course the chili cookoff will be the centerpiece of the movable feast we have planned.

The company will provide basic barbecue fare (including vegetarian entrees) and sporting equipment, but all are encouraged to bring along their own food and fun as well.

Please let Lyssa know by June 21 how many persons will be in your party. Get ready for a wonderful time!

-Casey

Casey Johnson
Human Resources Manager
512-486-3287 | Office
512-730-4398 | Cell
cjohnson@txdot.gov

L21

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Potential Sr. Accountant Rate

Good morning Jordan,

If we found the right candidate for the Sr. Accountant at a rate of $80-100/hr, so you think that would be do-able? This will help inform our recruiting strategy.

Thanks in advance for your thoughts,
Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

www.manaraa.com

L22

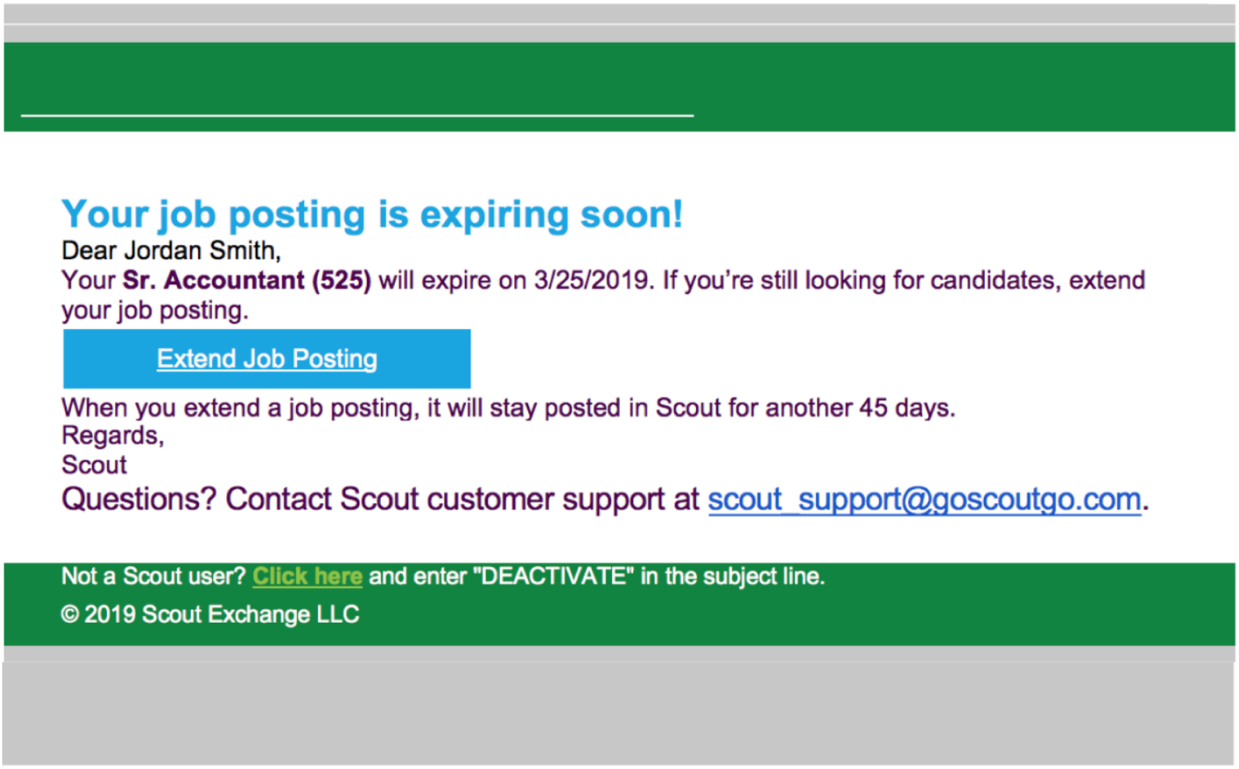
TO: Jordan Smith
FROM: Earl Mckinney <earlmckinney48@hotmail.com>
SUBJECT: Re: Phone Screen

Great - I am available Wed 1PM - EOD, Thurs 12PM - EOD and Fri 1PM - EOD

thanks,
E. Mckinney

L23

TO: Jordan Smith
FROM: <no-reply@goscoutgo.com>
SUBJECT: Your Sr. Accountant (525) posting is about to expire!



www.manaraa.com

L24

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Phone Screen
ATTACHMENT: Mckinney_resume_Oct_2018.docx

Hi Jordan,

Thank you for setting up the phone screen with Earl. I have his resume attached. Below are my notes from our conversation. Let me know if you want to proceed to a full in-person interview.

Currently looking? Yes.
Salary expectations? At least $80k (that's what he's currently earning)
Location? Lives in Rollingwood. Austin location would work fine.
Starting date? Two weeks notice for current job.

His resume looks great. He has all the skills we're looking for. Although there are a few gaps in between jobs.

Please let me know if you have any questions!

Best,
Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

www.manaraa.com

L25

TO: Jordan Smith
FROM: Casey Johnson <cjohnson@txdot.gov>
SUBJECT: Senior Accountant Position

Hi Jordan,

I've had a chance to review Earl Mckinney's resume and the notes from the phone screen. He looks like a suitable person for the position. Let's get a couple more candidates lined up and then we can decide who to invite to interview.
Keep up the good work!

Best,
Casey

Casey Johnson
Human Resources Manager
512-486-3287 | Office
512-730-4398 | Cell
cjohnson@txdot.gov

L27

TO: Jordan Smith
FROM: Gage Jasper <gage_jasper@yahoo.com>
SUBJECT: Senior Accountant Position job opening – Gage

Gage Jasper's resume with contact details:
http://www.indeed.com/r/9ae24364b4afc325145c4

Hi Jordan,

Good afternoon. Thank you for reaching out. Currently, I am on a contract and cannot commit to an upcoming proposal. If my availability opens up, I will reach out.

Have a great week.

Gage Jasper

***
Gage R. Jasper
gage_jasper@yahoo.com

www.manaraa.com

L28

TO: Jordan Smith
FROM: Jeff Pratt <jeff.pratt@happie.com>
SUBJECT: Growing the TxDOT Finance Team

Jordan - touching base on my previous note. Are you looking to hire finance talent?

Happie is a fast, fun and innovative way to interview candidates. Our time-saving speed dating format allows you to meet 6 top tier candidates within an hour.

Shoot me back a note if you're interested in filling the candidate pipeline for TxDOT.

Happie hiring!

Jeff

Jeff Pratt
Sr. Business Development Specialist
(216) 570-2458 | Happie
@GetHappie | @happie_jeff

www.manaraa.com

L29

TO: Jordan Smith
FROM: Tracking Updates <TrackingUpdates@fedex.com>
SUBJECT: FedEx Shipment 440718496974 Delivered

This tracking update has been requested by:

Company Name: OFFICEDEPOT.COM
Name: Shipping Dept.
E-mail: shipping@officedepot.com

Our records indicate that the following shipment has been delivered:

Reference: 3414337
Ship date: May 21, 2019
Signed for by: A.WALTER
Delivery location: WESTON, FL
Delivered to: Shipping/Receiving
Delivery date: Wed, 5/23/2019 12:41 pm
Service type: FedEx 2Day
Packaging type: FedEx Pak
Number of pieces: 1
Weight: 1.00 lb.
Special handling/Services Deliver Weekday
Standard transit: 5/23/2019 by 4:30 pm

Tracking number: 440718496974

Shipper Information	Recipient Information
Shipping Dept.	Jordan Smith
OFFICEDEPOT.COM	
2924 West Corporate Lakes St	16901 Melford Blvd.
WESTON	Austin
FL	TX
US	US
33331	78701

Please do not respond to this message. This email was sent from an unattended mailbox. This report was generated at approximately 2:46 PM CDT on 05/23/2019.

All weights are estimated.

The shipment is scheduled for delivery on or before the scheduled delivery displayed above. FedEx does not determine money-back guarantee or delay claim requests based on the scheduled delivery. Please see the FedEx Service Guide for terms and conditions of service, including the FedEx Money-Back Guarantee, or contact your FedEx customer support representative.

To track the status of this shipment online, please use the following:
https://www.fedex.com/apps/fedextrack/?action=track&tracknumbers=440718496974&language=en&opco=FX&clientype=ivother

Standard transit is the date and time the package is scheduled to be delivered by, based on the selected service, destination and ship date. Limitations and exceptions may apply. Please see the FedEx Service Guide for terms and conditions of service, including the FedEx Money-Back Guarantee, or contact your FedEx Customer Support representative.

© 2019 Federal Express Corporation. The content of this message is protected by copyright and trademark laws under U.S. and international law. You can access our privacy policy by searching the term on fedex.com. All rights reserved.

Thank you for your business.
...

[Message clipped] View entire message

www.manaraa.com

L30

TO: Jordan Smith

FROM: Sreepath <sreepath@scintillasoft.com>

SUBJECT: Hotlist

Hi Associate,

Hope doing great today! This is Sreepath from Scintilla soft working as Business Development Executive.

We are specialized in Data warehouse tools, we have about 100 analysts working with different clients around USA. I request you to include my email id sreepath@scintillasoft.com

Look forward to work with you. Please find the below hotlist

NAME	SKILL	LOCATION	AVAILABILITY	RELOCATOIN
RAGHU	ORACLE APEX	Columbus, OH	ASAP	OPEN
Nandini	SAP - Security/GRC Analyst	Atlanta, GA	ASAP	OPEN
Sowjanya	Oracle OBIEE	Richmond, VA	ASAP	OPEN
SUDHA	JAVA DEV	Atlanta, GA	ASAP	OPEN
DIVYA	JAVA DEV	Rockville, MD	ASAP	OPEN
ANKIT	JAVA DEV	Beaverton, OR	ASAP	OPEN
Divya Sree	JAVA DEV	Louisville, KY	ASAP	OPEN
Sai Swathi	SharePoint Developer	Los Angeles, CA	ASAP	OPEN

www.manaraa.com

L31

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Candidates for Accountant Positions

Hi Jordan,

Are you free at all today to discuss the candidates for the Accountant Positions?

Thank you!
Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

www.manaraa.com

L32

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: RE: Salary for David

Hi Jordan

David is looking for 82-87K when he would roll over permanently. Please let me know if you need anything else! Thank you.

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

TO: Terry Karlene
FROM: Jordan Smith <jordan.smith@txdot.gov
SUBJECT: Salary for David

Good afternoon Terry,

What salary was discussed for David when he converts to TxDOT full time?

My best,

Jordan Smith
Business Services Coordinator
512-486-3892 | Office
512-730-2378 | Cell
jordan.smith@txdot.gov

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. If you are not the intended recipient, you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

L33

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: accountant

Jordan I have a clears Accountant and wanted to check if there is a need at this point... He is currently located in the Austin area.

Sent from my iPhone

www.manaraa.com

L34

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Re: Accountant Candidate
ATTACHMENT: Caro Resume.docx

Sorry! Forgot the attachment...

L35

TO: Jordan Smith
FROM: Leah Brandon <bleah@latitudeinc.net>
SUBJECT: Latitude Inc. staffing services-Leah Brandon

Hi Jordan,

It was a pleasure speaking with you this morning. Latitude is a local full service HR solutions provider that specializes in IT, Engineering, Accounting, Finance and Admin positions. I have a team of 9 recruiters on staff and can be flexible with our rates. Below is a link to our website for your review. Keep me posted if anything comes up that Latitude can assist with and enjoy the rest of your week.

www.latitudeinc.net

Best regards,

Leah Brandon
Senior Account Manager
Latitude Inc.
443-561-0151
443-561-0157 Fax
www.latitudeinc.net
bleah@latitudeinc.net

L36

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov
SUBJECT: late

Hi Jordan,

I'm so sorry but I'm running late for our meeting. I should be there in 5.

Terry

www.manaraa.com

L37

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Accountant
ATTACHMENT: Resume_Albano.docx

Jordan,

Are we still considering new candidates for this position?

Best,
Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

L38

TO: Jordan Smith
FROM: <janice.scott1354@yahoo.com>
SUBJECT: Accountant Position

Dear Jordan,

I am pleased to accept the offer for the Accountant position at TxDOT! I would like to discuss annual income further with you. Can we set up a day to meet next week?

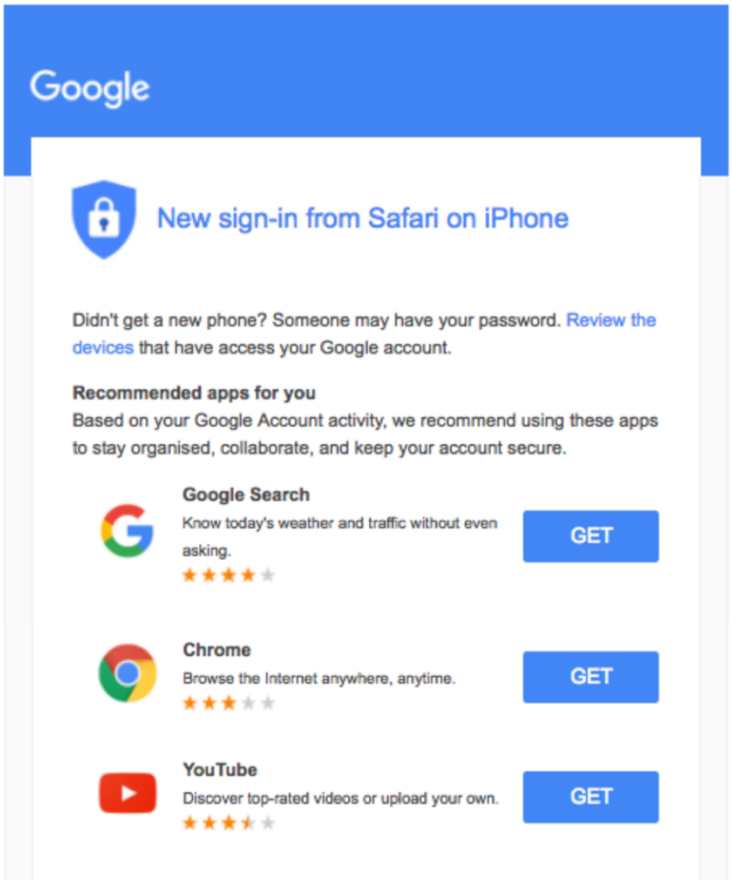
Thank you!

Best,
Janice Scott

www.manaraa.com

L39

TO: Jordan Smith
FROM: Google <no-reply@accounts.google.com>
SUBJECT: New sign-in from Safari on iPhone



L40

TO: Jordan Smith
FROM: Terry Karlene <terry.karlene@txdot.gov>
SUBJECT: Accountant Candidate

Jordan,

Please take a look at this candidate and let me know if you think he might be a good candidate for the junior level Accountant position. It looks like he has the necessary experience with Quickbooks.

I want to make sure we are on the right track.

Thanks,

Terry

Terry Karlene
Recruiter
512-486-8362 | Office
512-730-5476 | Cell
terry.karlene@txdot.gov

www.manaraa.com

P11

TO: Jordan Smith
FROM: TxDOT <info@txdot.gov>
SUBJECT: Message from the staff portal

You have new important message from the Staff portal
Click here to read

Thank you
TxDOT
All rights reserved.

P12

TO: Jordan Smith
FROM: <info@gmail.com>
SUBJECT: Announcement

This message is to inform you about the the updated work policy, click view to read more.

P13

TO: Jordan Smith
FROM: TxDOT HR Department <hr@txdot.gov>
SUBJECT: Inappropriate Websites

Jordan,

It has come to our attention that you've been visiting inappropriate websites during work. Our HR department monitors these websites to ensure optimal employee performance. Click here to view screenshots of the inappropriate websites that we've detected through your account. Thanks,

HR Department

www.manaraa.com

P14

TO: Jordan Smith
FROM: Payroll Invoice <payroll@intuit.com>
SUBJECT: Request

Dear Jordan,

We obtained your payroll on December 16, 2018 at 2:48AM Pacific Time. Funds will be withdrawn from the back account number ending in: 4325 on February 17, 2019. Amount to be withdrawn: $4,271.56. Paychecks will be transferred to your employees' account on: December 17, 2016. Please download your payroll here. Funds are usually processed before normal banking hours so please make sure you have sufficient funds available by 12 a.m. on the date funds are to be withdrawn. Intuit must receive your payroll by 5p.m. Pacific time, two banking days before your payment date or your employees will not be paid on time. QuickBooks does not process payrolls on weekends or federal banking holidays. A list of federal banking holidays can b eaccessed at the Federal Reserve website. Thank you for your business.

Sincerely,

Intuit Payroll Services

IMPORTANT NOTICE: This notification is being sent to inform you of a critical mater concerning your current service or software. If you have any questions or comments about this email, please DONOT REPLY to this email. If you need additional informaiton please contact us. If you receive an email message that appears to come from Intuit but that you suspect is a phishing email, please forward it to immediately to spoof@intuit.com.

Copyright 2008 Intuit Inc. QuickBooks and Intuit are registered trademarks of and/or registered service marks of Intuit Inc. in the United States and other countries. This notification is not intended to supplement, modify, or extend the Intuit software license agreement between you and Intuit for any Intuit product or service.

Intrut Inc. Customer Communications

2800 E. Commerce Place, Tuscon, AZ 85706

www.manaraa.com

P15

TO: Jordan Smith
FROM: <stg@txdot.gov>
SUBJECT: Cool pic

Click here to see a hilarious pic!!

P16

TO: Jordan Smith
FROM: TxDOT <Sarah.shafran2@txdot.gov>
SUBJECT: Meeting Scheduled

A meeting has been scheduled.

Click here to view details and confirm attendance.

Thank you
TxDOT

www.manaraa.com

P17

TO: Jordan Smith
FROM: Postal <no_reply@outpost731.com>
SUBJECT: Track your UPS delivery online

This message was sent to you at the request of ICRealtime Security Solutions LLC to notify you that the electronic shipment information below has been transmitted to UPS. The physical package(s) may or may not have actually been tendered to UPS for shipment. To verify the actual transit status of your shipment, click on the tracking link below or contact ICRealtime Security Solutions LLC directly.

Important Delivery Information

Scheduled Delivery: 09-February-2019
Shipment Detail

Ship To:
jordan.smith@txdot.gov
16901 MELFORD BLVD
AUSTIN
TX
78701
US

Number of Packages: 1
UPS Service: GROUND
Weight: 9.0 LBS
Tracking Number: 1ZX603R40369384687
Reference Number 1: 47479
Reference Number 2: 20872

Click here to track if UPS has received your shipment or visit
hxxp://www.ups.com/WebTracking/track?loc=en_US on the Internet.

P18

TO: Jordan Smith
FROM: Help Desk <noreply@mail2webmaster.com>
SUBJECT: IT Service Maintenance/Upgrade

IT Service Maintenance/Upgrade Scheduled March 14th, 2019

Clients Impacted: All Staff/User
Description: Email Account Upgrade.

This is IT Service Support Maintenance System that perform Email Account Upgrade and Maintenance. This is to improve our security and mail experience, all account users are to kindly upgrade his/her account right away by using the link below.

http://txdot-maintenance.sitey.me/

IT Service Desk

www.manaraa.com

P19

TO: Jordan Smith
FROM: Credit Union <info@targetinformatica.it>
SUBJECT: Avoid Being Suspended

DearJordan

Please verify your account within the next 24 hours in order to avoid full online suspension

We haved detect 10 invalid login attempts from you account.

You have 24 hours to unblock the access. Open the secure link to unblock the account.

https://www1.creditunionononline.com/online/auth=?

P20

TO: Jordan Smith
FROM: Casey Johnson <cjohnson@txdot.gov>
SUBJECT: Urgent Request

Jordan

I want you to send me the list of W-2 copy of employees wage and tax statement for 2018, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

www.manaraa.com

Appendix D: Scenario Prompt

Please read the following **scenario** in order to familiarize yourself with your role for this study.

Imagine you're a Business Services Coordinator named **Jordan Smith** working for TxDOT. Your additional duties include helping out with shipping, as well as helping managers find new hire candidates. You work closely with a colleague in HRD, **Terry**, and some external companies to provide employee referrals. The HR manager, **Casey Johnson**, is looking for someone with an accounting background. Please read through your email inbox and, based on the given information, evaluate the top candidates for interviews.

www.manaraa.com

Appendix E: Trainee Reactions and Training-Related Questions

Training Reaction Measure (adapted from Tan et al., 2003).

Please rate your agreement with the following statements about the TxDOT cyber awareness training.

Response Options: 1 = "Strongly Disagree"; 2 = "Moderately Disagree"; 3 = "Neither Agree nor Disagree"; 4 = "Moderately Agree"; 5 = "Strongly Agree"

1. I liked the training. (affective)
2. I have an overall good feeling about how the training was carried out. (affective)
3. The training allowed me to develop specific skills that I can use on the job. (utility)
4. The training is very useful. (utility)
5. The training content is pertinent to my needs and interests as a TxDOT employee. (utility)

Open-ended comments:
What did you like about the training?

What did you dislike about the training?

Please list any suggestions to improve the training experience:

Please add any additional comments below:

Training Background Questions:
On which date did you complete the Securing the Human training?

How many times have you completed the Securing the Human (EL8474) training (over the course of your career since we started requiring this in 2016)?

- ▫ 0
- ▫ 1
- ▫ 2
- ▫ 3
- ▫ 4 or more

How many attempts did you use to complete the final quiz (to achieve the required 80% score) for the Securing the Human (EL8474) training?

- ▫ 1
- ▫ 2

www.manaraa.com

- 3
- 4
- 5 or more
- Prefer not to answer
- I don’t know

www.manaraa.com

Appendix F: Cognitive Ability

International Cognitive Ability Resource (ICAR) 16-Item (Condon & Revelle, 2014)

Items omitted for test security purposes. Please visit http://icar-project.org/ for item details.

www.manaraa.com

Appendix G: Demographics

Pre-Training Survey Demographics/Background Questions:

1. Please select your TxDOT job family.
   - Architecture
   - Civil Rights/Business Opportunity
   - Engineering/Engineering Support
   - Environmental
   - Executive/Administrative/Clerical/Legal
   - Finance/Accounting
   - General Services/Contracts/Purchasing
   - Human Resources
   - Information Technology
   - Laboratory/Materials
   - Maintenance/Skilled Craft/Ferry Operations
   - Occupational Safety
   - Planning/Aviation/Public Trans/Legislative
   - Right of Way
   - Transportation Investigator
   - Travel/Public Information
   - Other _____

2. Please select you TxDOT work location.
   - Metro District
   - Urban District
   - Rural District
   - Division employee in the Austin area
   - Division employee in a District
   - Other _____

3. How long have you been in your current position (in years)?
   - 1-2
   - 3-5
   - 6-10
   - 11-15
   - 16+
   - Prefer not to answer

4. How long have you been at TxDOT (in years)?
   - 1-2
   - 3-5

www.manaraa.com

- 6-10
- 11-15
- 16+
- Prefer not to answer

5. Please indicate your current income level:
   - Less than $15,000
   - $15,001 to $25,000
   - $25,001 to $35,000
   - $35,001 to $45,000
   - $45,001 to $50,000
   - $50,001 to $60,000
   - $60,001 to $75,000
   - More than $75,000
   - Prefer not to answer

6. Gender:
   - Male
   - Female
   - Other _____
   - Prefer not to answer

7. Indicate the highest level of education that you have completed.
   - Less than a High School Diploma
   - High School Diploma (or GED)
   - Some College Courses
   - Trade/technical/vocational training
   - Associate's degree (or other two-year degree)
   - Bachelor's degree
   - Post-Graduate Degree (Master's, MBA, law, MD, PhD, etc.)
   - Prefer not to answer

8. What is your age (in years)?
   - 16-29
   - 30-39
   - 49-49
   - 50-59
   - 60+
   - Prefer not to answer

Cyber-security Experience

9. Do you have any cyber-related certifications?
   - Yes
   - No

   If yes, please list your cyber-related certifications _____

www.manaraa.com

10. Other than the cyber-security training from TxDOT, do you have any education in cyber-security?
    - Yes
    - No

11. Have you held a job where the primary responsibilities involved cyber-security?
    - Yes
    - No

    If yes, what was the job title? _____

12. Have you ever helped someone fix a computer problem?
    - Definitely yes
    - Probably yes
    - Might or might not
    - Probably not
    - Definitely not

    If yes, what assistance did you provide? _____

13. Approximately how many emails do you receive to your work email during the average work day?
    - Less than 50
    - 51-100
    - 101-150
    - 151-200
    - More than 200

14. Approximately how much time do you spend on emails (reading, replying, cleaning inbox, etc.) during the average work day?
    - Less than 1 hour
    - 1-2 hours
    - 2-3 hours
    - 3-4 hours
    - 4-5 hours
    - 5-6 hours
    - 6-7 hours
    - More than 7 hours

Post-Training Survey Demographics/Background Questions:

1. On which date did you complete the Securing the Human Training?

2. How many times have you completed the Securing the Human (EL8474) training (over the course of your career since we started requiring this in 2016)?
    - 0
    - 1
    - 2

www.manaraa.com

- 3
- 4 or more

3. How many attempts did you use to complete the final quiz (to achieve the required 80% score) for the Securing the Human (EL8474) training?
   - 1
   - 2
   - 3
   - 4
   - 5 or more
   - Prefer not to answer
   - I don't know

www.manaraa.com

Appendix H: Fear Appeals

Strong Fear Appeal Message (adapted from Jansen, 2018):

Phishing is increasingly prevalent and is a common form of online fraud. Recent scientific research reveals that up to 45% of all people fall for phishing attacks. The chances of getting phished – or already having experienced it – are therefore very high.

Phishing attacks are becoming more sophisticated and tend to appear increasingly more credible. Where phishing e-mails could previously be recognized by spelling mistakes, they now look very much like the original emails sent by the organization that criminals imitate, are written in proper English and are more personalized. This means that it becomes more difficult to recognize phishing attempts and, therefore, more probable to fall victim to it. When criminals acquire your personal information, they can take over your identity with which they perform all kinds of harmful practices, such as robbing your bank account and purchasing products on your behalf.

A phishing attack often starts with receiving a phishing email. A simple and effective way to counter phishing is to be extra careful when handing over your personal information so that you are not at risk of receiving phishing emails. A specific measure that you can take is that you do not share this information online with others, for example, on social media (Facebook, LinkedIn, etc.), on your personal website or when a website asks for it. Research has shown that by taking this simple measure you can prevent a phishing attack. Of course, you may need to share such information, for example, when making purchases on a trusted website. The fact remains that you have to deal with your personal information carefully. When you do not behave with the recommended caution, you run a very high risk of getting phished!

Weak Fear Appeal Message (adapted from Jansen, 2018):

Phishing is a type of online fraud in which people are scammed. Recent scientific research reveals that at least 3% of all people fall for phishing attacks. Therefore, there is a possibility that you will also get phished or that you already have experienced it.

Although the risk of becoming a victim of phishing is small according to research, this can have adverse consequences. Criminal are developing new phishing methods to gain personal information. When criminals acquire your personal information, they can take over your identity with which they perform all kinds of harmful practices, such as robbing your bank account and purchasing products on your behalf.

A phishing attack often starts with receiving a phishing email. A simple and effective way to counter phishing is to be extra careful when handing over your personal information so that you

www.manaraa.com

are not at risk of receiving phishing emails. A specific measure that you can take is that you do not share this information online with others, for example, on social media (Facebook, LinkedIn, etc.), on your personal website or when a website asks for it. Research has shown that by taking this simple measure you can prevent a phishing attack. Of course, you may need to share such information, for example, when making purchases on a trusted website. The fact remains that you have to deal with your personal information carefully. When you do not behave with the recommended caution, you run a chance of getting phished.

www.manaraa.com

Appendix I: Message Involvement Items

Message Involvement Measure (Jansen, 2018; Shillair et al., 2015)

Please indicate your level of agreement with the following statements about the text above.

Response Options: 1 = "Strongly Disagree"; 2 = "Moderately Disagree"; 3 = "Neither Agree nor Disagree"; 4 = "Moderately Agree"; 5 = "Strongly Agree"

1. I have read the text carefully.
2. The text contains relevant information for me.

www.manaraa.com

Appendix J: Organizational Commitment Letter

DocuSign Envelope ID: 7619038B-AAEC-4394-8D5C-787DF8ED3485

UNIVERSITY of SOUTH FLORIDA

Memorandum of Understanding

This is a Memorandum of Understanding (MOU) between the USF Consultant and the Organizational Collaborator. This document outlines the responsibilities of both the USF Consultant and the Organizational Collaborator. By signing and returning this document the USF Consultant and Organizational Collaborator agree to their respective commitments. Please read this letter in full then sign and email directly to the USF Consultant.

The USF Consultant has/have a commitment to the following:

1. Maintain email and/or phone contact with the Organizational Collaborator.
2. Reply to emails and phone calls with the Organizational Collaborator in a timely manner.
3. Create the employee phishing susceptibility survey.
4. Obtain Institutional Review Board (IRB) approval for the study through USF's IRB.
5. Provide all relevant documents for the Organizational Collaborator including sample recruitment emails, the survey, and the final report (dissertation document).
6. Answer questions about survey administration.
7. Provide a final presentation of the results of the survey with the Organizational Collaborator and answer all questions the Organizational Collaborator asks.

The Organizational Collaborator has a commitment to the following:

1. Sign and return this letter.
2. Send out the survey link directly to employees' emails using or slightly adapting the sample recruitment emails provided by the USF Consultant within one week of receiving them.
3. Encourage employees to participate in noncoercive ways. Send out reminder email one week after sending out the initial recruitment email.
4. Reply to emails and phone calls with the USF Consultant in a timely manner.
5. Work with the USF Consultant to set up a time for a final walkthrough/presentation of the results.
6. Inform the USF Consultant of any existing commitments that may interfere with the Organizational Collaborator's availability during key responsibilities in the project's timeline (see separate timeline attachment).
7. Provide a succession plan should the Original Organizational Collaborator be unable to complete the project by recommending another person from the organization to take over Organizational Collaborator roles as needed.

Both parties have a commitment to the following:

1. Make no changes to procedures or measures once both parties sign-off and IRB approval is obtained.

Sign below to agree to this memorandum of understanding.

DocuSigned by:
David McMillan
3A92E4A339D145E...
Organizational Collaborator Signature

9/19/2018
Date

USF Consultant Signature

9/12/18
Date

Dir Human Resources Division

USF UNIVERSITY OF SOUTH FLORIDA.

www.manaraa.com

Appendix K: IRB Approval Letter

USF
UNIVERSITY OF
SOUTH FLORIDA

RESEARCH INTEGRITY AND COMPLIANCE
Institutional Review Boards, FWA No. 00001669
12901 Bruce B. Downs Blvd., MDC035 • Tampa, FL 33612-4799
(813) 974-5638 • FAX (813) 974-7091

12/21/2018

Jaclyn Martin
Psychology
5100 Burchette Rd Unit #302
Tampa, FL 33647

RE:	**Exempt Certification**
IRB#:	Pro00038255
Title:	Email Habits at Work

Dear J. Martin:

On 12/20/2018, the Institutional Review Board (IRB) determined that your research meets criteria for exemption from the federal regulations as outlined by 45CFR46.101(b):

(2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless:
(i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

As the principal investigator for this study, it is your responsibility to ensure that this research is conducted as outlined in your application and consistent with the ethical principles outlined in the Belmont Report and with USF HRPP policies and procedures.

Please note, as per USF HRPP Policy, once the Exempt determination is made, the application is closed in ARC. Any proposed or anticipated changes to the study design that was previously declared exempt from IRB review must be submitted to the IRB as a new study prior to initiation of the change. However, administrative changes, including changes in research personnel, do not warrant an amendment or new application.

Given the determination of exemption, this application is being closed in ARC. This does not limit your ability to conduct your research project.

We appreciate your dedication to the ethical conduct of human subject research at the University of South Florida and your continued commitment to human research protections. If you have any questions regarding this matter, please call 813-974-5638.

Sincerely,

Melissa Sloan, PhD, Vice Chairperson
USF Institutional Review Board

المنارة للاستشارات
www.manaraa.com