AN ASSESSMENT OF USER RESPONSE TO PHISHING ATTACKS: THE EFFECTS OF FEAR AND SELF-CONFIDENCE

by

DEANNA HOUSE

Presented to the Faculty of the Graduate School of
The University of Texas at Arlington in Partial Fulfillment
of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON
August 2013

Acknowledgements

I would first and foremost like to thank my family for all of their help and support during my journey towards a PhD. Thank you to my husband, Mark. You are my best friend and greatest cheerleader. Your patronage, support, and encouragement kept me going. To my parents, Dr. Marvin and Judy Alff for their love, support, and inspiration. To my mother-in-law Nancy and late father-in-law Mark House for being supportive of my dreams and helping me achieve them. I hope that my children, Eliot and Emerson, have an ingrained appreciation of the value of education and the payoff of hard work and determination. To my brothers, brother-in-law, sisters-in-law, and niece and nephews, thank you for the love and encouragement.

Dr. Raja, my dissertation chair, has been an integral part of my success as a PhD candidate and always gave me the determination to keep going even when things seemed bleak. Dr. Wright provided me with guidance and support for my experiment and had insights that an outside committee member should. Dr. Wang gave me feedback to improve my research and gave me perspective on the research area. Dr. Slinkman gave me support with my methodology and helped me answer tough questions to keep me moving forward. Dr. Teng guided me through me the coursework portion of my dissertation and was always there to help. Thank you to Karen Scott, Dr. Davis, O'la Al-Laymoun, Ramakrishna Dantu, Ola Awe, Nisha Kulangara, Christie Chen, and Kim Whitehead for allowing me into your classrooms. To Rajat Mishra for being a great friend going through this process. Thank you to my classmates for everything. Evelyn and Nancy were always there to provide support and encouragement . And to the rest of the faculty in the Information Systems and Operations Management department for helping guide me through the program.

In addition, thank you Dr. Shannon Scielzo for assistance with the framework for my experiment and to Robin Dickey for assistance with IRB approval. And last but not least to Adrian Gawel for the idea for a paper that turned into a dissertation and to Dr. Ania Gawel for being a wonderful friend.

I am thrilled to be finished and am ready to face the world of academia.

August 7, 2013

Abstract

AN ASSESSMENT OF USER RESPONSE TO

PHISHING ATTACKS: THE EFFECTS

OF FEAR AND SELF-CONFIDENCE

Deanna House, PhD

The University of Texas at Arlington, 2013

Supervising Professor: MK Raja

Phishing attacks have threatened the security of both home users and organizations in recent years. Individuals of varying levels of computer proficiency are potential targets for a phishing attack; all that is needed is an email address and Internet access. Phishing uses social engineering to fraudulently obtain information that is confidential or sensitive. Individuals are targeted to take action by clicking on a link or providing information. At present, phishing research is lacking in both theory and actual behavioral data. This research aims to fill that gap by introducing a new model and collecting data from multiple sources (including an attempted phishing attack). The research draws upon existing theory and research in healthcare, criminology, psychology, and information systems and security. The survey results indicated that when individuals had a high level of fear arousal related to providing login credentials they had a *decreased* intention to respond to a phishing attack. Self-confidence did not significantly moderate the relationship between fear arousal related to providing login credentials and intention to respond to a phishing attack but it did have a significant direct positive influence on intention. The results from the experiment indicated that 18% of individuals overall clicked on the link. Level of training did make a difference in the

number of clicks (although not significant). More subjects clicked on the link when only basic training was received versus those that received expert level training. The combined data corroborated with the survey data to indicate that level of fear related to providing login credentials resulted in a decreased intention to respond to a phishing attack and a decreased actual click behavior. This research provides valuable information about similarities between self-reported data and actual behavior. The research explores how fear of providing login credentials influences both intention to respond and actual response to a phishing attack. When fear arousal related to providing login credentials is high, individuals are less likely to respond. This is interesting because there is an underlying concept of suspicion. When an individual is fearful of providing login credentials they may be suspicious of an email being fraudulent, thus making them less likely to respond. The experiment has provided an excellent foundation to build upon for future fear appeal experimental research to explore both the importance of the targeted website (i.e. bank information versus online shopping versus online wall street journal) and the fear appeal verbiage.

Table of Contents

List of Illustrations

List of Tables

Chapter 1

Introduction

1.1 Problem Statement

The Internet has evolved from an unfettered world of possibilities to a potentially perilous space with hazards such as identity theft, viruses, malware, and fraud. New threats are propagated in such a rapid manner that it can be difficult for individuals to stay abreast of the latest risks. One such threat, phishing is becoming a very damaging problem. Just the click of an email link can install malware software that can provide access to account numbers, databases, and login information (Anderson, 2013). Phishing attacks have increased in recent years (Vishwanath et al, 2011) yet there is still very little known about why individuals fall victim to phishing attacks. Much of the research related to phishing is lacking a strong theoretical foundation. There is currently a gap in the literature related to the influence that self-confidence and fear arousal have in response to a phishing attack. Specifically, does the level of training have an effect on an individual's response to a phishing attack and does the level of fear related to providing login credentials when a phishing email is received have an effect. Additionally, do fear of providing login credentials and self-confidence affect an individual's intention to respond to a phishing attack. Both survey and actual behavioral data are collected in an effort to determine if there is any disparity between self-reported data and individual response to an attack and to explore the reasons behind why an individual clicks on a link. Although as stated by Thaler & Sunstein (2008) when individuals have their intentions measured, they are more likely to act similarly to what they answer.

As the world becomes more Internet-savvy, those users must cast a wary eye on communications and interactions with websites. With over two billion Internet users in the world (Internet World Stats, March 2011), there is no shortage of potential victims to

gain identifying information from. Phishing has been described as a type of social engineering with the goal of gaining confidential or sensitive information through the guise of a trusted source (Myers, 2007). Social engineering is described by Easttom & Taylor (2011) as an "old-fashioned conning" (pg. 63) with considerable effort in place to gather relevant information (such as personal details or real information) to have a successful attack. The social engineer is very adept at manipulating victims by using persuasion and deception (Ramamoorti, 2008). Many times, the victim believes that the source of the communication is legitimate. This research, however, is focused on what individuals do when faced with an attack where there is a suspicion regarding the authenticity of an email. As is the case with any scam, those responsible for the phishing attacks use all of the basic human needs and desires to manipulate victims including fear and anxiety (Piper, 2007; Chiluwa, 2009).

Phishing attacks initiate with communications sent to millions of contacts either by email, text message, social media, or via the Internet. The magnitude of messages sent is one of the reasons that phishing scams are successful (Bocij, 2006). It is cheap, fast, and easy to send millions of emails in hopes of getting a response back from a handful of individuals. As argued by Blommaert & Omoniyi (2006), Internet fraud works and although communications may not be perfectly written, the globalized nature of them will still reach a large audience. "The Internet gives the criminal enterprise global reach and the whole world to hide in" (Hallam-Baker, 2008, pg.2). It is very difficult to track down criminals. This is in part due to the fact that they are very adept at masking their activities through the use of botnets. Botnets consist of several computers under control of malware that can be used for fraudulent activities (Gu et al, 2008).

The goal of any phishing communication is to receive a response. The messages are designed with the hopes of gaining the attention of a select few potential

victims (Wright & Marett, 2010). These communications have the purpose of gathering sensitive information (such as login information or account numbers). The messages mimic those of legitimate businesses (James, 2005; Sarel & Marmorstein, 2006) and can be very deceptive, leaving fakes virtually undetectable by the user (Dhamija et all, 2006). There will frequently be some sort of "bait" indicating to the recipient that an action must be taken or something bad will occur such as account shut down. Messages are perceived as coming from a legitimate source; which in turn makes them more persuasive (Sagarin et al, 2002). Victims, influenced by a simple request, unknowingly provide sensitive information to a phishing site that is set up to look like a legitimate company.

Once victims provide the requested information (and believe they are doing so to a legitimate organization) the phishing attack is considered successful (Dong et al, 2010). A user name and password is all that's needed to be that user; with all the rights and privileges (Soloman & Chapple, 2005). When the communication is via email, a url will be conveniently provided that either links to a fraudulent website that is a copy or "spoof" of a legitimate site or installs malware on a user's system that can gain access via keylogging. The attackers give the victims a sense of security by providing a thank you response message and sometimes even linking back to the legitimate website. The ambiguity of the Internet provides the perfect conditions for the transfer of funds into the wrong hands (Anderson, 2013).

The scam artists frequently use the information for identity theft (Butler, 2007; Hodgson, 2005; Monahan, 2009; Copes & Vieraitis, 2009). This includes fraudulent activities such as gaining access to bank accounts in order to steal funds. This is frequently done without the victim's knowledge and can be detrimental to his/her financial well-being. New scams continue to be developed (Piper, 2007; Png & Wang, 2009) and

gain in sophistication (Jakobsson, 2005; Downs et al, 2007; Dong et al, 2010). Research related to phishing must keep up with current trends so that as phishing trends change so can education and training.

According to Kumaraguru et al (2010) there are three important strategies typically used to protect individuals from falling victim to phishing emails. First, email providers and Internet service providers work behind the scenes by automatically detecting emails and flagging them as such. Second, the use of training arms users with knowledge to prevent attacks. Lastly, the use of tools such as browser warnings, toolbars, and extensions can help prevent users from being phished. Even with these strategies in place, individuals still provide sensitive information.

While prevention is essential, it is equally as important to find out why individuals ignore cues frequently identified as typical phishing attempts such as misspellings (Butler, 2007), illegitimate URLs (Butler, 2007; Kumaraguru et al, 2010), and requests for personal information (Butler, 2007; Kumaraguru,et al, 2010). There are many unknown factors related to how and why a victim responds to an attempted phishing attempt. Victims may be acutely aware of existing scams yet still make the choice to give out information and therefore fall victim to a scam (Deem, 2000). It is imperative that researchers find out as much information as possible regarding the factors that contribute to a person falling victim to a phishing attack and also resisting such attacks. Looking behind the scenes at the underlying emotions that are involved in decision-making can help researchers gain valuable insight regarding the response to phishing attacks. This will allow for the development of customized user training and assist in the prevention of individuals falling victim.

1.2 Importance of the Study

Loss of funds due to identity theft is a big problem. Estimated consumer losses are upwards of $1.5 billion according to the FTC's annual Consumer Sentinel Network Data Book for 2011 (FTC, 2011). This amount is possibly deflated considering only 68% of the victims reported an amount paid related to the theft. Many banks do not hold customers responsible for amounts greater than $50; which gives them a decreased risk of loss of funds (Lipka, 2012). However, it is still an inconvenience to both consumers and organizations. And in the case of checking accounts, consumers may be left waiting for the return of funds pending an investigation. The risk of providing sensitive information to a fraudulent source is something that all Internet users must face. Numerous Internet users lack the knowledge about information security that is needed to protect their private and identifying information (Kritzinger & von Solms, 2010). This research helps further explore threatening communications and training and how the fear of providing login credentials and/or self-confidence can alter the outcome of a phishing attack.

There is currently a deficit in behavioral research related to phishing. This research uses an experiment to collect actual behavioral data on the influence that level of fear and training level have on an individual's decision to click on a link. Education is key to prevent individuals from falling victim to social engineering attacks (Easttom & Taylor, 2011). The research will provide both the home user and organizations with valuable insight regarding the cognitive and emotional response that is invoked when a person is faced with a phishing attack. The risk of divulging sensitive information is high

and it is pertinent that research be conducted to determine the outcomes associated with phishing attacks. The training video provides valuable information related to phishing and gives the researcher the opportunity to explore the influence that training has on response to an attempted phishing attack. Fear, particularly the type that is brought forth from an external motivation, is also an important factor to study during an experiment. Namely, what effect does the level of fear (and more specifically fear of providing login credentials) have on a subject's response to a phishing attack? The literature review is presented in the next section followed by the research model/framework and research methodology.

Chapter 2

Literature Review

Research related to phishing brings in subject matter from multiple disciplines such as criminology, psychology, fraud, information systems, and security. This research is still relatively new and frequently changes as new threats continue to emerge. Providing a strong theoretical backing to the existing phishing research will not only help this area of research mature but will also give researchers the opportunity to discover more about the perceived reaction to phishing communications. This research introduces the Threat Appeal Behavioral Response Model to determine what factors influence intention to respond to a phishing communication. The Threat Appeal Behavioral Response Model has theoretical underpinnings in The Protection Motivation Theory (1975, 1983) and the Extended Parallel Processing Model (Witte, 1992). A review of research related to fear appeals and how they tie-in to phishing is presented in the next section.

2.1 Fear Appeals Theories

Fear appeals have been studied in psychology research since the early 1950's (Witte & Allen, 2000). Fear appeals are messages with persuasive properties that arouse fear in an individual (Witte, 1994). The focus of a fear appeal is to suggest a course of actions that can prevent a noxious consequence from occurring (Rogers, 1975). A variety of research has been conducted in relation to fear appeals and their persuasive properties (Rogers, 1975; Witte, 1994; Champion et al, 2004; Johnston & Warkentin, 2010; . There are three main groups that fear appeal theories can be separated into:

drive theories, parallel response models, and subjective expected utility (SEU) models (Dillard, 1994) such as Protection Motivation Theory (Witte & Allen, 2000).

Fear-as-acquired-drive model was introduced by Hovland et al, (1953) and later extended by Janis (1967). These models suggested that the response to a fear appeal (as implemented by the level of fear arousal) caused a drive to motivate actions and thus a low to moderate level of fear arousal would produce the largest attitude change (Witte & Allen, 2000). Persuasion was introduced to have an inverted u-shaped relationship to fear aroused (Janis, 1967). Both the u-shaped relationship and the fear-as-acquired drive model were rejected. The u-shaped relationship was not supported in research (Rogers, 1975; Rogers, 1983; Beck & Frankel, 1981; Leventhal, 1970). The fear-as-acquired-drive model was rejected due to a lack of predicted interaction among variables such as efficacy and specificity of recommendations (Rogers, 1983; Beck & Frankel, 1981; Leventhal, 1970). In addition, the direct relationship between drive and changes in attitude were never empirically supported (Rogers, 1983).

The next generation of fear appeal theories focused on parallel response. Leventhal (1970) came up with the parallel response model which included two independent processes. These are fear control processes and danger control processes. Fear control processes are defined as “primarily emotional processes where people respond to and cope with their fear” (Witte, 1992; p.341). Danger control processes are responses to the threat and the efforts to control it (Witte & Allen, 2000). This model has been refuted due to lack of a clear definition as to what evokes the fear control process or the danger control process (Rogers, 1975; Beck & Frankel, 1981; Witte, 1992).

Rogers (1975) attempted to address issues associated with the parallel response model by putting forth the Protection Motivation Theory. The premise of Protection Motivation Theory focuses on fear-arousing communications and how they influence

behavior and intentions (Boer & Seydel, 1996). According to Rogers (1983), Protection Motivation Theory posits that there are four beliefs as a motivation to the prevention of danger: "1) the threat is severe, 2) one is personally vulnerable to the threat, 3) one has the ability to perform the coping response, and 4) the coping response is effective in averting the threat" (pg. 170). Rogers' 1975 model has been backed empirically in that the original components of a fear appeal are made up of *magnitude of noxiousness*, *probability of occurrence*, and *efficacy of recommended response*. There is also evidence that a cognitive mediating process to these components exists as presented in Rogers' 1975 model (Rogers, 1983). These are: *appraised severity*, *expectancy of exposure*, and *belief in efficacy of coping response.* The model indicates that these cognitive mediating processes lead to protection motivation and the intent to adopt the recommended response. The change in attitude is a result of the protection motivation brought forth from the mediating processes mentioned previously (Rogers, 1975).

Rogers extended his 1975 model in 1983 to address the refuted lack of multiplicative properties of his original model and also further address the coping process and extend the cognitive mediating processes (Rogers, 1983). This model accounts for both maladaptive and adaptive responses that result in either a threat appraisal or a coping appraisal. Threat appraisal begins with a situation in which an individual receives an intrinsic or extrinsic reward which is reduced by the severity or vulnerability of the maladaptive response. The coping appraisal accounts for an individual's "ability to cope with and avert the threatened danger" (Rogers, 1983, pg. 169). The coping appraisal is a result of the response efficacy and self-efficacy that is reduced by the response costs of the adaptive response. Self-efficacy is an addition to both the original model and the updated model for its role in fear appeal research (Beck & Frankel, 1981, Beck & Lund, 1981; Rogers, 1983; Maddux & Rogers, 1983) and its effect on attitude change (Bandura,

1977). Rogers (1985) accounts for fear arousal in his model but does not indicate that fear has a direct relationship to outcome or appraisal.

Protection Motivation Theory research has been conducted on a variety of different topics such as adolescent driving (Simons-Morton et al., 2006); physical activity among adults (Plotnikoff et al, 2009); and specific to information technology for research related to safe security-related behavior (Anderson & Agarwal, 2010); omissive behaviors (Workman et al, 2008); and plagiarism software adoption (Lee, 2011). PMT originated in healthcare, but has recently been extended to areas such as information systems and information security (Johnston & Warkentin, 2010; Lee, 2011; Zhang & McDowell, 2009). However, PMT does not directly look at the relationship that fear related to a topic has on an individual's response.

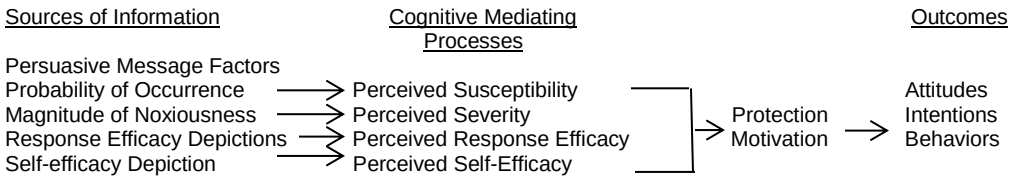


Figure 2-1 Protection Motivation Theory with Self-Efficacy (Adapted from Rogers 1975; Maddux & Rogers 1983; Witte, 1992)

Witte (1992) proposed a model that brings together both Leventhal's (1970) parallel response model and Rogers' PMT. The Extended Parallel Processing Model (EPPM) clarifies and refines Leventhal's (1970) model and resolves the discrepancies between the theory and empirical testing of the PMT. Additionally, EPPM specifically looks at both message acceptance and message rejection; which the other theories seemed to ignore (Witte, 1992). The EPPM states that message processing will result in

one of two outcomes. These are protection motivation and the acceptance of a message or a defensive motivation that is triggered by fear and leads to the rejection of a message.

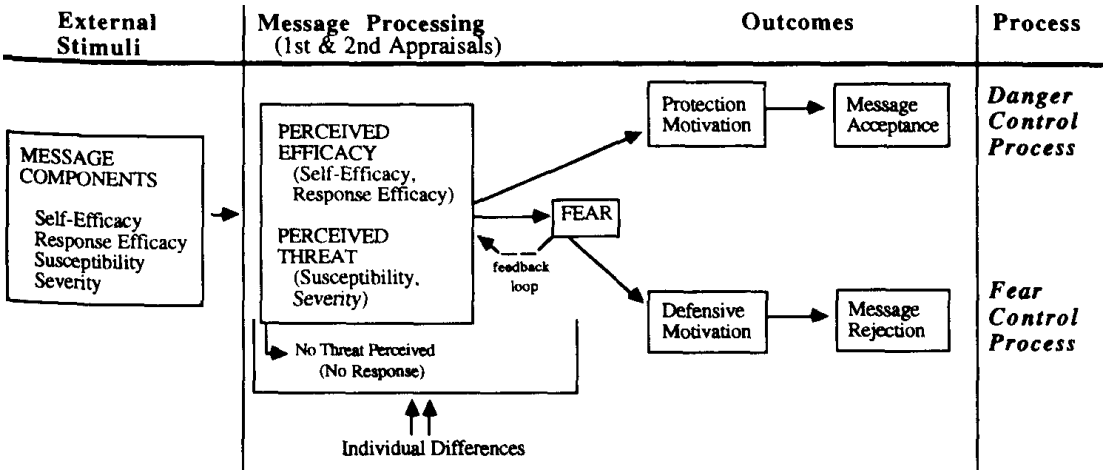


Figure 2-2 The Extended Parallel Processing Model (Witte, 1994)

If faced with a serious threat, EPPM provides the reasoning that an individual will respond to their fear and take an action to reduce it (Witte & Allen, 2000). EPPM also takes into account the variables perceived efficacy (which is a combination of self-efficacy and response efficacy) and perceived threat (which includes susceptibility and severity). According to Witte & Allen (2000), “perceived efficacy determines whether people will become motivated to control the danger of the threat or control their fear about the threat” (pg. 594). EPPM has been used to explain the reactions that individuals have to a health threat and whether or not they follow the recommended response.

2.2 Fear Appeals Related to Phishing

Using fear to scam individuals have been documented as early as the 1800s. Early examples involve “medicines” made from various inert ingredients that were toted to cure ailments (Nash, 1976). Reaction to fear can create a sense of urgency to take immediate action. Research has been conducted related to other areas of security and taking protective action (such as installing anti-virus software). When faced with a security threat, users will take some sort of action to protect themselves (Liang & Xue, 2009). The more severe the threat, the more likely the individual will take the recommended action (Das et al, 2003). Protection motivation theory can help us figure out how attitudes and behaviors change when threats are evident (Floyd et al, 2000). Additionally, EPPM accounts for message appraisal related to threat and the motivation for processing the message (Witte & Allen, 2000). In the case of phishing, the user is protecting him/herself by not providing sensitive information or being less likely to respond to a phishing email. Performing an action such as not clicking on links from emails and not providing sensitive information are protective measure that individuals can employ to prevent falling victim to phishing attacks.

Fear communications work best when there is an accompanying suggestion of how to cope with the threat (LaRose et al, 2008). This means that communications that give recipients an option to alleviate the threat (such as providing account information to prevent an account from being shutdown) will be more effective. Alleviating the threat for an attempted phishing attack is slightly different, however. The message recipient is under the false impression that he/she is alleviating the threat when in fact he/she is taking an action that is actually harmful. If the individual provides a user name and password he/she will become a victim to a phishing attack. However, communications that threaten the shutdown or lockout of an account are difficult for users to detect as

fraudulent (Davinson & Sillence, 2010). Therefore, the user is frequently unaware that they are providing sensitive information to a fraudulent source. When this is the case, those that are behind the phishing attacks have more time to wreak havoc on the victims' lives. While this information provides details of why the attacks may work, this research is exploring the effect that fear of providing login credentials has on motivating an individual to respond. Individuals may be fearful of providing login credentials when they have suspicion that the email is fraudulent. If the individual is unaware that the email is fraudulent, he/she will not be fearful of providing login credentials to a legitimate cite.

Giving the victims the tools and knowledge to not fall victim to an attack is necessary to reduce the number of individuals that give out sensitive information. Once a victim is successfully phished, the likelihood of the culprit being prosecuted is low. Crimes related to phishing are difficult to investigate for numerous reasons such as delays in crime reporting; off-shore servers; and short-lived phishing sites (Easttom & Taylor, 2011). Victims will frequently neglect to report the crime to police; particularly if the financial loss is negligible (White & Fisher; 2008). User responses tend to be high during the initial onset of the mass emailing (Moore & Clayton, 2007; Wright & Marett, 2010; Kanich et al, 2008; Kanich et al, 2009). In fact, while phishing sites are frequently taken down in a hasty manner, Moore & Clayton (2007) found that if a site is removed one day after it is reported, it may have numerous potential victims prior to its removal. Other factors such as strongly worded communications and high email load can all increase the possibility of falling victim to a phishing attack (Vishwanath et al, 2011).

2.3 Efficacy

Efficacy focuses on the impediment or aversion of a response as related to ease, feasibility, and effectiveness (Witte, 1994). Self-efficacy refers to "a person's ability to

carry out a recommended response" and response efficacy refers to "the effectiveness of the recommended response in averting the threat" (Witte, 1994, pg. 114). Research has indicated that situations involving high efficacy result in the acceptance of the recommended response (Roskos-Ewoldsen et al, 2004). With this in mind, even the experienced Internet user can fall victim to a phishing scam with a brief moment of distraction to blame (Regan, 2010).

2.4 Threat

Threats are considered "harms or losses that have not yet taken place but are anticipated" (Lazarus & Folkman, 1984, p. 32). When a threat is received, there is a coping process that takes place in order to assess what the best outcome is (Lazarus & Folkman, 1984). There is no known method for completely mitigating threats that are induced by user behaviors (Dodge, Jr. et al., 2007). Users may be aware of potential security threats but this awareness does not necessarily equate to action (Furnell et al, 2007; Workman et al, 2008). This can open up the potential for risk of falling victim to an attack. Influences such as email load may also affect a user's response with an increased response; particularly when relevant (Vishwanath et al, 2011). Users feeling time constraints may only rely on heuristic or visual indicators (such as logos or layouts) of a website in order to verify its legitimacy (Davinson & Sillence, 2010). This is not always accurate provided that logos are easily copied (Alexander, 2009). According to Blythe et al (2011), detection rates for phishing emails were higher when a logo was not included. Communications that look legitimate are not difficult to replicate. This research will provide valuable insights regarding the behavioral response to phishing attacks and also determine the effect that training has on the response.

2.5 Self-Confidence

Self-Confidence is the "belief that one can successfully execute an activity" (Feltz, 1988, pg. 423). It is a judgment about achieving one's goals (National Research Council, 1994). Self-confidence has a strong influence on individual's behavior (Bandura, 1986). Self-Confidence has a "stable influence on a person's behavior" (Zulkosky, 2009, pg. 99). There has been research related to self-confidence that indicates an individual can have self-confidence yet inaccurate (Kahneman, 2011). According to research conducted by Gigerenzer et al, 1991, self-confidence that is "immediate and spontaneous rather than a product of long-term reflection" (pg. 526) is not affected by the same accuracy issues. The former rather than the latter would apply specifically to a response to a phishing attack. When phishing attacks occur, individuals are more likely to respond in a spontaneous manner rather than after careful thought and reflection. Specific to this study, the researchers are interested in how self-confidence can change the relationship between fear arousal and intention to respond to a phishing attack. Subjects with a high self-confidence will focus less on their fear and have a decreased perception of fear (Carver & Blaney, 1977). Lazarus (1999) found that individuals can address a situation as either a threat or a challenge. Self-confidence varies among individuals but those that have a high level of self-confidence are more likely to be challenged in overcoming an obstacle (Feltz, 1988; Taylor, 1987). In other words, those that have a high level of self-confidence will not respond to the attack.

2.6 Summary

The use of fear appeal research to explore the factors that influence an individual's response to phishing attacks is a relatively recent area of research. While research has been conducted in similar streams, this research attempts to unite those

areas that have been explored and bring forth new insights related to phishing and fear of providing login credentials.

Chapter 3

Research Model and Hypotheses Development

3.1 Overview

This research provides the Threat Appeal Behavioral Response Model to explore the influence that fear of providing login credentials and self-confidence have on an individual's intention to respond to a phishing communication. While the fear appeals models discussed in the previous section are applicable to the context in which they have mostly been studied (i.e. protective healthcare), they do not specifically address the behavioral response to a phishing attack. More specifically, phishing attacks have the goal of receiving a response. Individuals are able to protect themselves by not clicking on the link. Conversely, individuals that have self-confidence related to phishing attacks are predicted to respond differently. These individuals will not exhibit protective behavior and instead will not respond to the phishing attack. Individuals that have self-confidence will moderate the relationship between fear of providing login credentials and intention to respond to a phishing attack. The Threat Appeal Behavioral Response Model attempts to explain the different effects that self-confidence and fear of providing login credentials as related to becoming a victim have on intention to respond to a phishing attack. The fear of providing login credentials has operationalized to fear arousal and henceforth fear arousal will mean fear of providing login credentials.

There are numerous types of phishing attacks that are designed solely to elicit a response. Commonly, phishing communications are designed in one of two ways. The first types of communications have a goal of targeting an individual's greed. Examples of such attacks are communications that claim the recipient won the lottery, has been

selected to participate in a money-making venture, or has been bequeathed a fortune (Chiluwa, 2009). The second type of common phishing attacks are designed to manipulate victims by using communications that are threatening. The use of words that intend to invoke fear are prevalent. Phrases such as “urgent reply”, “failure to abide will result in account suspension”, and “permanent suspension” are commonly used. An example of such a communication is a recent email that was distributed stating that an email account had exceeded the storage limit of 20 GB. The sender threatened that the ability to send and receive email would be revoked once that limit was reached. A recipient of such an email might not think twice about providing log-in information so that he/she would be able to send and receive email. A password expiration reset would be another type of phishing attack that is considered high in threat and would invoke a response from recipients that is initiated by fear.

Other communications are seen as low fear and do not have urgency cues such as those mentioned above. An example of such a communication would be a recently distributed request for “mystery shopper” participation. The email asked for personal information such as: Name, Address, Occupation, Age. A payment of $200 is promised for each mystery shopping experience. Undoubtedly, if the recipient responded with an agreement to participate, the “company” would need bank information so that a “direct deposit” could be initiated. Another example uses the social networking site Facebook. The message is manipulated to look like it is from Facebook and states “Sarah has sent you a message”. The embedded link in the email take the user to a fraudulent site set up to collect the recipient’s user name and password. This research explores the latter; communications that have a fear appeal. Preying upon individual’s insecurities using threat is common (Davinson & Sillence, 2010) and the researcher hopes to gain insight regarding this type of phishing attack.

User response related to phishing attacks are inherently difficult to study. In particular, it is challenging to gather data that accurately reflects individuals' behavioral responses. The experimental and survey data collected will give researchers a full picture of what occurs when an individual is presented with a phishing attack. Specifically, the empirical data collected during the experiment will provide researchers with data related to how users respond when faced with a phishing communication. Collecting both survey and experimental data will not only give the researcher data about an individual's intention to respond to an attack but also pair that data with clicking on a link in response to a phishing attack. It is important that researchers learn as much as possible regarding the psychological and cognitive factors that are involved during an attempted phishing attack in order to prevent said attacks. The researcher is interested in determining whether or not expert-level training that specifically addresses phishing communications will affect user response. This information is vital in forming future user phishing training.

The model is shown below in Figure 3.1.

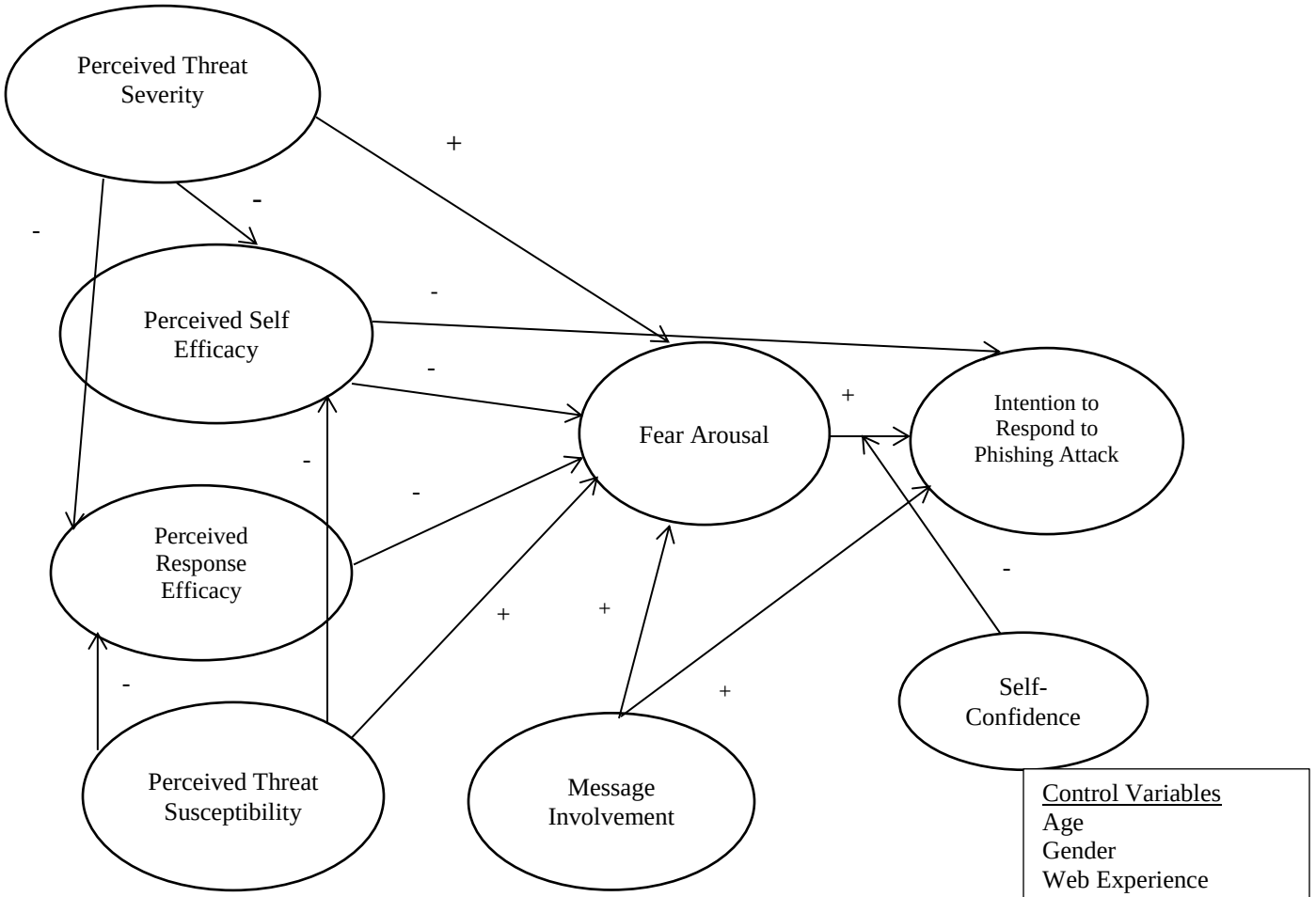


Figure 3.1: Research Model

This model incorporates both self-efficacy and response efficacy from previous research related to PMT and EPPM. Self-efficacy refers to the ability in carrying out a recommended response while response efficacy refers to on how effective the response recommended is in avoiding the threat. In this case, the threat is phishing and the recommended response is the recommended response to a phishing attack. While research has made the distinction between self-efficacy and self-confidence difficult, there is a clear difference. Self-confidence is "a consequence of behavior" and self-efficacy is something that influences outcomes (Cramer et al, 2009, pg. 326).

Self-confidence related to general-knowledge tasks has been related to an overconfidence bias such that individuals tend to be confident yet inaccurate (Koriat, 2011; Lichtensten et al, 1982; Brenner, Koehler, Leiberman, & Tversky, 1996; Griffin & Brenner, 2004; Hoffrage, 2004). Those that are highly self-confident are not concerned with being wrong, however. The human brain has an innate need to repress contradictions (Lehrer, 2009).

The next section includes the hypotheses described in greater detail.

3.2 Hypotheses

Phishing communications are designed so that users can easily click on a provided link and give out the requested sensitive information. Self-efficacy is considered "a person's ability to carry out a recommended response" (Witte, 1994, p.114). A person can have the belief that they are able to perform the action which is defined as perceived self-efficacy. Individuals that have high self-efficacy can not only approach difficult tasks with ease but are also able to make high-quality decisions (Zulkosky, 2009). In relation to a phishing communication, those that have high perceived self-efficacy will have the belief that it is possible to prevent his/her login information from being compromised. This

ability will influence the individual to not fall victim to the attempted phishing attack and result in a decreased intention to respond to the phishing communication.

H1: Perceived self-efficacy will decrease the intention to respond to a phishing communication.

Perceived threat severity is defined by Witte (1992) as “an individual’s beliefs about the seriousness of the threat” (p.332). Individuals that perceive a threat as severe will have doubts in his/her ability to prevent the threat. Perceiving a threat as severe can affect one’s belief in one’s abilities (Wood & Bandura, 1989). This is particularly evident when the level of severity is high; defined by Witte (1994) as the critical point. The critical point occurs when the threat is so high that the ability to carry out the recommended action is no longer possible (Witte, 1994). Additionally, when the level of threat is high, perceived response efficacy can be affected. In particular, individuals can feel that if something is seen as a severe threat, it is futile to try to prevent the threat because the actions will not prevent the occurrence of the threat (Witte, 1991-1992). High threat levels can trigger a reduced self-efficacy (Cauberghe et al, 2009).

Phishing communications frequently contain a fear appeal and have the goal of being perceived as threatening and severe. Having ones’ access terminated to a bank account or email account can be perceived as serious for many individuals. Similar to results found by Wurtele & Maddux (1987), it is expected that when an individual is exposed to a severe threat, he/she will react with a reduced perceived self-efficacy. When a threat is deemed “distressing”, any efficacious suggestions can be discounted and smothered (Bandura, 1977). As stated by H2a, when perceived threat severity is high, individuals will have a decreased level of self-efficacy. Response efficacy is defined

as “the effectiveness of the recommended response” (Witte, 1992, p. 332). Along these lines, perceived response efficacy is an individual’s belief that the action he or she is taking will actually avert the threat (Rogers, 1975). This brings us to H2b, that when a threat is perceived as severe the response to avert the threat (i.e. not clicking on or providing sensitive information through links from emails and verifying the address of the sender) will be deemed useless. It is predicted that perceived threat severity will reduce the effects of both perceived self-efficacy and perceived response efficacy.

H2a: Perceived threat severity will have a negative influence on perceived self-efficacy.

H2b: Perceived threat severity will have a negative influence on perceived response efficacy.

Perceived threat susceptibility is concerned with individuals’ beliefs regarding risks of experiencing a threat (Witte, 1994). The threat does not have to truly be harmful; the individual need just believe that it is (Lazarus, 1966). Individuals that believe they have a high risk of falling victim to a phishing attack will not believe that they can avert the threat by performing the recommended action. This high threat situation can result in complete avoidance of the issue at hand (Janis & Feshbach, 1953) or just a reduced ability in identifying fraudulent emails to prevent sensitive information from being compromised. When perceived threat susceptibility is high, individuals will have a reduced perceived self-efficacy.

When an individual has a high level of perceived threat susceptibility, or belief that something is likely to occur, the use of a recommended response can backfire and cause a disbelief in the recommended action’s effectiveness (Witte, 1996). As an individual’s belief of the likelihood of sensitive information being compromised as a result

of a phishing attack increases, the belief that avoiding clicking on links from emails, not providing sensitive information through links, and verifying the address of the sender will avert the threat will be reduced. Individuals that believe that they are highly susceptible to falling victim to phishing by having their logins compromised will be less likely to believe that actions such as not clicking on links from emails, not providing sensitive information through links in emails and verifying the address of the sender will prevent their login credentials from being compromised. This will result in a reduced influence on perceived response efficacy.

H3a: Perceived threat susceptibility will have a negative influence on perceived self-efficacy.

H3b: Perceived threat susceptibility will have a negative influence on perceived response efficacy.

Fear is likely when an individual feels that he/she does not have the ability to control the outcome (Rachman, 1978). Research has shown that when a person is lacking the efficacy to handle the threat, fear ensues (Lazarus & Folkman, 1984). However, individuals that have high self-efficacy and feel capable of dealing with a situation will "behave assuredly" when faced with a fearful situation (Bandura, 1977a, p. 194). In addition, those that have a high self-efficacy have a reduction in fear. (Bandura, 1977b). An individual can modify his/her behavior related to his/her abilities in the wake of fear (Marks & Tobeña, 1990). When self-efficacy is low, however, reactions to fear can be different.

Phishing communications are frequently written to elicit a response that is provoked out of fear. Fear can be brought about during the evaluation of a stressful situation (Lazarus & Folkman, 1984) such as an attempted phishing attack. However,

individuals with high self-efficacy will be better equipped to process the phishing communication and will have a decreased fear arousal based on abilities to differentiate between legitimate and illegitimate emails. When an individual has a high level of response efficacy and are aware that actions they are taking will avert the threat. This will result in a decreased fear arousal when perceived response efficacy is high.

H4: Perceived self-efficacy will have a negative influence on fear arousal.

H5: Perceived response efficacy will have a negative influence on fear arousal.

Perceived susceptibility and perceived threat cause fear and motivate action (Green & Witte, 2006). When perceived threat is elevated, fear is also elevated (Witte & Allen, 2000; Witte, 1992; Witte, 1998). Future harms are what constitute the threat (not present danger) (Lazarus, 1966) as is the case with phishing attacks. Phishing attacks are an indication of anticipation that sensitive information will be gathered and identity theft or access to funds will be gained. When harm is seen as highly threatening and perceived as occurring in the near future, the threat has the highest impact (Lazarus, 1966). Individuals can foresee a threat and have an anticipatory reaction such as if they determine a threat is severe, they will have an increased fear arousal (Bandura, 1977b). As noted by Connor & Norman (1995), when both threat susceptibility and severity are high, fear arousal will be engaged. Thus, hypotheses 6 and 7 state:

H6: Perceived threat severity will have a positive influence on fear arousal.

H7: Perceived threat susceptibility will have a positive influence on fear arousal.

Confidence is a feeling or consciousness of one's powers or reliance on one's circumstances; while self-confidence is confidence in oneself and in one's powers and abilities (Merriam-Webster Dictionary online). Research by Cramer et al (2000) indicates

that confidence can be thought of as a degree of certainty in one's statements or actions. Self-confidence is a judgment of a situation (Hollenbeck & Hall, 2004). Self-confidence affects behavior in the wake of a threatening situation and can give individuals the focus needed to handle the situation effectively (Bandura, 1977). Research has indicated that overconfidence can be a potential peril related to confidence and have a negative impact on accuracy (Kahneman, 2011), but this particular study is unlikely to face such a problem. Self-confidence is related to accuracy and judgments and is context-specific (Cramer et al, 2009). According to Gigerenzer et al, 1991, there is a different mental process that is used for self-confidence related to a single event versus something that is habitual. Attempted phishing attacks typically occur as a single event. There is a distinct differentiation between self-efficacy and self-confidence. Differentiating between an illegitimate email and a legitimate email when faced with a phishing attack focuses specifically on an individual's skills and abilities. However, having the self-confidence to make the decision to ignore the request is something separate from ability. Attempted phishing attacks frequently contain a fear appeal in order to arouse fear in an individual. Individuals with a high self-confidence can face their fears and discount the fear appeal (Byrne, 2004; Giaquinto & Spridigliozzi, 2007). Therefore, when self-confidence is high, an individual will be less likely to respond to a phishing communication and this will negatively impact the relationship between fear arousal and the intention to respond to a phishing communication.

H8: Self-confidence will moderate the relationship between fear arousal and intention to respond to a phishing communication such that when self-confidence is higher, the relationship will be weaker.

A threat appeal can arouse fear so that an individual is motivated to make a behavioral change (Witte, 1991-1992). Fear is aroused when there is a perception of a serious threat that is personally relevant (Witte, 1994). Related to a phishing attack, individuals do not continue to experience a reaction to the stimulus after responding (or not) to the communication. Intention has been linked with the effectiveness of the attempted persuasion of a communicator (Floyd et al, 2000) which can be related to underlying factors associated with why phishing attacks work. According to Boer & Seydel (1996), if a communication causes a person to experience fear, the person will try to reduce that fear and alleviate the threat. An individual's fear arousal will be heightened and result in an increased intention to respond. Research has also shown that fear-arousing messages are an effective means of changing behavior (De Hoog et al, 2007). When fear is strongly aroused, an individual will make a concerted effort to ward off the threat (Janis, 1967) and will cope with the threat and seek reassurance (Lazarus, 1966). If the individual has a high fear arousal related to providing login credentials, the recipient is more likely to respond with the requested sensitive information.

H9: Fear arousal will have a positive influence on the intention to respond to the phishing communication.

Message involvement entails how important a message is to oneself (Petty & Cacioppo, 1990). If individuals find a message to be irrelevant, the message may be deflected (Slavin et al, 2007). However, if an individual sees a message that highlights something that is conceived to be relevant, such as a phishing message, he/she will be have a heightened fear arousal. It is hypothesized that similar to findings by Cheah (2006), high message involvement will have a positive influence on fear arousal. When message involvement is high, an increased personal connection will be felt (Wang et al,

2012). It is expected that message involvement will have a positive influence on intention to respond; similar to findings by Cauberghe et al (2009).

H10: Message involvement will have a positive influence on fear arousal.

H11: Message involvement will have a positive influence on intention to respond to the phishing communication.

3.3 Covariates

A number of control variables have been used related to fraud research. Research has indicated that younger people are more at risk for becoming victims of consumer fraud (Van Wyk & Mason, 2001; Titus et al, 1995). Older email users can have difficulty understanding terminology, be intimidated by using technology, and want to avoid making mistakes (Sayago & Blat, 2010). They may likely have decreased motor skills and memory yet an overconfidence in knowledge of Internet and computer use (Lam & Lee, 2006).

In a study by Pratt et al (2010), victims of Internet crime tended to be younger and more educated. Age and privacy on the Internet have somewhat varied results in that the older users are more concerned with privacy-related items such as access to personal information, identity theft, and spam (Paine et al, 2007). Decision-making as a result of activities such as fraud or manipulation can be difficult for older adults that are experiencing dementia or reduced functioning intellectually (Pinsker et al, 2010). Based on the research mentioned above, the participants' age will be collected.

Those with advanced IT skills will be more likely to speak with their community regarding threats and be more apt to engage in protective activities (Dinev & Hu, 2007). In fact, those that have more years' experience using the Internet and log more hours per week are more knowledgeable about potential threats and how to protect themself (Paine

et al, 2007). Users typically deflect the responsibility of having secure systems and controls in place to other parties (Hallam-Baker, 2008). Data was collected related to experience. In addition, gender has been shown to be a factor for research related to fear. It has been shown that admission of fear is discouraged among men (Rachman, 1978). Gender was collected as part of the survey.

3.4 Summary

This research design is described in detail in the next section. The experiment will give the researcher the opportunity to collect data on individual response in relation to a simulated phishing attack. Survey data will also be collected to further explore the cognitive and emotional responses of the subjects. The Threat Appeal Behavioral Response Model presented above is used to describe the relationship that fear arousal (as related to fear of providing login credentials) and self-confidence have on intention to respond to a phishing attack.

Chapter 4

Research Methodology

4.1. Methodology

This chapter provides details regarding the research methods and additional details about the sample and measurements. The model was tested by collecting both empirical and quantitative data using an experiment and a survey. The use of multiple types of data collection is recommended to gain insight of what is in the minds of the subjects (Lazarus, 1999). The best way to collect accurate data in phishing experiments is to use realistic scenarios that incorporate social engineering (Bakhshi et al, 2009). This research makes a unique contribution by not only providing self-reported survey data using a realistic scenario with an email actually received on campus but also collecting actual behavior in response to a phishing attack. The methods employed by attackers to gain access to sensitive data via phishing are in a state of constant flux. This means that research that is flexible enough to apply to existing and upcoming phishing attacks must be developed. This research explores subject response to phishing attacks related to the Threat Appeal Behavioral Response Model. Additionally, data was collected to determine if phishing training materials and level of fear appeal affect a subject's response to a phishing attack.

4.2. Subjects

Survey data was collected from students currently taking courses at university in the southern United States. The subjects have a variety of backgrounds including (but not limited to) marketing, accounting, information systems, economics, operations, political science, biology, psychology, mathematics, education, nursing, engineering,

music, and architecture. Random sampling of the population minimized threats to external validity. A total of 400 survey emails were sent and 223 surveys were returned resulting in a 56% response rate.

The subjects for the experiment were currently enrolled in the Introduction to Management of Information Systems course at a southern university. For the feasibility of the study, the subjects were not informed specifically about details of the research. Subjects that filled out the original informed consent had the option of opting out of future contact. More details on the informed consent process are in the next section. If the subjects did not opt out of future contact, they were included in the experiment. 144 subjects that previously gave informed consent participated in the training. After removing the subjects that did not consent for future contact, the final count was 101. Of those, 59 subjects (matched by participant number) both filled out a survey and participated in the experiment.

4.3. Survey

The research was approved by the university's Institutional Review Board. Subjects were required to sign an informed consent document prior to participating in the study. The researcher visited classrooms to explain the informed consent process and collect signatures. The document is located in Appendix B. The subjects were offered the chance to win a drawing for a $25 Amazon gift card. One gift card was given away per section. Subjects were given the option to opt out of future contact during the informed consent process and at any time during or after the data collection period. The subjects were informed that the study was related to email usage. It was important for

the success of the research that the subjects did not know the training, phishing attempt, and survey were related.

Subjects were assigned a participant number and sent an individual link to the electronic survey via email. The survey data was collected using Qualtrics (www.qualtrics.com). The survey questions are located in Appendix C. The researcher used adapted survey instruments for all constructs. Survey items for Perceived Self-Efficacy, Perceived Response Efficacy, Perceived Threat Severity, Perceived Threat Susceptibility, and Intention were adapted from Witte (1996). Items measuring Self-Confidence were adapted from Shrauger & Schohn (1995). Fear Arousal items were adapted from Champion et al (2004). Items for Message Involvement were from Vishwanath et al, 2011. Items for Web Experience were (Wright & Marett, 2010). The use of instruments adapted from prior research for the survey portion of the experiment reduced threats to construct validity. The use of surveys in conjunction with experiments has been used to conduct research on phishing response (Downs et al, 2007; Sheng et al, 2010) without putting undue stress on the subjects. The researchers are also able to make a connection between the survey responses and the actual behavioral responses for those individuals that participated in both.

4.4 Experiment

An experiment was conducted using a subset of the population that consisted of subjects that were currently enrolled in Introduction to Management of Information Systems. The experiment was set-up so that data could be collected in response to a realistic phishing attack. Knowledge is a major component in protecting individuals from scams (Weisman, 2008). The students in Introduction to Management of Information

Systems are introduced to phishing early on in the course. Specifically, the course materials address introduce the term phishing and provide information about password theft by means of phishing. In order to set up a plausible scenario in which to gain sensitive information, the subjects were given a course-related assignment. Ideally, studies should involve real-life activities to try to mimic encounters and reduce suspicion (Herzberg & Margulies, 2011). All students in the seven sections that participated in the research were given a training assignment as part of course material.

The experiment collected data from subjects faced with a phishing attack attempt. The experiment was set up as a 2X2 (Training, Fear appeal). The subjects were randomly assigned to one of four experimental treatments. The possible combinations were Low Fear/Baseline Training, Low Fear/Advanced Training, High Fear/Baseline Training, High Fear/Advanced Training. A table showing the possible treatments is below. A flowchart of the experiment is located in Appendix A.

Table 4-1: Possible Treatments

	Basic Training	Advanced Training
Low Fear	Treatment A	Treatment B
High Fear	Treatment C	Treatment D

The researcher had a training site created to provide flexibility in the design of the experiment and treatments. The site was web-based and allowed the subjects to create a password that was stored as a salted hash. A plausible training url was used to ensure the subjects did not doubt the legitimacy of the site. The instructors were sent instructions that they were to introduce the training site as part of the course material. All of the students in the course were assigned the task and given training materials that

contained the link and instructions on how to set up a username and password. The materials are located in Appendix D. In order to access the materials and create a situation in which the subjects had sensitive information to protect, the site requested a user name, password, and email address. As requested by the campus office of information technology, each student was pre-assigned a user name which consisted of their first and last name concatenated.

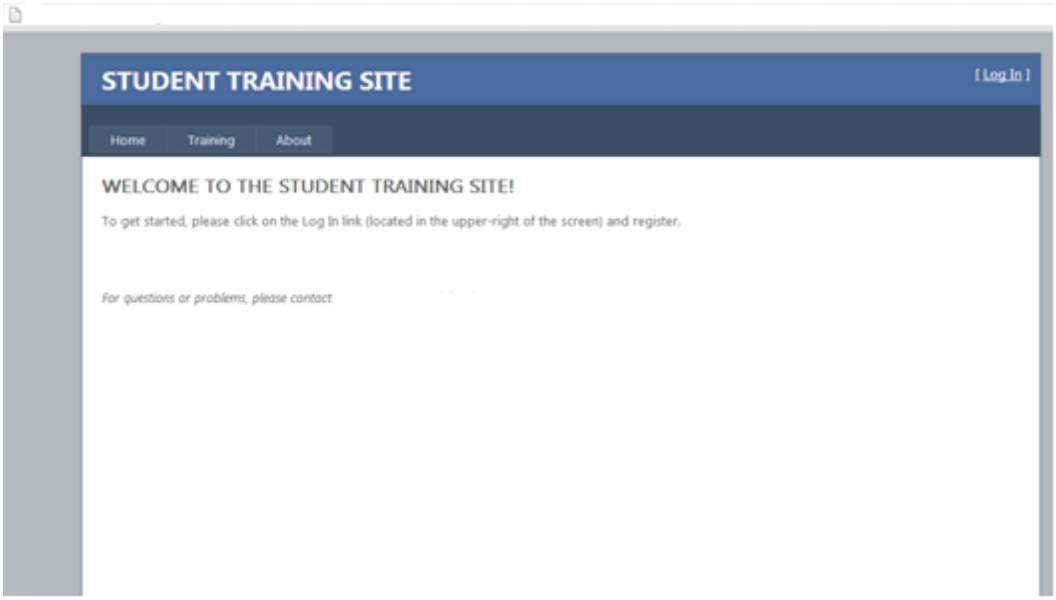


Figure 4-1: Student Training Site Welcome Page

The subjects were randomly pre-assigned treatments when the user names were created. In total, 529 logins were created. Randomly assigning subjects to treatments minimized threats to internal validity. The breakdown by treatment is shown in the table below.

Table 4-2: Treatment Assignment for All Students

Fear	Training: *Basic*	Training: *Advanced*
Low	133	133
High	133	130

After setting up the login information, students were shown a training video with either basic phishing information or advanced phishing content. The video was created using Prezi (www.prezi.com) to engage the students and increase the likelihood of information absorption (Beecroft, 2012). Both videos had the same basic content but the advanced video gave more detailed information about how phishing attacks occur and how to prevent them. The beginning screen of the video is shown in Figure 4-2. The training content is located in Appendix F. The basic video was 1 minute, 21 seconds long and the advanced video was 2 minutes, 47 seconds long. The videos provided images with specific examples as shown in Figures 4-3 and 4-4.

Figure 4-2: Phishing Training Example

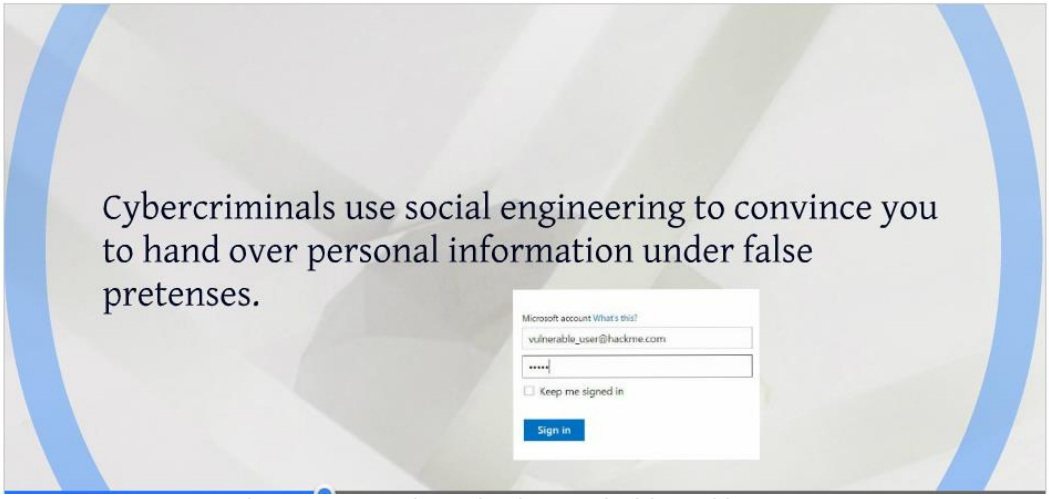


Figure 4-3: Basic and Advanced Video with Image

One week after the training task was due; the subjects that provided consent for future contact were sent a phishing email. The subjects that were pre-assigned to the low fear group received the low fear email and the subjects that were pre-assigned to the high fear group received the high fear email. The university IT department was contacted

prior to the phishing attack to make them aware of any potential problems that might arise and to reduce alarm if information was forwarded to them about the attack. The url was chosen so that it was not a spoofed link to the site. This was done to prevent spam filters from being triggered and disabling the link (Solomon & Chapple, 2005).

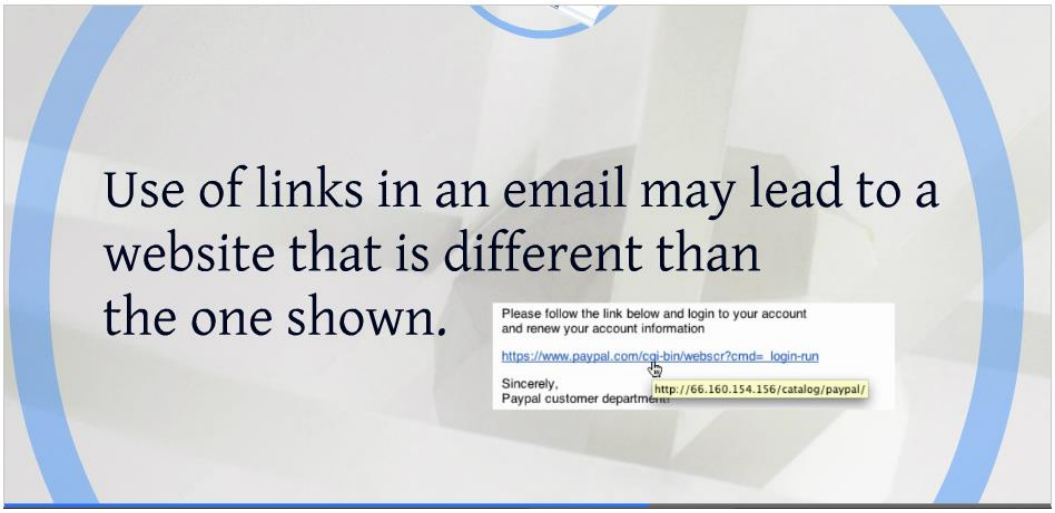


Figure 4-4: Advanced Training with Image Example

One of the reasons that phishing attacks work is that potential victims are manipulated into providing information (Dhillon, 2007). Frequently, the emails request that the recipients take immediate action in order to correct a make-believe flaw (Dhillon, 2007). The low fear and the high fear emails were both worded so that the subjects we instructed to provide credentials to remedy a problem with the database storing their login information. When individuals are acutely aware that they are vulnerable to danger, they are less likely to resist an authoritative request such as the one that is put forth in this research experiment (Janis, 1976).

The low fear appeal message contained neutral language and the high fear appeal message contained very personalistic and vivid language (as specified by Witte 1991-1992). As recommended by Janis (1967), careful consideration was paid to the fear appeals messages to provide seriousness to the threat so that it is not discounted completely but not so much that the subject is left in a distressed state and ignore it. The low fear email asked subjects for verification of his/her login and password that that the site would remain accessible. The high fear email asked for verification of login and password or the account information would be deleted. Both emails contained a link to a fraudulent site that had a login page very similar to the original site. As mentioned by Easttom & Taylor (2011), the perpetrator may setup the phishing site using third party hosting paid for with a prepaid credit card. Upon entering the requested information, the subjects were immediately shown the debriefing document informing them of the purpose of the experiment. This reduced any undue stress placed on the subject. The low fear and high fear appeal emails are located in Appendix G. A diagram of the experiment is provided in Appendix A.

4.5 Pilot Testing

Survey Pilot

Prior to pilot testing, the items were reviewed by three PhD candidates for face validity. The fourth question for fear arousal: “when I think about providing my login credentials, I get depressed” and the fifth question “when I think about providing my login credentials, I get jittery” were dropped because they did not make sense in the context of fear arousal related to a phishing attack and providing login credentials. A pilot test was conducted for the survey using two undergraduate sections in the College of Business in a southern university. A total of 59 responses were received. The data was analyzed

using SmartPLS software (Ringle et al, 2005). Composite reliability for the pilot study ranged from .8844 to .9919 which is well within the range (>.70) for reliability recommended by Hair et al, 2010. Additionally, Cronbach's alpha ranged from .8459 to .9838. This is well within the range recommended by Nunnally, 1978. Cronbach's alpha .70 or above is considered acceptable.

Table 4-3: Composite Reliability and Cronbach's Alpha for Pilot Study

	Composite Reliability	Cronbachs Alpha
Fear Arousal	0.9202	0.9045
Intention to Respond to Phishing Communication	0.9919	0.9838
Perceived Response Efficacy	0.9011	0.8401
Perceived Self-Efficacy	0.9292	0.8878
Perceived Threat Severity	0.9757	0.9626
Perceived Threat Susceptibility	0.9097	0.9005
Self-Confidence	0.8844	0.8459

Experiment Pilot

The experiment training site was reviewed by outside practitioners, PhD students, and professors at the university for accessibility and content quality. Additionally, test emails were sent to various emails using several different email providers to verify that the link would be active (and not disabled by spam filters) in the email. Suggested adjustments were made to the training materials and the video. Software testing was conducted to verify that the training could be accessed and that the backend database was tracking information such as participant number, click, and time/date training accessed.

A formal pilot was conducted using a graduate class in the College of Business at a southern university. A total of 12 subjects were assigned the training task. Subjects were randomly assigned to one of four treatments: high fear/basic training, low fear/basic training, high fear/advanced training, and low fear/advanced training. A week after the task was assigned the subjects were sent the phishing email. Zero subjects responded to the email. A number of respondents sent emails directly to the professor questioning the validity of the email. The subjects were all information systems majors so it was expected that the click response rate would be very low. However, the pilot allowed the researcher to collect feedback from the subjects and suggested adjustments were made to the phishing email content and the phishing link in the email. All of the subjects were able to easily set up login information from the instructions and view the training video.

4.6 Summary

The data was collected over the course of one semester. The survey provided necessary insights to explore the model. The experiment was set up to provide insights to explore the influence that fear and level of training have on an individual's decision to click on a link. The next section details the results of the data collection. The preliminary analysis section provides information about validity and reliability. Next, the results of the hypotheses are explained. Additional exploration of the survey data is presented in the post-hoc analysis section. A write-up of the results of the experiment is last.

Chapter 5

Research Results

5.1 Preliminary Analysis

This study entailed survey and experimental data collection. The survey data was collected electronically using Qualtrics (www.qualtrics.com). The survey data was analyzed using SmartPLS software (Ringle et al, 2005). Partial Least Squares (PLS) is more flexible with sample size when compared to Structural Equation Modeling (SEM) (Hair et al, 2006). The data was reviewed for missing data, unengaged responses, and outliers. The total number of survey responses was 225. After removal of cases due to missing data, unengaged responses, and outliers (in accordance with procedures outlined in Aguinis et al, 2013) the total usable sample size was 192. The table below shows the demographics for the survey sample.

Table 5-1: Demographics of the Survey Sample

Demographic	Category	Count	Percentage
Gender	Male	97	50.5%
	Female	95	49.5%
Age	18-29	179	93.3%
	30-39	7	3.6%
	40-49	4	2.1%
	50-59	2	1%
Education	High School	4	2.1%
	Some College	170	88.5%
	Bachelor's Degree	16	8.4%
	Other	2	1%

A principle components analysis was performed in SPSS. This resulted in 8 factors. The items for perceived self-efficacy, perceived response efficacy, fear arousal, perceived threat severity, perceived threat susceptibility, and intention to respond all loaded under the appropriate construct. However, self-confidence loaded as 2 separate items. CON1 “I have more confidence in myself than most people I know”, CON3 “I have fewer doubts about my abilities than most people”, and CON7 “If I were more confident about myself, my life would be better “ loaded as one construct. CON2 “When things are going poorly, I am usually confident that I can successfully deal with them”, CON4 “Much of the time I don’t feel as competent as many of the people around me”, CON5 “I lack some important capabilities that may keep me from being successful”, and CON6 “I often feel unsure of myself, even in situations I have successfully dealt with in the past” loaded as one construct. This indicated problems with this measurement item. Reliability for items 1, 3, and 7 is .7021 and Cronbach’s alpha is .6941. However, items 3 and 7 had very low factor loadings (.146 and -.041). These items were dropped and resulted in 1 item remaining. Item Reliability for items 2, 4, 5, and 6 is .4593 and Cronbach’s alpha is .4634. Dropping item 6 improved composite reliability to .7865 but did not improve the Cronbach’s alpha beyond .6560. Cronbach’s alpha of < .7 (but not less than .6) is considered acceptable in exploratory research (Hair et al, 2006). More details are explained on self-confidence in section 5.2 below.

The constructs were checked for validity, reliability, and internal consistency. Reliability evaluates the consistency of the measurements of a variable (Hair et al, 2006). As mentioned by Hair et al (2006) it is best to use several measures for internal consistency. Composite reliability looks at the items and if they do a satisfactory job measuring the construct (Gotz et al, 2007). The recommended cutoff for composite reliability is .70 (Fornell & Larcker, 1981; Gefen & Straub, 2005). All of the variables had

a composite reliability of .8159 or greater which falls well within the recommended cutoff. In addition, Cronbach's alpha is recommended as between .60 and .70 to be in the range of acceptable (Hair et al, 2006). The Cronbach's alpha range from .6016 to .9754 which fall within the range and indicate no problems with internal consistency.

Table 5-2: Composite Reliability and Cronbach's Alpha

	Composite Reliability	Cronbach's Alpha
Fear Arousal	0.8949	0.8681
Intention to Respond to Phishing Communication	0.9879	0.9754
Perceived Self-Efficacy	0.9352	0.8964
Perceived Threat Severity	0.8159	0.7019
Perceived Threat Susceptibility	0.8486	0.7625
Perceived Response Efficacy	0.8329	0.6016

Next, validity was evaluated. Validity looks at whether a variable represents what it should (Hair et al, 2006). Convergent validity can be validated by looking at the loadings of factors on other factors and also the average variance extracted (AVE). In order to satisfy convergent validity, the factor item loadings should be greater than .6. Several of the items had low loadings and had to be removed from the model. Perceived threat severity 1, and fear arousal 5, and web experience 1, and response efficacy 1 were removed. The cross loadings from SmartPLS for the remaining variables are displayed in the table below. There is no evidence of cross loading on other constructs. The AVEs for the variables are also displayed in the table below. It is recommended that for adequate convergent of items, the AVEs exceed .50 (Hair et al, 2006). All of the AVEs exceeded .50.

Table 5-3: Cross-loadings

	Fear Arousal	Intention to Respond to Phishing Communication	Message Involvement	Perceived Response Efficacy	Perceived Self-Efficacy	Perceived Threat Severity	Perceived Threat Susceptibility	Self-Confidence
CON1	0.1433	0.1153	0.0491	0.0446	0.1204	-0.0139	-0.0864	**1**
FA1	**0.6684**	-0.1043	0.1523	-0.0598	-0.0574	0.0697	0.0005	0.117
FA2	**0.6945**	-0.1289	0.0503	-0.0191	-0.0858	0.0802	0.0568	0.078
FA3	**0.8206**	0.0369	0.1559	-0.1107	-0.1707	0.051	0.1891	0.1292
FA6	**0.835**	0.0251	0.2409	-0.1664	-0.1523	-0.0396	0.242	0.1341
FA7	**0.7607**	-0.055	0.03	-0.0156	-0.1164	0.1452	0.1378	0.0799
FA8	**0.8046**	0.1175	0.145	-0.0906	-0.1121	0.067	0.1486	0.0999
INT1	0.0281	**0.9883**	0.3943	-0.1264	-0.3507	-0.0599	-0.0179	0.1306
INT2	-0.008	**0.9875**	0.3911	-0.11	-0.3268	-0.0109	-0.0342	0.0967
MIIndex	0.1912	0.3975	**1**	-0.2137	-0.2299	-0.1374	-0.0397	0.0491
RE2	-0.1098	-0.0565	-0.1568	**0.8732**	0.292	0.1358	-0.1607	0.0248
RE3	-0.096	-0.1549	-0.2096	**0.8156**	0.1847	0.158	-0.0821	0.0533
SE1	-0.1082	-0.2973	-0.2054	0.2529	**0.912**	0.0721	-0.1078	0.1571
SE2	-0.1991	-0.2903	-0.2132	0.2898	**0.9182**	-0.0489	-0.2139	0.0663
SE3	-0.1315	-0.3486	-0.2084	0.2379	**0.8996**	0.0135	-0.0912	0.1134
TSE2	0.0139	-0.0543	-0.1397	0.1744	0.014	**0.8941**	0.0221	0.0097
TSE3	0.0956	-0.0061	-0.099	0.1251	0.002	**0.8603**	0.0507	-0.0372
TSU1	0.2221	-0.0528	-0.0218	-0.0945	-0.1173	0.0608	**0.8757**	-0.0751
TSU2	0.1497	0.0237	-0.0303	-0.1813	-0.1696	0.0179	**0.8941**	-0.0753
TSU3	0.065	-0.1131	-0.1099	-0.0046	-0.02	-0.0011	**0.6214**	-0.0664

Table 5-4: Average Variance Extracted (AVE)

Construct	AVE
Fear Arousal	0.6012
Intention to Respond to Phishing Communication	0.976
Perceived Self-Efficacy	0.8279
Perceived Threat Severity	0.7046
Perceived Threat Susceptibility	0.6551
Perceived Response Efficacy	0.7139

5.2 Hypotheses Testing

Perceived self-efficacy is the belief that a person has in their ability to carry out a recommended action. In this case, individuals were asked about their ability to prevent their login credentials from being compromised. It was hypothesized that individuals that have a belief that they are able to prevent their login credentials from being compromised

were less likely to respond to a phishing scenario (-.307, t=4.942). Hypothesis 1 was supported at p <.001.

Individuals that had the belief that the threat of having login credentials compromised is serious were more likely to believe that they are able to prevent an attack. The relationship was not significant (.017, t=.123). Hypothesis 2a is not supported. Individuals with the belief that the threat of having login credentials compromised is serious are more likely to believe that doing things such as not clicking on links in emails and verifying the address of the sender will prevent an attack (.181, t=2.113). Although the relationship is significant, the relationship was not in the hypothesized direction thus making hypothesis H2b unsupported.

Individuals that believe having login credentials compromised is likely to occur have a decreased belief in their ability to prevent an attack. The relationship is significant (-.150, t=1.96) and provides support for hypothesis 3a. Individuals that believe having login credentials compromised is likely to occur have a decreased belief that they their actions (not clicking on links in emails, verifying the address of the sender, etc..) will avert the threat. The relationship is significant (-.150, t=1.96) and provides support for hypothesis 3b.

When individuals are in a situation that they believe they are able to face and have high efficacy, their fears can be reduced or even eliminated (Bandura et al, 1977). Individuals that had a decreased belief in their ability to prevent their login credentials from being compromised had a decreased fear arousal (-.092, t=1.246). The results were not significant therefore hypothesis 4 is unsupported. Individuals that had a high level of their belief that the actions they took would advert the threat had a decreased intention to respond to the phishing email scenario. The relationship was not significant (-.044, t=.557) thus making hypothesis 5 unsupported.

Individuals that have a high threat severity will have an increased fear arousal. The results for hypothesis 6 were positive though not significant (.081, t = .791). Thus, hypothesis 6 was not supported. Individuals that have a high threat susceptibility had an increased fear arousal (.189, t=2.23) thus supporting hypothesis 7.

Hypotheses 8 stated that individuals that have a high self-confidence have a moderating effect on the relationship between fear arousal and the intention to respond to the phishing attack. The relationship was not in the predicted direction and was not significant thus making hypothesis 6 unsupported (-.028, t=.382). As mentioned in the previous section, there were was indication that the items separated into two constructs. When the data was analyzed in SmartPLS, there were also problems with the item loadings, reliability, and Cronbach's alpha. There was no indication of this during the pilot study. Analysis was run in SPSS to find the Cronbach's alpha for the construct if items are deleted. The analysis indicated that if item 6 "I often feel unsure of myself, even in situations I have successfully dealt with in the past" was deleted, the Cronbach's alpha would improve from .697 to .712. This is within the recommended cutoff of .70. However, composite reliability for those items was .4593. The results from the exploratory factor analysis resulted in retaining Item number one, "I have more self-confidence in myself than most people I know". This question refers to Relational Self-Confidence and can be used to reflect self-confidence compared to others. This relationship was explored and resulted in a positive significant relationship (.137, t=2.410). Individuals with a high relational self-confidence were more likely to respond to the email. The retention of items CON2, CON4,and CON5 as a self-confidence variable resulted in a decreased intention to respond to a phishing attack which would be expected. However, the relationship was not significant (-.08, t = .938). It is possible that

the scale, adapted from Shrauger & Schohn (1995) for general self-confidence was not situationally specific enough. Items that measure both general self-confidence and context-specific self-confidence (Shrauger, 1972).

H9: Individuals that had a high level of fear arousal related to providing login credentials were less likely to respond to the phishing email. The hypothesized relationship was that fear would have a positive influence on intention to respond. The relationship was significant (-.130, t=2.267) but not in the hypothesized direction. These results are explained by an underlying level of suspicion that is associated with a phishing message. When an individual receives a message that is suspicious and he/she has a high level of fear associated with providing login credentials, the intention to respond will be lower. A high level of fear of providing login credentials indicates that the individual is aware that the message is potentially fraudulent and thus will be less likely to respond. Another explanation could be that the targeted research demographic is frequently exposed to fear-inducing messages and thus has achieved habituation or a decreased level of fear (Rachman, 1978). Yerkes-Dodson law is another area that may explain why the relationship between fear arousal and intention to respond to a phishing attack was negative (Yerkes & Dodson, 1908). The relationship between arousal and performance has an inverted u-shaped curve. When fear arousal is high, performance is affected and impairs the working memory/decision-making capability.

Message involvement had a positive influence on fear arousal. The relationship was significant (.182, t=2.159). When individuals are engaged in the message, they had an increased fear arousal. This provides support for hypothesis 10. In addition, message involvement had a positive influence on intention to respond to a phishing

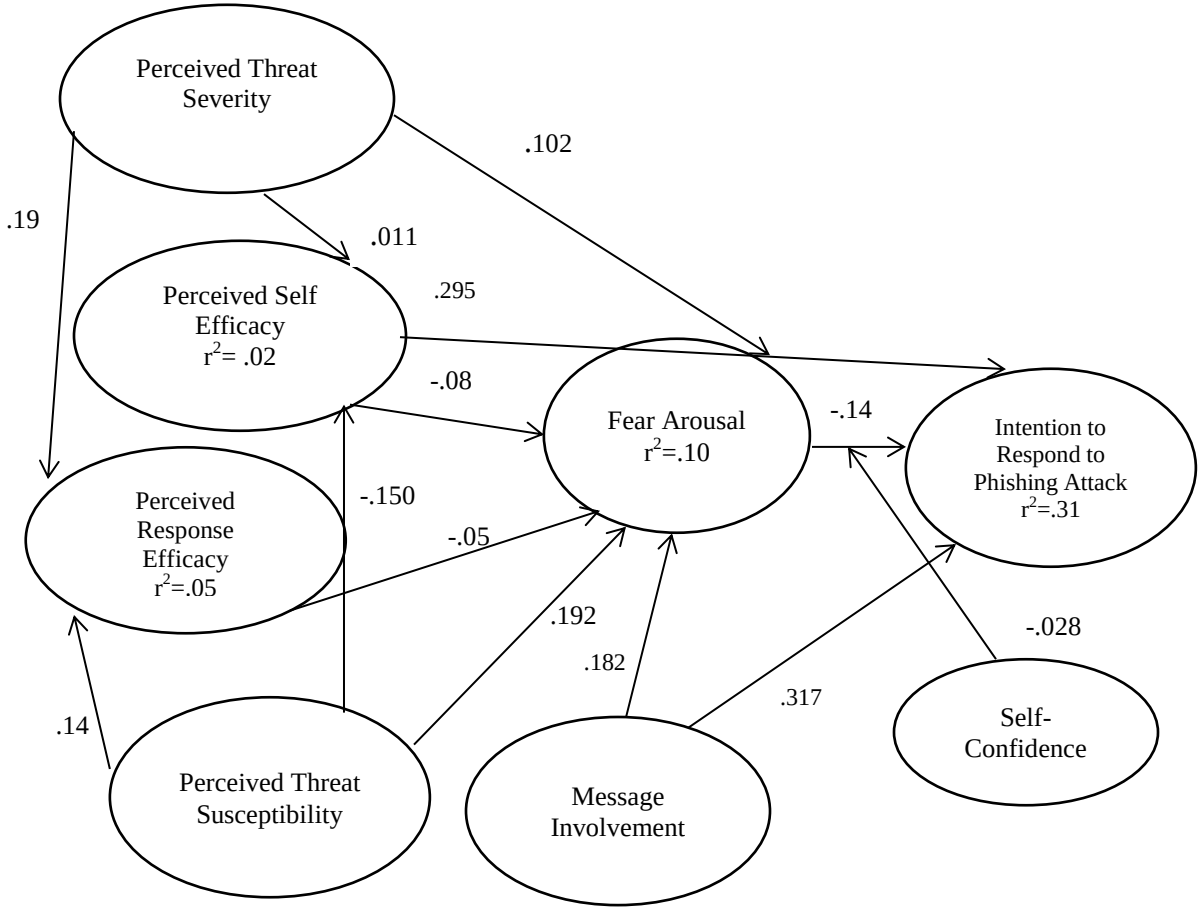
attack. The relationship was significant (.317, t=4.864). Individuals that had a high level of message involvement had an increased intention to respond to a phishing attack. This provides support for hypothesis 11. Table 5-5 below provides a summary of the hypotheses and figure 5-2 below summarizes the results for the hypothesis testing.

Table 5-5 Summary of the Survey Results

	t-statistic	p-value (1-tailed)	
H1	4.942	<.0001***	Supported
H2a	0.017	0.4932	Not Supported
H2b	2.113	0.0179**	Supported
H3a	1.96	0.0257**	Supported
H3b	1.96	0.0257**	Supported
H4	1.246	0.1071	Not Supported
H5	0.557	0.2891	Not Supported
H6	0.791	0.2150	Not Supported
H7	2.23	0.0135**	Supported
H8	0.382	0.3514	Not Supported
H9	2.267	0.0123**	Significant, Opposite Direction
H10	2.159	0.0160	Supported
H11	4.864	<.0001***	Supported

*p<.10
**p<.05
***p<.001

Figure 5-2: Results in SmartPLS



5.3 Post-hoc Analysis

The researcher conducted additional post-hoc analysis to evaluate the difference between groups that were “high” risk and groups that were “low” risk. Survey data was collected using an adapted scale from Van Wyk & Benson (1997). While risk did not significantly influence intention to respond to a phishing attack (-.006, t = .131), the relationship was negative. This is similar to what Van Wyk & Benson (1997) found in their study; risk-taking did not significantly influence fraud victimization. Risk also did not significantly influence fear arousal (.041, t = .510).

To further explore the influence of risk, the researcher was interested in evaluating high risk versus low risk groups. The survey data was assessed in SPSS using a data split. The high risk group had a significant decreased intention to respond when fear arousal was high. This is interesting because Van Wyk & Benson (1997) found that high risk individuals are more open to fraudulent transactions but risk taking did not equate to a successful victimization. This research was in agreement with those findings; risky individuals were less likely to respond out of fear. Another interesting finding was that web experience resulted in an increased intention to respond to the phishing communication. Those with increased web experience were *more likely* to respond. Web experience had a significant positive influence on intention to respond (.167, t = 2.370)

Table 5-6: Risk Group High/Low

Coefficients[a]

RiskGrp	Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
			B	Std. Error	Beta		
High	1	(Constant)	6.592	1.521		4.335	.000
		FearArousal	-.213	.127	-.160	-1.674	.097
		PerceivedSelfEfficacy	-.502	.134	-.372	-3.733	.000
		PerceivedThreatSeverity	.038	.158	.023	.242	.809
		PerceivedThreatSusceptibility	.067	.107	.059	.630	.530
		Gender	-.369	.338	-.107	-1.091	.278
		Age	-.335	.336	-.098	-.997	.321
Low	1	(Constant)	3.924	1.323		2.966	.004
		FearArousal	-.041	.112	-.035	-.360	.719
		PerceivedSelfEfficacy	-.233	.105	-.221	-2.219	.029
		PerceivedThreatSeverity	.050	.143	.034	.353	.725
		PerceivedThreatSusceptibility	-.102	.099	-.100	-1.035	.303
		Gender	.232	.300	.077	.775	.440
		Age	-.365	.310	-.114	-1.178	.242

a. Dependent Variable: IntentiontoRespondtoPhishingAttack

The data was split by gender (Male = 1; Female = 2). For women, fear had a significant negative relationship on intention to respond to a phishing attack. Also of interest is that men had a decreased influence of fear arousal on intention to respond to a phishing attack. This is interesting because men are taught not to express fear as an emotion (Rachman, 1978).

Table 5-7: Split by Gender (1=Male, 2=Female)

Coefficients[a]

Gender	Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	
			B	Std. Error	Beta			
1	1	(Constant)	3.048	1.601		1.904	.060	*
		FearArousal	-.047	.121	-.041	-.388	.699	
		SelfConf245	-.078	.116	-.069	-.672	.503	
		PerceivedSelfEfficacy	-.447	.143	-.321	-3.129	.002	**
		PerceivedThreatSeverity	.112	.148	.075	.757	.451	
		PerceivedThreatSusceptibility	-.031	.112	-.029	-.278	.781	
		SelfConfidence1	.193	.104	.196	1.849	.068	*
		WebExperience	.270	.151	.177	1.788	.077	*
2	1	(Constant)	6.475	1.294		5.005	.000	***
		FearArousal	-.186	.111	-.154	-1.667	.099	*
		SelfConf245	-.242	.115	-.206	-2.113	.037	**
		PerceivedSelfEfficacy	-.461	.093	-.466	-4.979	.000	***
		PerceivedThreatSeverity	-.121	.130	-.087	-.930	.355	
		PerceivedThreatSusceptibility	-.178	.100	-.165	-1.785	.078	*
		SelfConfidence1	.208	.102	.197	2.036	.045	**
		WebExperience	.202	.124	.155	1.632	.106	

a. Dependent Variable: IntentiontoRespondtoPhishingCommunication

*p<.10
**p<.05
***p<.001

5.4 Experiment

The experiment was conducted using students enrolled in the Introduction to Management of Information course in the College of Business at a southern university. The students were told by their instructors that the department was testing out a new site and they were to go to the training site url to sign up for an account. They were given one week to complete a training task and provided with training materials. All students in the course were assigned the task.

A total of 527 logins were created and 335 individuals participated in the training. Of those participants, 144 had consent forms on record and 101 gave prior consent for future contact. The final total of subjects for the experiment was 101. Since the random assignment of participants to treatments occurred prior to both the training video assignment and the fear appeal level assignment, the resulting breakdown of subjects to treatments is unbalanced. Table 1 below shows the final assignments for the experiment.

Table 5-8: Final Subject Treatment Assignment

	Training	
Fear	*Basic*	*Advanced*
Low	26	21
High	25	29

The independent variables are: Level of Fear (low, high) and Level of Training (low, high). The dependent variable, Email Click, was dichotomous (click, no click). The recommended statistical method for analyzing data with a dichotomous dependent variable is logistic regression (Kutner et al, 2005).

The researcher created a spoofed phishing site that was very similar to the student training site login page. The color and login information were similar but not a direct copy. A comparison of the two sites is shown below in Figures 1 and 2. The url chosen was something that was realistic but not an obvious phishing site. The original url was included in the link in the email along with other random data to mask the participant number used to track the clicks. Additionally, care was taken so that the url would not be

flagged as spam. The subjects were sent an email based on their fear appeal assignment. The email examples are located in Appendix G. The emails were sent from the spoofed site mail account. Random emails were sent before, during, and after the phishing attack to ensure that the emails were still being allowed through the university mail server.

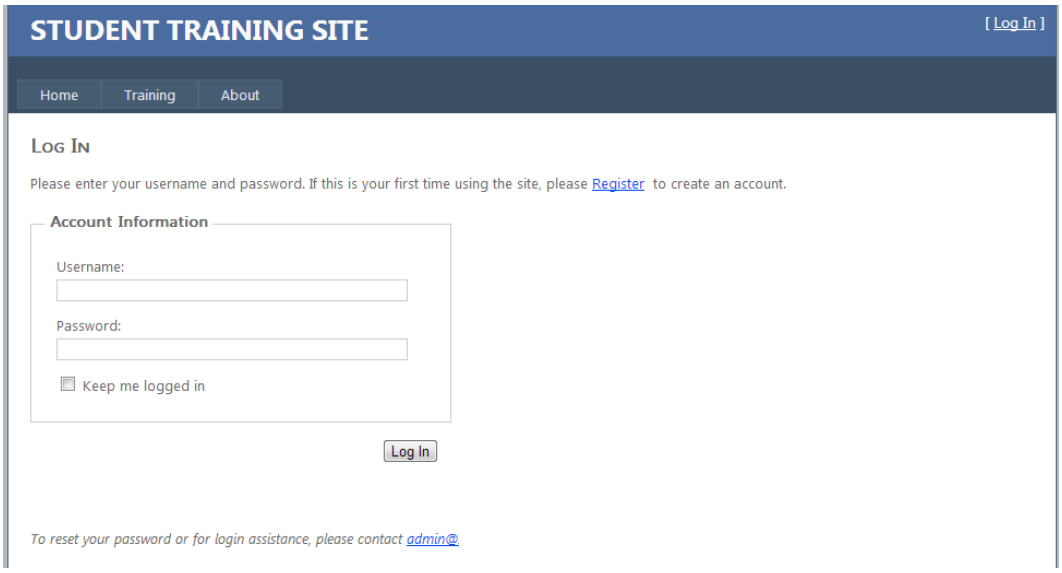


Figure 5-3: Original Login Screen

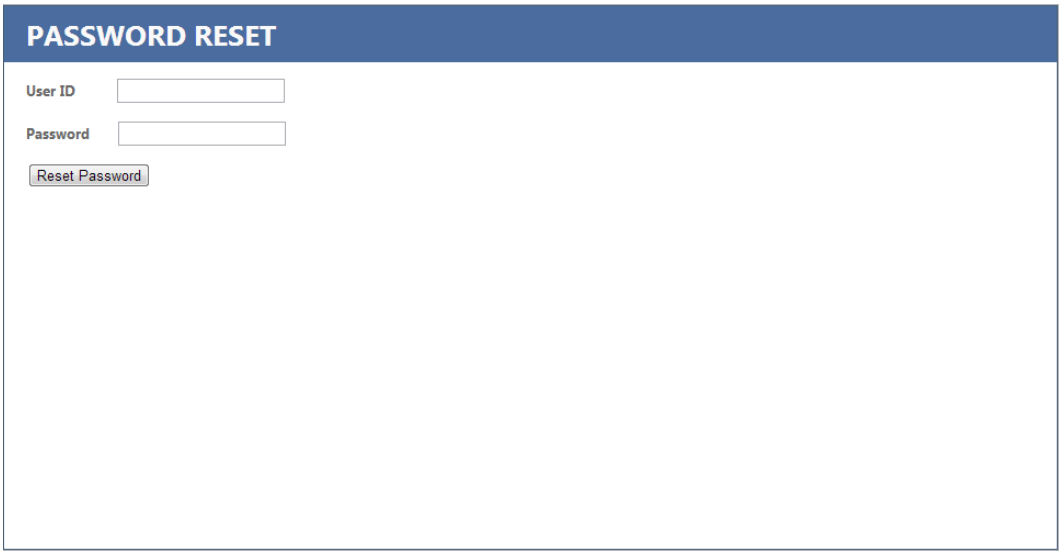


Figure 5-4: Spoofed Login Screen for Fraudulent Site

The subjects were sent individual links so that the participant number could be preserved. Of the 18 subjects that clicked on the link, 11 also completed survey data. A summary of gender among subjects that clicked on the link is shown in the table below.

Table 5-9: Gender of Subjects that Clicked on Link

Gender	Count
Male	3
Female	8
Unknown	7

Table 5-10: Number of Clicks (and Ratio Clicked) by Treatment

	Training	
Fear	Basic	Advanced
Low	6 (23%)	3 (14%)
High	5 (20%)	4 (14%)

Logistic regression was performed on the original experimental dataset which consisted of 101 subjects. The dependent variable, click, was dichotomous and coded as "1" if the subject clicked on the link and "0" if they did not click. The training level was "0" for basic training and "1" for advanced training. The fear level was "0" for the low fear email and "1" for the high fear email. The analysis was run using SPSS software. The results are shown below.

Table 5-11: Intercept Only

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 0	Constant	-1.528	.260	34.558	1	.000	.217

Table 5-10 above represents the model with the intercept-only. Of the 101 subjects, 18 clicked on the link and 83 did not click on the link. The predicted odds of clicking on the link are .217.

When level of fear and level of training are added as predictors, the results are shown below. The regression equation for training level is

$$\ln(ODDS) = -1.231 + (-).513 TrainingLevel$$

Given this information, the odds of clicking on the link based on training level can be calculated. This is calculated using the equation $ODDS = e^{a+bX}$. The odds of clicking on the link for subjects that had basic training (Training = 0) is $ODDS = e^{-.513 + (-)1.231(0)}$. If a subject had basic training they were .60 times less likely to click on the phishing link. The odds of clicking on the link for subjects that had advanced training (Training = 1) is $ODDS = e^{-.513 + (-)1.231(1)}$. If a subject had advanced training they were .175 times less likely to click on the phishing link. Probabilities can also be calculated from this information. The probability equation is $\hat{Y} = \frac{ODDS}{1+ODDS} = \frac{.60}{1.60} = .375$. 37.5% of those that have basic training will click on the link. For advanced training the probability is $\hat{Y} = \frac{ODDS}{1+ODDS} = \frac{.175}{1.175} = .149$. 14.9% of those that had advanced training will click on the link. However, training level was not a significant predictor of click with p>.05.

The regression equation for fear level is

$$\ln(ODDS) = -1.231 + (-).125 FearLevel$$

The odds of clicking on the link for subjects that received the low fear email can be calculated as $ODDS = e^{-.125 + (-)1.231(0)}$. If a subject received the low fear email they were .88 times less likely to click on the phishing link. The probability of clicking on the link for subjects that received the low fear email is $\hat{Y} = \frac{ODDS}{1+ODDS} = \frac{.88}{1.88} = .468$. If a subject received the low fear email the probability that he/she would click on the link is 46.8%. The odds of clicking on the link for subjects that received the high fear email is $ODDS = e^{-.125 + (-)1.231(1)} = .257$. If a subject received the high fear email they were .257 times less likely to

click on the phishing link. To calculate the probabilities for high fear, the equation is $\hat{Y}$ = $\frac{ODDS}{1+ODDS}$ = $\frac{.257}{1.257}$ = .205. If a subject received the high fear email the probability that he/she would click on the link is 20.5%.

Table 5-12: Dependent Variable Click in SPSS

Variables in the Equation

		B	S.E.	Wald	df	Sig. (1-tailed)	Exp(B)
Step 1[a]	TrainLev	-.513	.533	.927	1	.168	.598
	FearLev	-.125	.525	.056	1	.406	.883
	Constant	-1.231	.421	8.540	1	.0015	.292

a. Variable(s) entered on step 1: TrainLev, FearLev.

The model did not provide a better fit to the data than the intercept-only model (Constant) above. It is possible that the high-fear message provided an excessively high level of arousal and thus deflected the response mechanism. While the research supports the use of fear appeals to cause individuals to take action; there has been additional research that indicates that fear can go too far (Witte, 1996).

Logistic regression was performed using the matched survey/experiment data. The initial total was 56 and after the removal of 5 outliers and unengaged response a total of 51 responses remained. Logistic regression was performed using the dependent variable “click” which indicates whether or not the subject clicked on the link. Perceived self-efficacy, perceived threat severity, and fear arousal were significant at the .05 level ($p < .05$). Perceived self-confidence and perceived threat susceptibility were not significant ($p > .10$).

Table 5-13: DV Click with Survey Data

Variables in the Equation

		B	S.E.	Wald	df	Sig. (1-tailed)	Exp(B)
Step 1[a]	PerceivedSelfEfficacy	-.586	.310	3.583	1	.0290**	.556
	PerceivedThreatSeverity	1.042	.616	2.864	1	.0455**	2.835
	PerceivedThreatSusceptibility	.396	.334	1.411	1	.1175	1.486
	SelfConfidence	-.351	.311	1.281	1	.1290	.704
	FearArousal	-.775	.411	3.562	1	.0295**	.461
	Constant	-1.871	3.999	.219	1	.3200	.154

**p<.05

Individuals that had a high fear arousal had a decreased actual behavior to click on the link. These results corroborate with the self-reported data which indicated that fear arousal had a negative relationship with intention to respond to a phishing attack.

Chapter 6

Discussions and Conclusions

6.1 Discussion

This research explored how fear and self-confidence influenced individuals' response to a phishing communication. The model presented is also applicable to other security research. As more knowledge is gained regarding how fear of providing login credentials can affect responses to phishing attacks and additionally how self-confidence can affect the relationship between fear and intention to respond, research can provide valuable information to assist in preventing the use of social engineering to obtain sensitive information. The world is at a time where security vulnerabilities are in a state of ever-evolving transition. It is pertinent that researchers explore influential emotional reactions that affect an individual's decision to click on a phishing link.

The relationship between fear arousal related to providing login credentials and intention to respond was significant though opposite of what was hypothesized. Fear arousal led to a decreased intention to respond. This is in line with Rachman (1978) who wrote that when an individual has a perceived state of mastery, in this case login credentials being compromised, that fear is decreased. So although a person might be fearful providing their login credentials that will not result in an increased level of response. It is possible that experience counteracted the effects of fear. Feelings and emotions tie in with experience to allow individuals to learn from mistakes (Lehrer, 2009).

Behaviors related to deceptive/fraudulent practices by email and computer-related communications have not been extensively studied (Chiluwa, 2009). There is currently a research gap; specifically in the area of phishing. Research is still very exploratory in nature and is lacking strong theoretical grounding. In addition, it is difficult to collect actual behavioral data. According to Finn & Jakobsson (2007), phishing

research can be tricky to set up; particularly in light of the fact that subjects are being deceived into providing sensitive information. However, there is not an actual risk of exploitation as long as the researcher does not gain access to any sensitive information. In light of this issue, the researcher took extra precautions to ensure the security of any potential sensitive information collected. Similar to research conducted by Kanich et al (2008; 2009), this research will *reduce* harm to its subjects. The training site was created to provide a plausible scenario for a phishing attack without risk to the subjects. The research collected data related to subjects' reaction to a stimulus – in the form of a fear appeal message. The subjects that participated in the experiment gained valuable knowledge about phishing and the potential dangers of providing sensitive information. The expert-level training group has an added advantage by receiving additional training and knowledge about phishing. Even though the results were not statistically significant, there were fewer clicks for subjects that received advanced training when compared to subjects that received basic training. 18% of individuals *did* click on the link. Those responsible for phishing attacks do not need a large number of clicks per campaign to gain funds with just one or two out of 100 emails sent deemed a successful hunt (Armerding, 2012). Even with education and training in place there will likely be Internet users that lack the skills necessary to prevent sensitive information such as user name and password from being compromised (Hallam-Baker, 2008). Although there was not a statically significant difference between the low fear and high fear treatments, there is still additional research that can be done with fear appeals and phishing. Some of the limitations of the study are mentioned below.

6.2 Limitations

This research was approved by the university's institutional review board (IRB) which helps to ensure that the subjects are not subjected to undue stress or harm. The

study required an informed consent which typically describes the study in detail. However, if subjects knew the true nature of the study, an attempted phishing attack, it would have jeopardized the validity of the experiment. The subjects were told that they were participating in a study on email usage. The subjects filled out the survey at the beginning of the semester. The experiment was conducted at the end of the semester. Because there were multiple instructors that allowed the researcher to use their classes to participate in the research, the instructors were given specific instructions on how to introduce the training. A list of "Dos" and "Don'ts" is shown in the table below.

Table 6-1: Dos and Don'ts for Instructors

Please Do:
- Provide the instructions to your students and ask them to register and watch a training video. Please have them complete the task by the specified date.
- Tell the students that we are trying out a new site and the training is related to course material.
- Have them email admin@ the training site with any problems related to the site, login information, or any other issues.
Please Do Not:
- Mention that there are two different training videos.
- Show the video or log in with the Test login during class.
- Mention that I created the site or that it is an experiment.
- Mention that there will be any further communication related to this site (I will be sending emails for those that consented to be contacted. I will let you all know when that happens).

The phishing emails were approved to be sent to individuals that did not check a box on the informed consent to prevent future contact regarding the research. The statement “If you prefer not to be contacted for future research opportunities, please check this box” was at the bottom of the consent. Both the requirement for an informed consent and the requirement for permission for future contact had an effect on the sample size for the experiment. A total of 335 individuals participated in the training. Of those, only 101 provided informed consent with permission for future contact. Because the dependent variable was dichotomous, click yes or no, there was just not enough data to come to a definitive conclusion on the treatments. The combined survey/experiment data analysis does indicate a significant relationship between fear and click which gives the researcher a starting point for future studies.

All of the data for this study was collected using students for the sample which can be concerning from a generalizability standpoint. Different groups (undergraduates included) will interpret different things as persuasive (Anderson & Agarwal, 2010). However, this study is exploratory and begins groundwork for future studies involving Internet users. Additionally, for the experiment, it was necessary to select subjects that 1) had baseline, common knowledge of phishing to help control for phishing knowledge and 2) had phishing discussed in class so that the training material did not raise suspicion.

Additionally, the training site was only introduced for one training task. The subjects did not have the opportunity to use the site to watch other training videos. It is possible that if there was more of a sense of importance placed on the site and its login that subjects would have been influenced differently on their response. The subjects did not have a sense of wanting to protect their login the same as something of importance such as a bank account.

Lastly, it is possible that the high fear email was too strong and the low fear email too weak persuasively. According to Ray & Wilkie (1970) moderate fear arousal may result in the largest response rate. Janis & Feshbach (1953) found that individuals were the most compliant when fear-arousing materials were at a minimum. Fear appeals that are too strong can cause message avoidance (Ray & Wilkie ,1970) which may be the case in this study with reference to the subject's account being "deleted". However, fear is a necessary component in the fear appeal process to assist with information processing (Tanner et al, 1991). Additionally, recurrence of an incident can take away the surprise (Kahneman, 2011). Subjects that are repeatedly exposed to fear-appeal messages may have a desensitized reaction; thus reducing its effect. In particular, a judgment or beliefs and knowledge can reshape a situation in a manner that no longer is an anticipation of harm (Lazarus, 1966). The use of undergraduates for the experiment may have influenced the click results. The majority of the subjects were in the 18-29 age group (93%). As mentioned by Anderson & Agarwal (2010) although this age group is representative of a majority of Internet users, they may have differing opinions on what is persuasive.

6.3 Contributions to Research and Practice

The contribution that this research will make is much more valuable than any risk of harm to the subjects in the experiment. The results have provided researchers and practitioners with valuable insight as to how threatening emails can influence a subject's response to a phishing attack. When a fear appeal is very threatening, subjects shut down and did not respond at all.

This research contributes to both academia and practice in that anyone who has access to the Internet is at risk of being phished. Phishers do not differentiate between the home user and a user that is within an organization. Hackers will continue to exploit security loopholes such as providing false IP addresses to redirect Internet traffic to fraudulent websites (Schneider, 2008). The Internet has "expanded to a point where a problem can no longer be traced to a source" (Hallam-Baker, 2008) which creates the perfect environment to commit crime and get away with it. There is also a lag in the detection and shutdown of phishing sites thus stressing the importance of user education (Stamatellos, 2007). It is important that Internet users are prepared to handle phishing attacks. By attempting to gain insight into the underlying reasons that motivate an individual to respond to a phishing communication, researchers will be able to improve user education to specifically address this susceptibility. The best method for reducing cybercrime such as phishing is to encourage the prevention of it. This can be accomplished by implementing education specific to the risks faced by individuals and organizations (Brenner, 2010).

6.4 Future Research

While experiments on large-scale phishing attacks provide interesting research, the researcher is also interested in exploring the factors associated with what influences responses to spear phishing emails. Spear phishing is a focused phishing campaign that has more of a targeted approach such as a specific organization or group (Wang et al, 2012). As mentioned by Amin et al, 2012, those that are responsible for phishing attacks are not just after quick money but instead exercise patience in harvesting valuable information that can be used for bigger and better things.

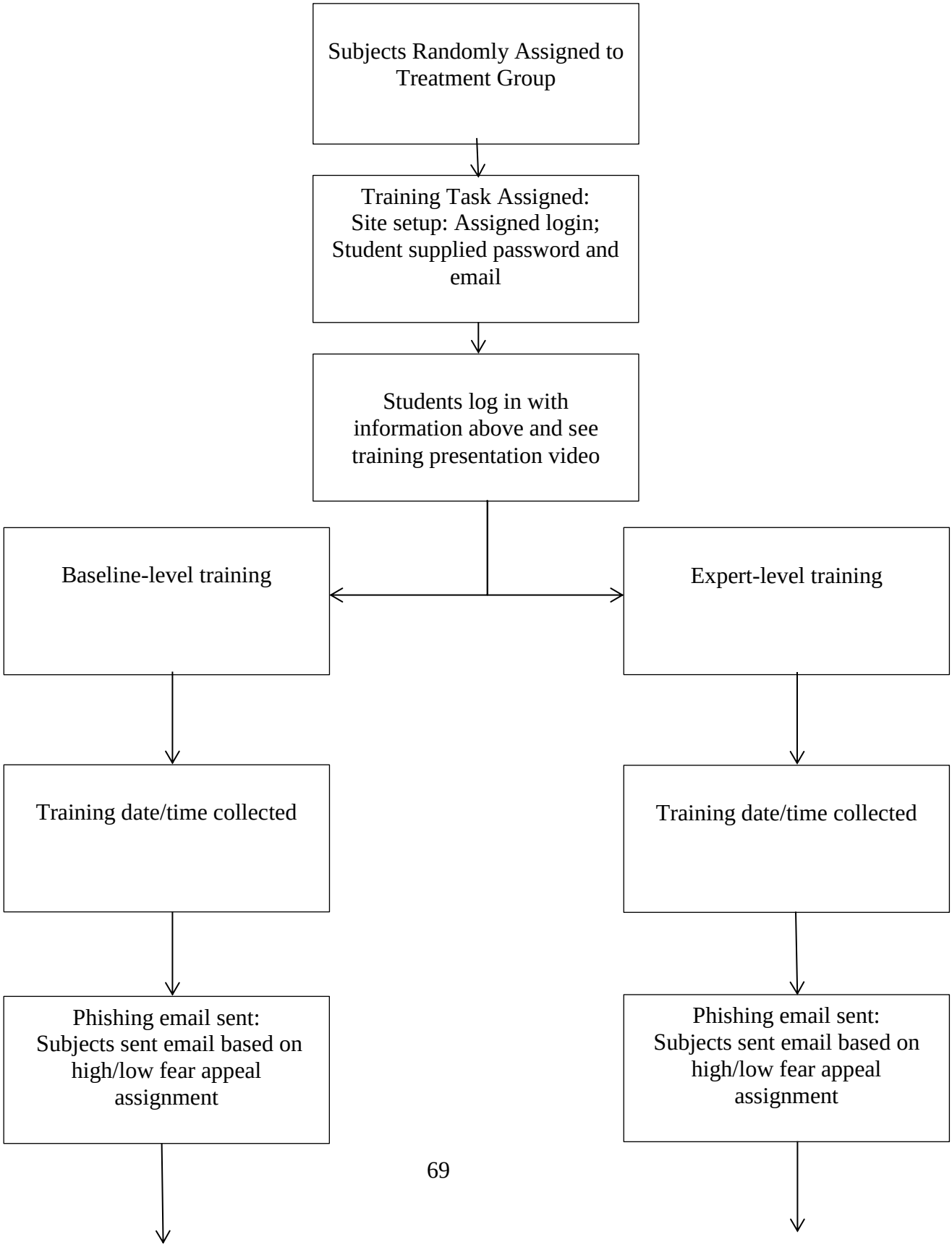
Additionally, research related to social engineering is also of future interest to the researcher. Those responsible for phishing attacks can use social engineering to gain access to photos, relationships, and other details that create the illusion of acquaintanceship (Crossman, 2012). Victims can receive files with malware that is unknowingly installed by downloading an attachment or even clicking on a link.

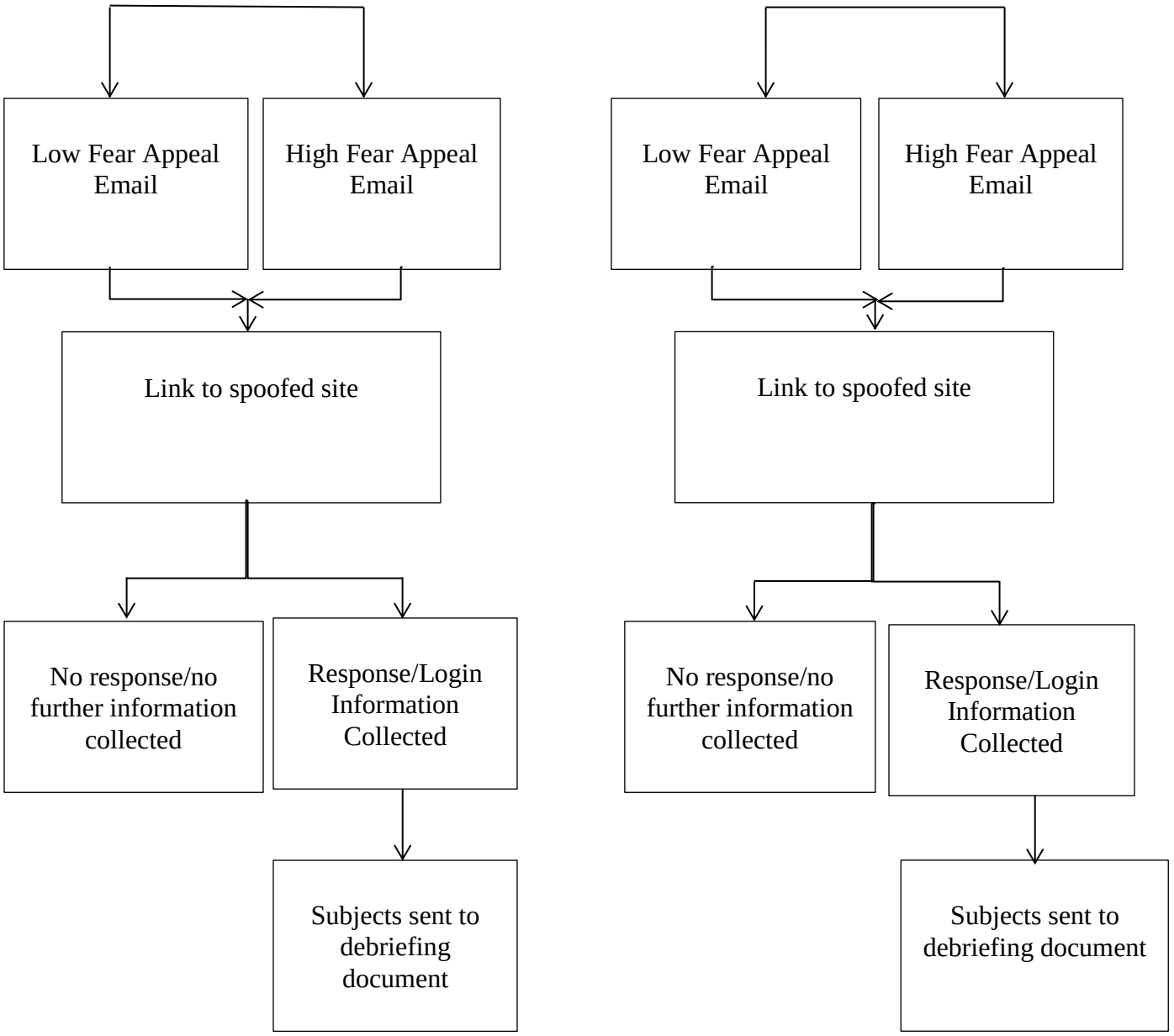
Prior experience, in addition to cultural influences, tend to have a heavy influence on a reaction to an adverse event (Furedi, 2006). As mentioned by Furedi (2006), this can cause a type of sensitization to problems. This can similarly be said for reactions to phishing attempts with those that are familiar with certain types of attempts more sensitized to the process.

This research looked at the behavioral response to phishing by sending individuals actual phishing communications and tracking whether or not information is provided. This information allowed researchers to gain further insight regarding the part that fear arousal related to providing login credentials and self-confidence play in response to phishing attacks. The brain is the safest place to store login credentials yet it is also something that has control over emotions, feelings and decisions which can lead to the unintentional divulgence of sensitive information to illegitimate sources. "Insecurity towards expected forms of behaviour and suspicion about the motives of others provide a fertile terrain where perceptions of threats can flourish" (Furedi, p.5). As researchers find out more information regarding the reasoning behind an unintentional divulgence, safeguarding tools can do a better job of keeping Internet users safe.

Appendix A

Flowchart of the Experiment


Subjects Randomly Assigned to Treatment Group
Training Task Assigned: Site setup: Assigned login; Student supplied password and email
Students log in with information above and see training presentation video
Baseline-level training
Expert-level training
Training date/time collected
Training date/time collected
Phishing email sent: Subjects sent email based on high/low fear appeal assignment
Phishing email sent: Subjects sent email based on high/low fear appeal assignment


Low Fear Appeal Email
High Fear Appeal Email
Link to spoofed site
No response/no further information collected
Response/Login Information Collected
Subjects sent to debriefing document
Low Fear Appeal Email
High Fear Appeal Email
Link to spoofed site
No response/no further information collected
Response/Login Information Collected
Subjects sent to debriefing document

Appendix B

Informed Consent Document

PRINCIPAL INVESTIGATOR

Deanna House, MS
Department of Information Systems and Operations Management
deanna.house@mavs.uta.edu
817-272-3584

FACULTY ADVISOR

Dr. MK Raja,
Department of Information Systems and Operations Management
raja@uta.edu
817-272-3540

TITLE OF PROJECT
Email Usage Behavior

INTRODUCTION
You are being asked to participate in a research study about email usage behaviors. Your participation is voluntary. Refusal to participate or discontinuing your participation at any time will involve no penalty or loss of benefits to which you are otherwise entitled. Please ask questions if there is anything you do not understand.

PURPOSE
The purpose of this research is to collect information regarding email usage behaviors.

DURATION
Participation in this research should take no more than 30 minutes of your time.

NUMBER OF PARTICIPANTS
The number of anticipated participants in this research study is 800.

PROCEDURES
You will be asked a series of questions related to email usage behaviors. The survey data will be collected electronically through an online survey system.

POSSIBLE BENEFITS
The major benefits you will receive from participation in this research are increased familiarity with behavioral science research methods and exposure to a specific research

problem area. The benefits to this investigator are increased understanding of email usage behaviors.

POSSIBLE RISKS/DISCOMFORTS

You might experience discomfort or fatigue during this research study. Possible discomforts experienced while filling out the questionnaire may include fatigue, boredom, or frustration. You have the right to quit any study procedures at any time at no consequence and may do so by informing the researcher.

COMPENSATION

Upon completion of the study, you will be entered to win 1 of 5 $25 Amazon Gift Cards.

ALTERNATIVE PROCEDURES

There are no alternative procedures offered for this study. However, you can elect not to participate in the study or quit at any time at no consequence.

VOLUNTARY PARTICIPATION

Participation in this research study is voluntary. You have the right to decline participation in any or all study procedures or quit at any time at no consequence. Should you choose not to complete all study procedures, you will still be eligible for the raffle for (5) $25 Amazon Gift Cards.

CONFIDENTIALITY

Every attempt will be made to see that your study results are kept confidential. A copy of this signed consent form and all data collected [including transcriptions/tapes if applicable] from this study will be stored in Dr. MK Raja's office, Room 522B for at least three (3) years after the end of this research. The results of this study may be published and/or presented at meetings without naming you as a participant. Additional research studies could evolve from the information you have provided, but your information will not be linked to you in anyway; it will be anonymous. Although your rights and privacy will be maintained, the Secretary of the Department of Health and Human Services, the UTA Institutional Review Board (IRB), and personnel particular to this research have access to the study records. Your records will be kept completely confidential according to current legal requirements. They will not be revealed unless required by law, or as noted above. The IRB at UTA has reviewed and approved this study and the information within this consent form. If in the unlikely event it becomes necessary for the Institutional Review Board to review your research records, the University of Texas at Arlington will protect the confidentiality of those records to the extent permitted by law.

CONTACT FOR QUESTIONS

Questions about this research study may be directed to Deanna House at deanna.house@mavs.uta.edu or Dr.MK Raja at raja@uta.edu. Any questions you may have about your rights as a research participant or a research-related injury may be directed to the Office of Research Administration; Regulatory Services at 817-272-2105 or regulatoryservices@uta.edu.

As a representative of this study, I have explained the purpose, the procedures, the benefits, and the risks that are involved in this research study:

_____

Signature and printed name of principal investigator or person obtaining consent
Date

CONSENT

By signing below, you confirm that you are 18 years of age or older and have read or had this document read to you. You have been informed about this study's purpose, procedures, possible benefits and risks, and you have received a copy of this form. You have been given the opportunity to ask questions before you sign, and you have been told that you can ask other questions at any time.

You voluntarily agree to participate in this study. By signing this form, you are not waiving any of your legal rights. Refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You may discontinue participation at any time without penalty or loss of benefits, to which you are otherwise entitled.

_____

SIGNATURE OF VOLUNTEER **DATE**

_____

EMAIL ADDRESS

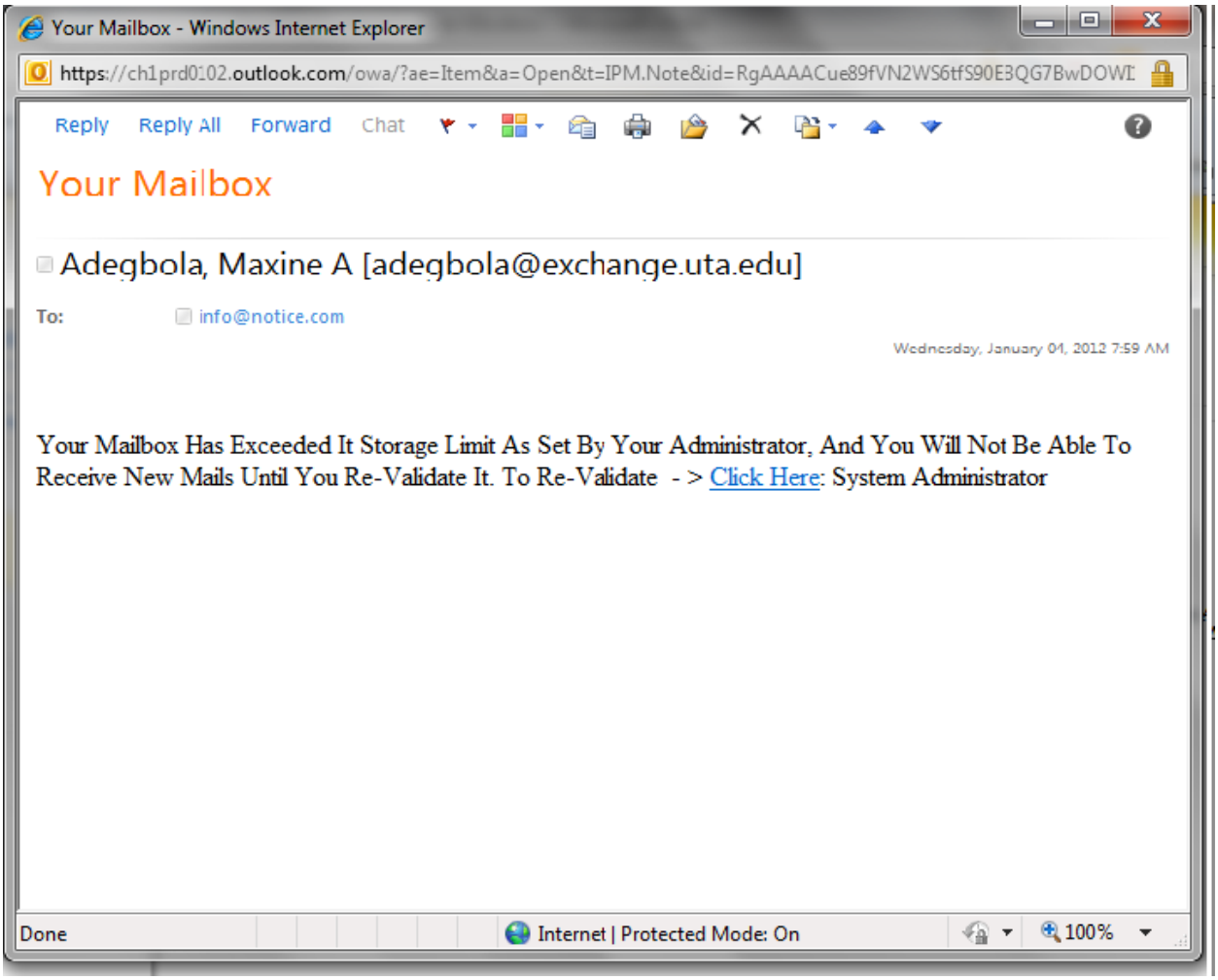
☐ If you prefer not to be contacted for future research opportunities, please check this box.

Appendix C

Survey Instrument

Survey Instrument

Please answer the following questions related to your judgment of emails such as this one.



(All scales are a 7-point Likert scale with 1= Strongly disagree and 7= Strongly agree unless otherwise noted).

Self-Efficacy (Adapted from Witte (1996) – Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale.

Instructions: Please read the following questions carefully and provide your response in relation to the email scenario above.

SE1: I am able to differentiate illegitimate emails from legitimate emails to prevent my login credentials from being compromised.

SE2: Differentiating illegitimate emails from legitimate emails is easy to do to prevent my login credentials from being compromised.

SE3: I am comfortable with my ability to differentiate illegitimate emails from legitimate emails to prevent my login credentials from being compromised.

Threat Severity:

Instructions: Please read the following questions carefully and provide your response in relation to the email scenario above.

~~TSE1: I believe that having my login credentials compromised is severe.~~*

TSE2: I believe that having my login credentials compromised is serious.

TSE3: I believe that having my login credentials compromised is significant.

Response Efficacy:

Instructions: Please read the following questions carefully and provide your response in relation to the email scenario above.

RE1: I can prevent my login credentials from being compromised by not clicking on links in emails.

RE2: . I can prevent my login credentials from being compromised by verifying the address of the sender.

RE3: . I can prevent my login credentials from being compromised by not providing sensitive information through links in emails.

Threat Susceptibility:

Instructions: Please read the following questions carefully and provide your response in relation to the email scenario above.

TSU1: My login credentials are at risk of being compromised.

TSU2: It is likely that my login credentials will be compromised.

TSU3: It is possible that my login credentials will be compromised.

Self-Confidence Items:

Instructions: Please read the following questions carefully and choose a response that best describes you.

(From Shrauger & Schohn, 1995)

CON1: I have more confidence in myself than most people I know.

CON2: When things are going poorly, I am usually confident that I can successfully deal with them.

~~CON3: I have fewer doubts about my abilities than most people.~~**

CON4: Much of the time I don't feel as competent as many of the people around me. *

CON5: I lack some important capabilities that may keep me from being successful .*

~~CON6: I often feel unsure of myself, even in situations I have successfully dealt with in the past.*~~**

~~CON 7: If I were more confident about myself, my life would be better. *~~**

*Reverse Scored

Intention to Respond:

Instructions: Please read the following questions carefully and provide your response in relation to the email scenario above.

INT1: I intend to provide my login credentials in the email scenario above.

INT2: I plan to provide my login credentials in the email scenario above.

Fear Arousal

Instructions: Please read the following questions carefully and provide your response in relation to the email scenario above.

Champion et al (2004)

FA1: The thought of providing my login credentials scares me.

FA2: When I think providing my login credentials, I feel nervous.

FA3: When I think about providing my login credentials, I get upset.

~~FA4: When I think about providing my login credentials, I get depressed.~~**

~~FA5: When I think about providing my login credentials, I get jittery.~~**

FA6: When I think about providing my login credentials, my heart beats faster.

FA7: When I think about providing my login credentials, I feel uneasy.

FA8: When I think about providing my login credentials, I feel anxious.

Message Involvement (from Vishwanath et al, 2011; Wang et al, 2012)

Instructions: Please provide the choice that best reflects your opinion regarding information in the above email scenario.

Did you think the information contained in the email was:

MI1: Insignificant…Significant

MI2: Unimportant…Important

MI3: Not Needed…Needed

MI4: Irrelevant to you…Relevant to you

MI5: Of no concern to you…Of concern to you

MI6: Doesn't matter to you…Matters to you

MI7: Means nothing to you…Means a lot to you

Web Experience (Wright & Marett, 2010)

Instructions: Please read the following questions carefully and provide a response related to the amount of time spent on web activities.

On average, how much time per week do you spend on each of the following web activities?

~~WX1: Reading news on the web?~~*

WX2: Reading and/or posting messages to social sites?

WX3: Accessing information on the Web about products and services you may buy?

WX4: Shopping (e.g., actually purchasing something) on the Web?

Instructions: Please answer the following questions related to demographic information. This information will not be used to identify individuals responses.

Age

AGE 1 __ 18 to 29

AGE2 __ 30 to 39

AGE3 __ 40 to 49

AGE4 __ 50 to 59

AGE5 __ 60 to 69

AGE6 __ 70 and over

Gender

GEN1__ Male

GEN2__ Female

Education

ED1__ High school

ED2__ Some college

ED3__ Bachelor's degree

ED4__ Master's degree

ED5__ Doctorate

ED6__ Other

**Items dropped

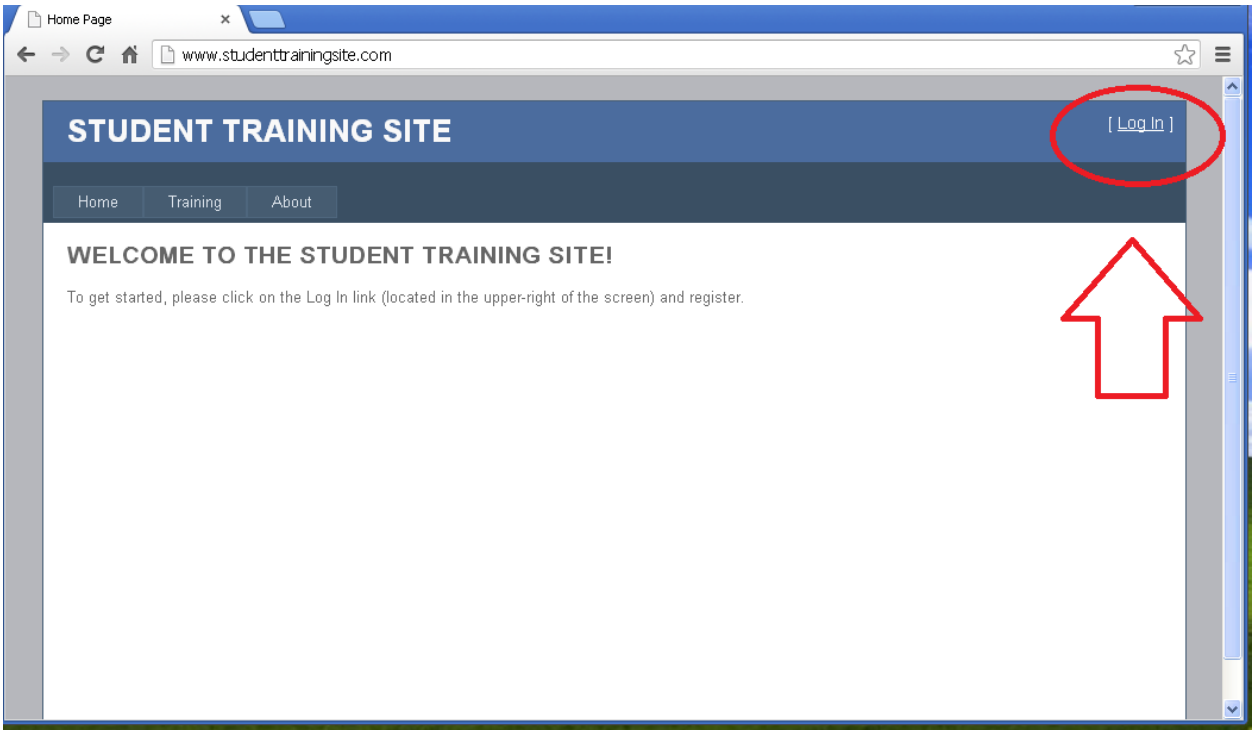
Appendix D

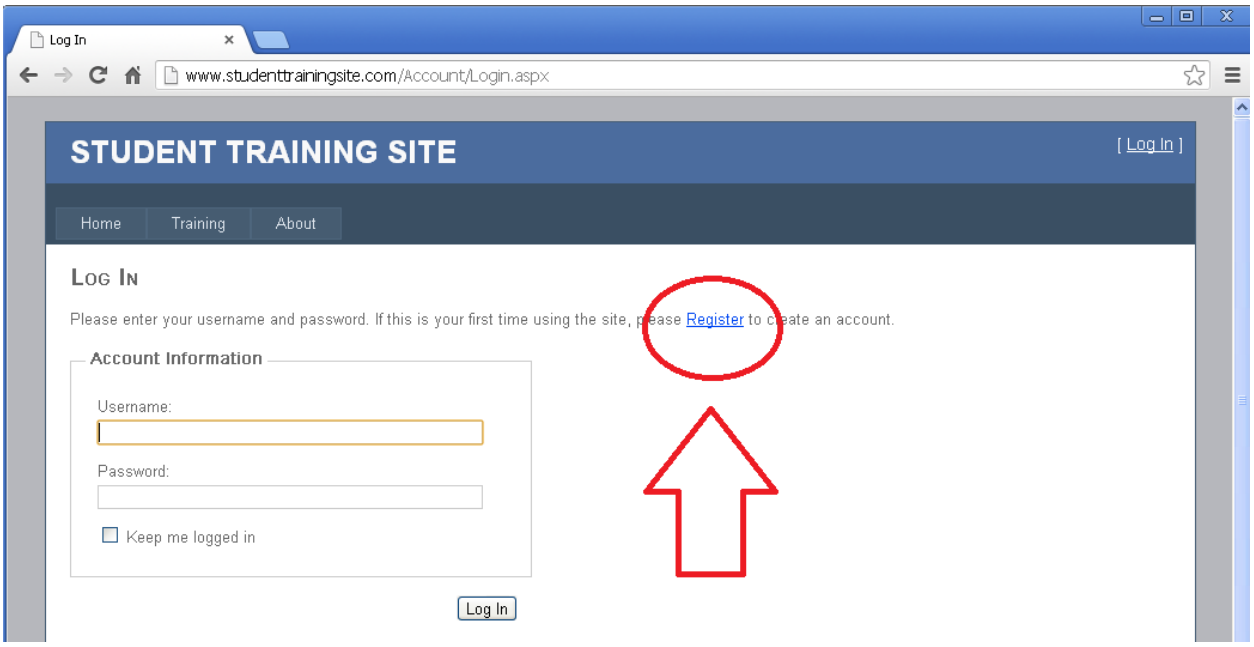
Training Materials

Training Materials

Please go to this site: to watch a short training video related to topics presented in class. **Please be aware that Mozilla Firefox and Opera do not support the video format. Please use an alternative browser.**

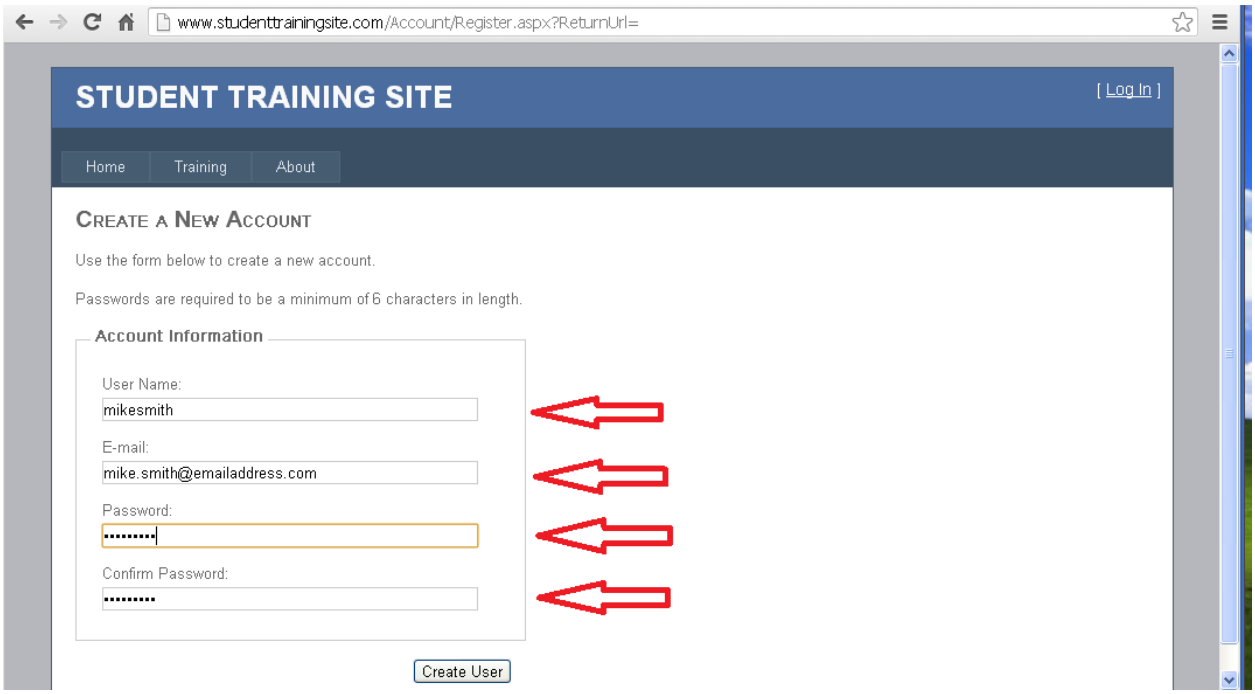
You will need to register for an account. To get started, click on the *Login* button located in the upper right hand corner of the screen. You will need to click on *"Register"* if this is your first time using the system.





Your *user name* is assigned to you and is your *first name* and *last name* combined (in Blackboard) with *no spaces or special characters*. For example if your name is Mike Smith, your username is mikesmith.

Please *create a password* and also provide a *current email address*.



After you create your account, you will be directed to the video. The entire process should take no more than 10 minutes.

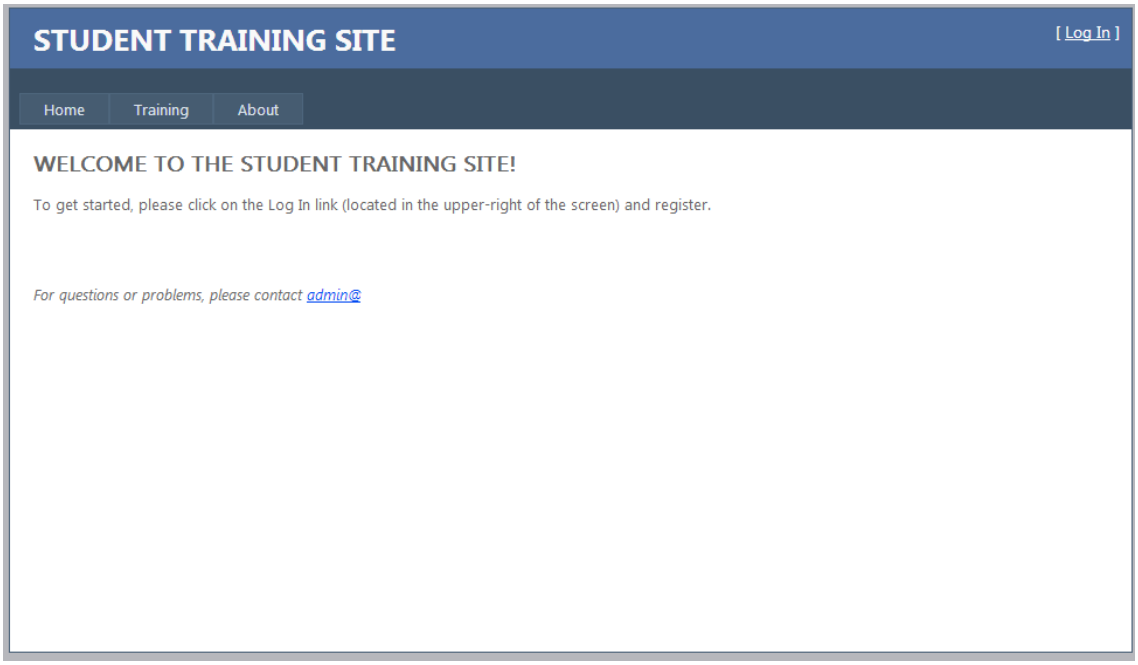
If you have any *problems* with the site, please email admin@.

If you need to *reset your password* at any time please email admin@ .

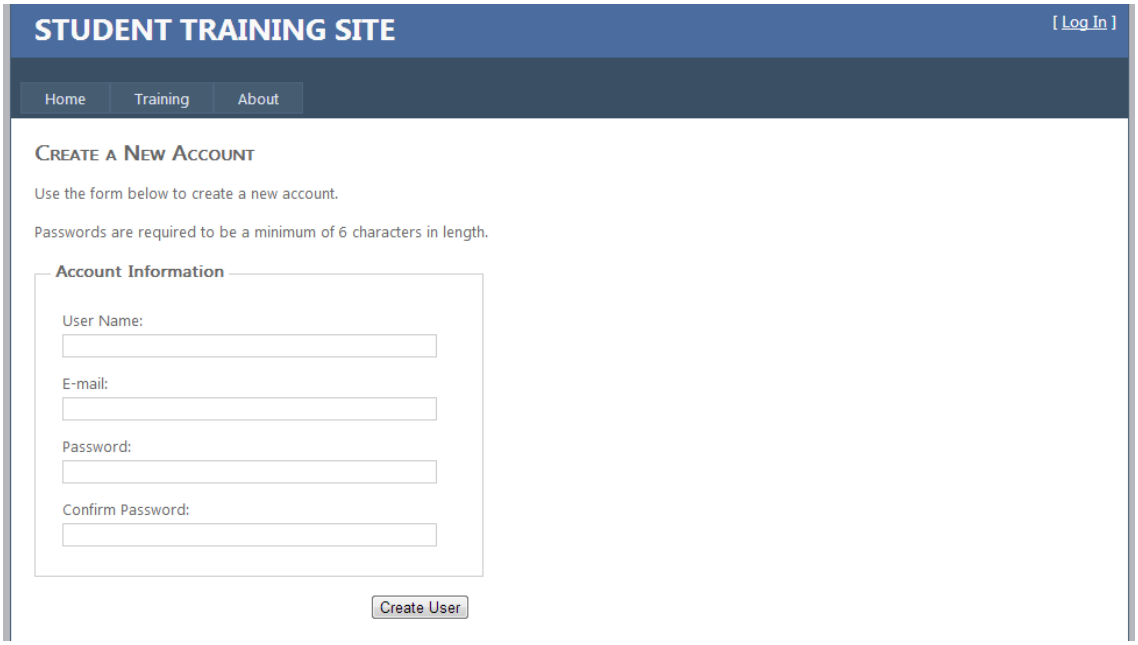
Appendix E

Student Training Site

Student Training Site



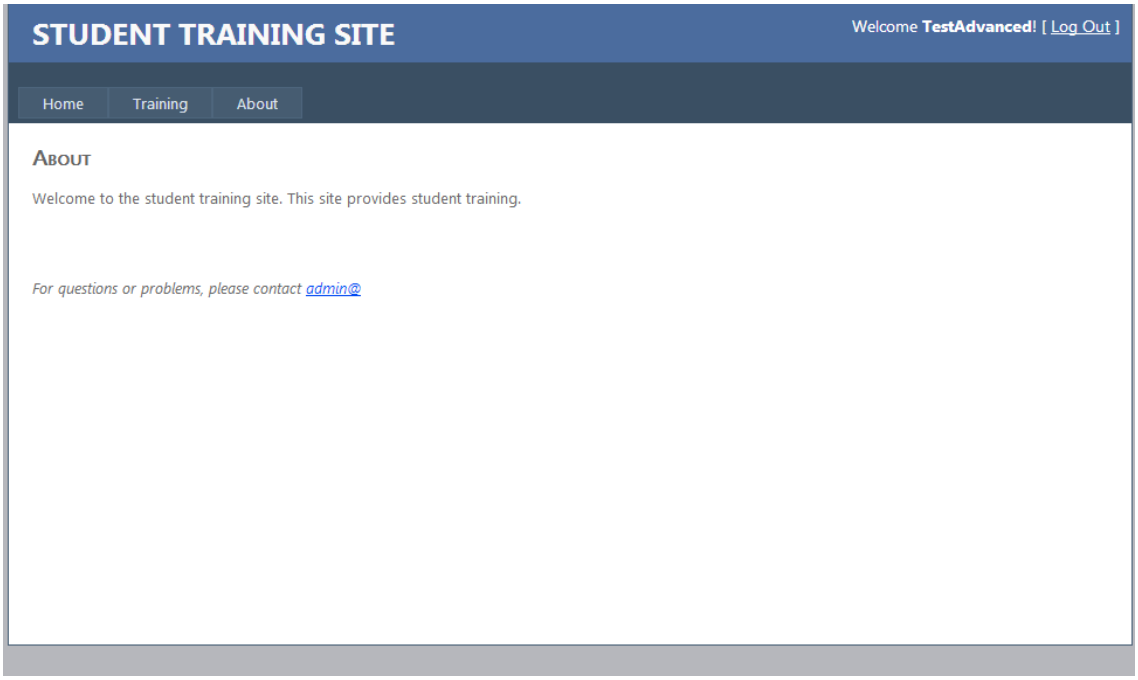
Welcome Screen



Registration Screen

Pre-assigned video treatment (Basic) upon login

Pre-assigned video treatment (Advanced) upon login


STUDENT TRAINING SITE
Welcome TestAdvanced! [Log Out]
Home
Training
About
About
Welcome to the student training site. This site provides student training.
For questions or problems, please contact admin@

"About" page

Appendix F

Training Video Content

Training Video Content

Basic Training:

What is Phishing?

Phishing is a sophisticated approach to password theft.

How Do Phishing Scams Work?

A hacker poses as a legitimate organization to persuade you to disclose confidential information.

Phishing scams require that you reply to an email message or click on an embedded website for the scam to unfold.

Phishing Disguises

A fake website can look similar to the real thing and can contain logos and other graphics copied from legitimate sites.

Hackers can obtain a website that is similar to one used by a legitimate company.

Avoiding Phishing Scams

Phishing emails request that you click on a link to verify information.

To avoid phishing scams avoid clicking on links in email messages.

Advanced Training:

What is Phishing?

Phishing is a sophisticated approach to password theft.

How Do Phishing Scams Work?

A hacker poses as a legitimate organization to persuade you to disclose confidential information.

Phishing scams require that you reply to an email message or click on an embedded website for the scam to unfold.

Cybercriminals use social engineering to convince you to hand over personal information under false pretenses.

Email is a common source of phishing communication.

Phishing Disguises

A fake website can look similar to the real thing and can contain logos and other graphics copied from legitimate sites.

Hackers can obtain a website that is similar to one used by a legitimate company.

Common Indicators of Phishing Communications (Source: http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx)

Use of threats to indicate your security has been compromised

Use of links in an email may lead to a website that is different than the one shown.

Fake emails that look legitimate (use of logos and graphics and fake web addresses)

Bad spelling/grammar

Avoiding Phishing Scams

Phishing emails request that you click on a link to verify information.

To protect yourself from phishing scams

Don’t click links in email messages

Type addresses directly into your browser or use your personal bookmarks

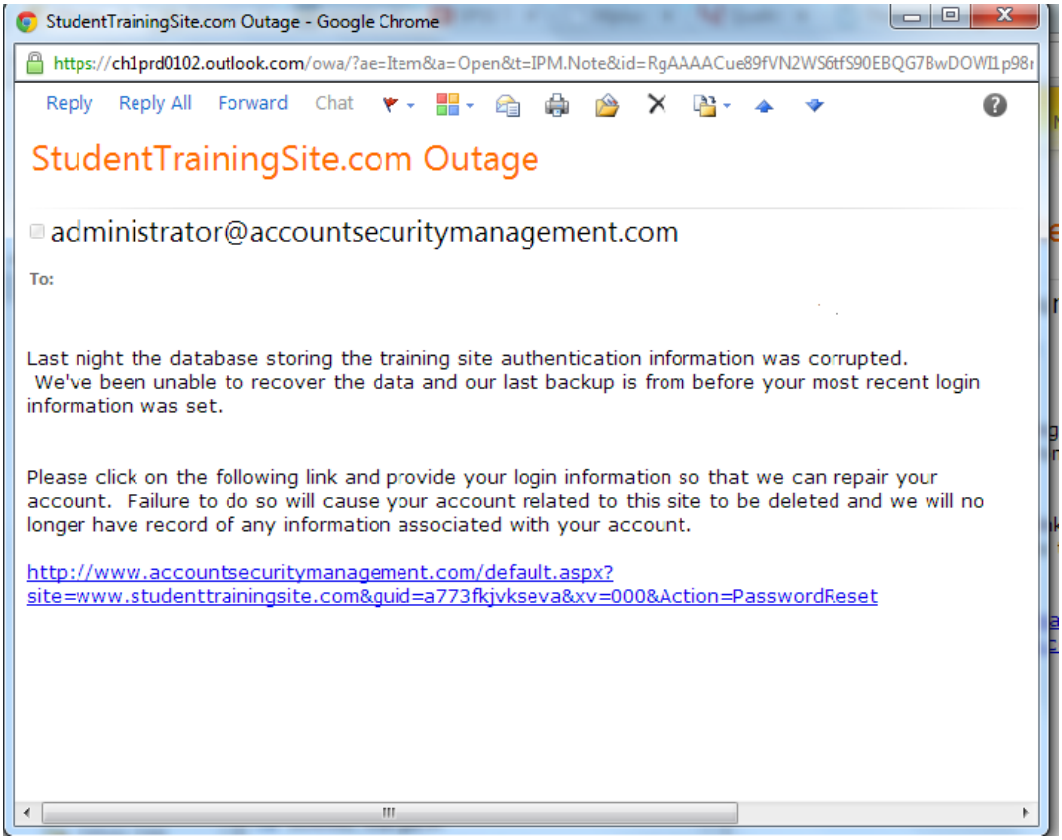
Check the sites security certificate before you enter personal or financial information into a website

Don’t enter personal or financial information into pop-up windows

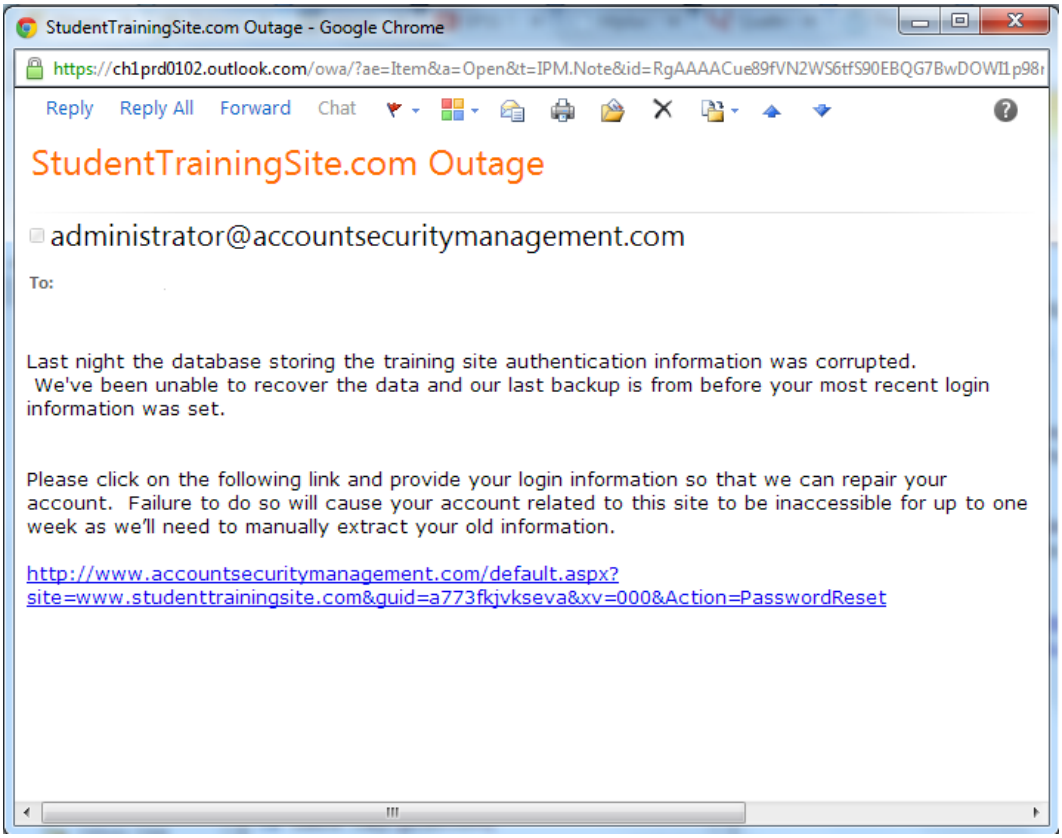
Keep your computer software current with the latest security updates.

Appendix G

Phishing Email Examples



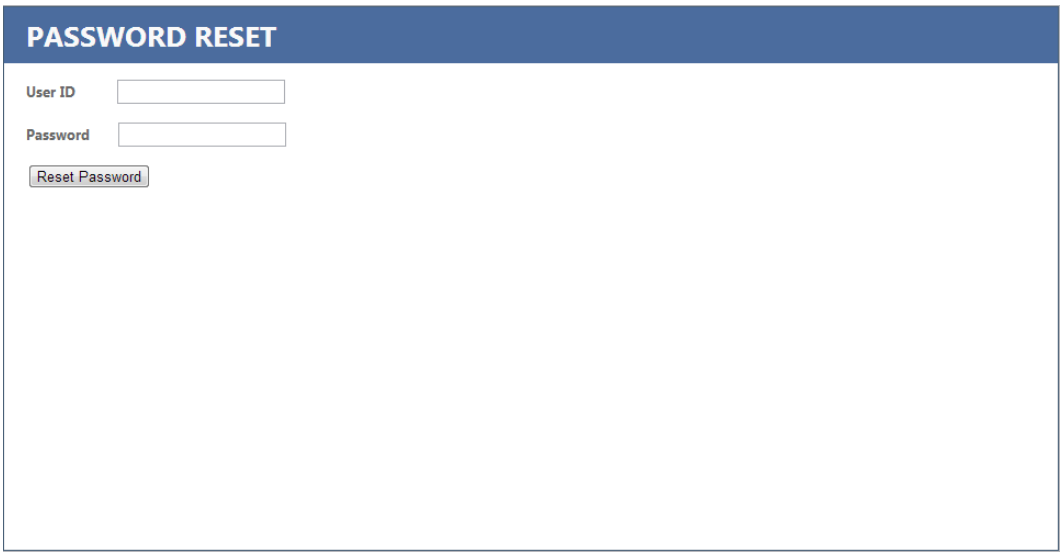
High Fear Email



Low Fear Email

Appendix H

Spoofed Training Site



Login Screen for Fraudulent Training Site

Appendix I

Debriefing Document

PRINCIPAL INVESTIGATOR: DEANNA HOUSE, deanna.house@mavs.uta.edu

TITLE OF PROJECT: EMAIL USAGE BEHAVIORS

This Debriefing Form will explain the purpose of this semester's experiment. It is important that you read this material carefully. Thank you for your participation in this study.

You recently participated in a research study titled, "Email Usage Behaviors" in which you were told would involve the following procedures: A survey link was emailed to you asking your opinion on various manners in which you keep your login information confidential. In addition to the data that was collected from the survey, the online training system that provided you with information related to phishing and the prevention on phishing attacks was also related to the study. More specifically, you were sent an email that indicated that your information had been lost and you needed to provide your login information so that it could be recovered. This was a simulated phishing email to determine whether or not you clicked on the link to provide information. The login information was not corrupted and you were not actually phished.

You participated in research related to phishing and how recipients of phishing emails react to threatening emails. The study was set up so that information could be collected related to phishing. This data is very important to help prevent future phishing attacks. Your class was chosen due to the course content related to phishing. Your submissions will allow the researchers to explore valuable information regarding the behavioral reactions individuals experience when faced with a phishing attack.

PROCEDURES:

The study was divided into two parts. The first part of the study involved data collected from the online survey that you completed related to email usage behaviors. You were sent a link via email and answered questions related to phishing. The second part of the study involved your response to a simulated phishing email. You were asked to participate in an assignment in which you received information specific to phishing. This information was distributed to you via the student training site. You submitted a login name, password, and email in order to

access the training materials. The login name was assigned to you and the password was stored in such a manner that the researcher could at no time access it. After you received that training, you may remember receiving an email from a site administrator indicating that your training login information had been corrupted. This was a simulated phishing email. Please be assured that no login or password information was stored in relation to this exercise. The only data that was collected was 1) did you click on the link and 2) did you click on the submit button. The simulated phishing email was sent to the email address that you provided upon initial setup. However, please be assured that this email information will not be used for any further purpose now that the study is over. In addition, any login data collected will be deleted now that the study is completed. The combination of both parts of the study will allow the researcher to obtain valuable information related to circumstances that make phishing attacks successful. This exercise provided you with hands-on training and experience with a simulated phishing attack. This study will impress upon you the importance of not providing sensitive information when clicking on links from emails and hopefully reduce your susceptibility to future attacks.

CONFIDENTIALITY:

We ask that you keep this information strictly confidential. Do not talk about this experiment, your feelings about participation, or the purposes of this research to anyone. The success and validity of scientific research depends on subjects being "blind" to the purpose of the experiment.

We appreciate your participation and confidentiality in helping us move behavioral science forward!

Your participation in this research study is completely voluntary. Now that you are aware of the true nature of the study, if you would prefer that your data not be used for the purposes of this research please discuss the situation and decision with the researcher, Deanna House at deanna.house@mavs.uta.edu or 817-272-3584. Please keep in mind that none of the data collected will identify you individually, you will remain anonymous.

References

Aguinis, H., Gottfredson, H.K., & Joo, H. (2013). Best Practice Recommendations for Defining, Identifying, & Handling Outliers. *Organizational Research Methods,* 16(2), 270 – 301.

Ajzen, I., & Fishbein, M. (2005). The Influence of Attitudes on Behavior. In Albarracín, D., Johnson,B.T., & Zanna, M.P. (Eds.), The Handbook of Attitudes. pg. 173-221. Mahwah, NJ: Erlbaum.

Alexander, P. (2009). Home and Small Business Guide to Protecting Your Computer Network, Electronic Assets, and Privacy. Westport, CT: Praeger.

Amin, R.M., Ryan, J.J.C.H., & Van Dorp, R. (2012). Detecting Targeted Malicious Email. *IEEE Security & Privacy,* 10(3), 64 – 71.

Anderson, A. (2013). Small Businesses: Targets of Deception. *Business Credit,*115(5), 48 – 52.

Anderson, C.L. & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly,* 34(3), 613 – 643.

Armerding, T. (2012). Paypal Phishing Scams Ramp up for Holidays. *CIO,* Retrieved from: http://www.csoonline.com/article/723379/paypal-phishing-scams-ramp-up-for-holidays.

Bagozzi, R.P., Gopinath, M., & Nyer, P.U. (1999). The Role of Emotions in Marketing. *Journal of the Academy of Marketing Science.* 27(2), 184 – 206.

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social Engineering: Assessing Vulnerabilities in Practice. *Information Management & Computer Security,* 17(1), 53 – 63.

Bandura, A. (1977a). Self-Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review,* 84(2), 191 – 215.

Bandura, A.(1977b). Social Learning Theory. Englewood Cliffs, NJ: Prentice-Hall, Inc.

Bandura, A. (1986). Social Foundations of Thought and Action: A Social Cognitive Theory. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1997). Self-Efficacy: The Exercise of Control. New York, NY: W.H. Freeman and Company.

Bandura, A., Adams, N.E., & Beyer, J. (1977). Cognitive Processes Mediating Behavioral Change. *Journal of Personality and Social Psychology,* 35(3), 125 – 139.

Beck, K.H. & Frankel, A. (1981). A Conceptualization of Threat Communications and Preventive Health Behavior. *Social Psychology Quarterly,* 44(3), 204 – 217.

Beck, L.K. & Lund, A.K. (1981). The Effects of Health Threat Seriousness and Personal Efficacy Upon Intentions and Behavior. *Journal of Applied Social Psychology,* 11(5), 401 – 415.

Beecroft, C. (2012). Prezi: A Gift for the Modern Information Professional! *Multimedia Information & Technology,* 38(1), 15 – 16.

Beresford, A.D. (2003). Foucault's Theory of Governance and the Deterrence of Internet Fraud. *Administration & Society,* 35(1), 82 – 103.

Block, L.G. & Keller, P.A. (1998). Beyond Protection Motivation: An Integrative Theory of Health Appeals. *Journal of Applied Social Psychology,* 28(17), 1584 – 1608.

Blommaert, J. & Omoniyi, T. (2006). Email Fraud: Language, Technology, and the Indexicals of Globalisation. *Social Semiotics,* 16(4), 573 – 605.

Boer, H. & Seydel, E.R. (1996). Protection Motivation Theory. In Connor, M. & Norman, P. (Eds.). Predicting Health Behaviour. pg. 95 – 120. Buckingham, U.K.: Open University Press.

Bocij, P. (2006). The Dark Side of the Internet: Protecting Yourself and Your Family From Online Criminals. Westport, CT: Praeger.

Brenner, S.W. (2010). Cybercrime: Criminal Threats from Cyberspace. Santa Barbara, CA: Praeger.

Briñol, P., Petty, R.E., & Barden, J. (2007). Happiness Versus Sadness as a Determinant of Thought Confidence in Persuasion: A Self-Validation Analysis. *Journal of Personality and Social Psychology,* 93(5), 711 – 727.

Briñol, P., Petty, R.E., & Rucker, D.D. (2006). The Role of Meta-Cognitive Processes in Emotional Intelligence. *Psichotema,* 18(1), 26 – 33.

Butler, R. A Framework of Anti-Phishing Measures Aimed at Protecting the Online Consumer's Identity. *The Electronic Library,* 25(5), 517 – 533.

Byrne, J.A. (2004). Why Courage? *Fast Company,* 86, 16.

Carver, C.S. & Blaney, P.H. (1977). Perceived Arousal, Focus of Attention, and Avoidance Behavior. *Journal of Abnormal Psychology,*86(2), 154 – 162.

Cauberghe, V., De Pelsmacker, P., Janssens, W., & Dens, N. (2009). Fear, Threat, and Efficacy in Threat Appeals: Message Involvement as a Key Mediator to Message Acceptance. *Accident Analysis and Prevention,* 41(), 276 – 285.

Cheah, W.H. (2006). Issue Involvement, Message Appeal, and Gonorrhea: Risk Perceptions in the US, England, Malaysia, and Singapore. *Asian Journal of Communication,* 16(3), 293 – 314.

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences,* Waikoloa, Hawaii, 1 – 10.

Chiluwa, I. (2009). The Discourse of Digital Deceptions and '419' Emails. *Discourse Studies,* 11(6), 635 – 660.

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. Hillsdale, NJ: Lawrence Erlbaum Associates, Publishers.

Confidence. (n.d.) In *Merriam-Webster Dictionary* online. Retrieved from http://www.merriam-webster.com/dictionary/confidence

Connor, M. & Norman, P. (1995). The Role of Social Cognition in Health Behaviours. In Connor, M. & Norman, P. (Eds.). Predicting Health Behaviour. pg. 1 – 22. Buckingham, U.K.: Open University Press.

Copes, H. & Vieraitis, L.M. (2009). Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes. *Criminal Justice Review,* 34(3), 329 – 349.

Cox, R.H., Martens, M.P., & Russell, W.D. (2003). Measuring Anxiety in Athletics: The Revised Competitive State Anxiety Inventory-2. *Journal of Sport & Exercise Psychology,* 25(4), 519 – 533.

Cramer, R.J., Neal, T.M.S., & Brodsky, S.L. (2009). Self-Efficacy and Confidence: Theoretical Distinctions and Implications for Trial Consultation. *Consulting Psychology Journal: Practice and Research,* 61(4), 319 – 334.

Crossman, P. (2012). Advanced Malware Threats on the Rise, Experts Warn. *American Banker,* 177(56), 7 – 12.

Das, E.H.H.J., de Wit, J.B.F., & Stroebe, W. (2003). Fear Appeals Motivate Acceptance of Action Recommendations: Evidence for a Positive Bias in the Processing of Persuasive Messages. *Personality and Social Psychology Bulletin,* 29(5), 650 – 664.

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.

De Hoog, N., Stroebe, W., & de Wit, J.B.F. (2007). The Impact of Vulnerability to and Severity of a Health Risk on Processing and Acceptance of Fear-Arousing Communications: A Meta-Analysis. *Review of General Psychology,* 11(3), 258 – 285.

Deem, D.L. (2000). Notes from the Field: Observations in Working with the forgotten Victims of Personal Financial Crimes. *Journal of Elder Abuse & Neglect,* 12(2), 33 – 48.

Dhamija, R., Tygar, J.D., & Hearst, M. (2006). Why Phishing Works. *Proceedings of CHI Conference on Human Factors in Computing Systems,* Montreal, Quebec, Canada, 581 – 590.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. Hoboken, NJ: John Wiley & Sons, Inc.

Dillard, J.P. (1994). Rethinking the Study of Fear-Appeals: An Emotional Perspective. *Communication Theory,* 4(4), 295 – 323.

Dinev, T. & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies. *Journal of the Association for Information Systems,* 7(2), 386 – 408.

Dodge, Jr., R.C., Carver, C., Ferguson, A.J. (2007). Phishing for User Security Awareness. *Computers & Security,* 26(1), 73 – 80.

Dong, X., Clark, J.A., & Jacob, J.L. (2010). Defending the Weakest Link: Phishing Websites Detection by Analysing User Behaviours. *Telecommunication Systems,* 45(2-3), 215 – 226.

Downs, J.S., Holbrook, M., & Cranor, L.F. (2007). Behavioral Response to Phishing Risk. *Proceedings of the Anti-Phishing Working Group 2nd Annual e-Crime Researchers Summit,* Pittsburgh, PA, 37 – 44.

Easttom, C. & Taylor, J. (2011). Computer Crime, Investigation, and the Law. Boston, MA: Course Technology.

Feltz, D.L. (1988). Self-Confidence and Sports Performance. *Exercise and Sport Sciences Reviews,* 16(1), 423 – 458.

Finn, P. & Jakobsson, M. (2007). Designing Ethical Phishing Experiments, *IEEE Technology and Society Magazine,* 26(1), 46 – 58.

Fishbein, M. & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley.

Fisher, J.D., & Fisher, W.A. (1992). Changing AIDS-Risk Behavior. *Psychological Bulletin,* 111(3), 455 – 474.

Floyd, D.L., Prentice-Dunn, S., & Rogers, R.W. A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology,* 30(2), 407 – 429.

Fornell, C. & Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research,* 18(1), 39 – 50.

Fry, R.B. & Prentice-Dunn, S. (2005). Effects of Coping Information and Value Afirmation on Responses to a Perceived Health Threat. *Health Communication,* 17(2), 133 – 147.

Furedi, F. (2006). Culture of Fear Revisited. London, UK: Continuum.

Furnell, S.M., Bryant, P., & Phippen, A.D. (2007). Assessing the Security Perceptions of Personal Internet Users. *Computers & Security,* 26(5), 410 – 417.

Gefen, D. & Straub, D. (2005). A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. *Communications of the Association for Information Systems,* 16, 91 – 109.

Giaquinto, S. & Spiridigliozzi, C. (2007). Possible Influences of Spiritual and Religious Beliefs on Hypertension. *Clinical and Experimental Hypertension,* 29(7), 457 – 464.

Gies, L. (2008). How Material Are Cyberbodies? Broadband Internet and Embodied Subjectivity. *Crime Media Culture,* 4(3), 311 – 330.

Gigerenzer, G., Hoffrage, U., & Kleinbolting, H. (1991). Probabilistic Mental Models: A Brunswikian Theory of Confidence. *Psychological Review,* 98(4), 506 – 528.

Gollwitzer, P.M. (1993). Goal Achievement: The Role of Intentions. In Stroebe, W. & Hewstone, M. (Eds.), European Review of Social Psychology. Vol. 4 (pg. 141 – 185). Chichester, UK: Wiley.

Gotz, O., Liehr-Gobbers, K., & Krafft, M. (2007). Evaluation of Structural Equation Models Using Partial Least Squares (PLS) Approach. In Handbook of Partial Least Squares. (691 – 711). Berlin: Springer-Verlag.

Grabner-Krauter, S. & Faullant, R. (2008). Consumer Acceptance of Internet Banking: The Influence of Internet Trust. *International Journal of Bank Marketing,* 26(7), 483 – 504.

Green, E.C. & Witte, K. (2006). Can Fear Arousal in Public Health Campaigns Contribute to the Decline of HIV Prevalence? *Journal of Health Communication,* 11(3), 245 – 259.

Griffin, D. & Brenner, L. (2004). Perspectives on Probability Judgment Calibration. In D.J. Koehler & N. Harvey (Eds) Blackwell Handbook of Judgment and Decision Making. (177 – 198). Malden, MA: Blackwell.

Gu, G., Perdisci, R., Zhang, J., & Lee, W. (2008). BotMiner: Clustering Analysis of Network Traffic for Protocol and Structure-Independent Botnet Detection. Paper presented at USENIX Security '08, San Jose, CA. Retrieved July 1, 2013 from www.usenix.org.

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). Multivariate Data Analysis. Upper Saddle River, NJ: Prentice Hall, Inc.

Hallam-Baker, P. (2008). The DotCrime Manifesto: How to Stop Internet Crime. Boston, MA: Pearson Education, Inc.

Herzberg, A. & Margulies, R. (2011). Training Johnny to Authenticate (Safely). *IEEE Security & Privacy,* 10(1), 37 – 45.

Higbee, K.L. (1969). Fifteen Years of Fear Arousal: Research on Threat Appeals: 1953 – 1968. *Psychological Bulletin,* 72(6), 426 – 444.

Hodgson, P.W. (2005). The Threat to Identify From New and Unknown Malware. *BT Technology Journal,* 23(4), 107 – 112.

Hoffrage, U. (2004). Overconfidence. In R.F. Pohl (Ed.), Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgment, and Memory. (235 – 254). Hove, England: Psychology Press.

Hollenbeck, G.P. & Hall, D.T. (2004). Self-confidence and Leader Performance. *Organizational Dynamics,* 33(3), 254 – 269.

Hovland, C.I., Janis,I.L, & Kelley, G.H. (1953). Communication and Persuasion. New Haven, CT: Yale University Press.

Hutton, D.G. & Baumeister, R.F. (1992). Self-Awareness and Attitude Change: Seeing Oneself on the Central Route to Persuasion. *Personality and Social Psychology Bulletin,* 18(1), 68 – 75.

Jakobsson, M. (2005). Modeling and Preventing Phishing Attacks. Panel in *Financial Cryptography '05*. 2005. Retrieved online January 27, 1998 from http://www.informatics.indiana.edu/markus/papers/phishing_jakobsson.pdf.

Jakobsson, M. & Myers, S. (2007). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Hoboken, New Jersey: John Wiley & Sons, Inc.

Janis, I.L. (1967). Effects of Fear Arousal on Attitudinal Change: Recent Developments in Theory and Experimental Research. In Berkowitz, L. (Ed). Advances in Experimental Social Psychology (Vol. 3). (166 – 225). New York, New York: Academic Press.

Janis, I.L. & Feshbach, S. (1953). Effects of Fear-Arousing Communications, *Journal of Abnormal Psychology,* 48(1), 78 – 92.

Johnston, A.C. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly,* 34(3), 549 – 566.

Kahneman, D. (2011). Thinking, Fast and Slow. New York, NY: Farrar, Straus, and Giroux.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.M., Paxson, V., & Savage, S. (2008). Spamalytics: An Empirical Analysis of Spam Marketing Conversion. *Proceedings of the 15th ACM Conference on Computer and Communications Security (ACM CCS),* Alexandria, VA, 3 – 14.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.M., Paxson, V., & Savage, S. (2009). Spamalytics: An Empirical Analysis of Spam Marketing Conversion. *Communications of the ACM,* 52(9), 99 – 107.

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

Klein, W.M.P., Harris, P.R., Ferrer, R.A., & Zajac, L.E. (2011). Feelings of Vulnerability in Response to Threatening Messages: Effects of Self-Affirmation. *Journal of Experimental Social Psychology,* 47(6), 1237 – 1242.

Koriat, A. (2011). Subjective Confidence in Perceptual Judgments: A Test of the Self-Consistency Model. *Journal of Experimental Psychology: General,* 140(1), 117 – 139.

Kritzinger, E. & von Solms, S.H. (2010). Cyber Security for Home Users: A New Way of Protection Through Awareness Enforcement. *Computers & Security,* 29(8), 840 – 847.

Kruck, G.P. & Kruck, S.E. (2006). Spoofing – A Look at an Evolving Threat. *Journal of Computer Information Systems,* Fall, 95 – 100.

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.

Kutner, M.H., Nachtsheim, C.J., Neter, J., & Li, W. (2005). Applied Linear Statistical Models. Boston, MA: McGraw-Hill/Irwin.

Kuttschreuter, M., Gutteling, J.M. (2004). Experience-Based Processing of Risk Information: The Case of the Millennium Bug. *Journal of Risk Research,* 7(1), 3 – 16.

Lam, J.C.Y. & Lee, M.K.O. (2006). Digital Inclusiveness – Longitudinal Study of Internet Adoption by Older Adults. *Journal of Management of Information Systems,* 22(4), 177 – 206.

LaRose, R., Rifon, N.J., & Enbody, R. (2008). Promoting Personal Responsibility for Internet Safety. *Communications of the ACM,* 51(3), 71 – 76.

Lazarus, R.S. (1966). Psychological Stress and the Coping Process. New York, New York: McGraw-Hill Book Company.

Lazarus, R.S. (1999). Stress and Emotion: A New Synthesis. New York, New York: Springer Publishing Company.

Lazarus, R.S. & Folkman, S. (1984). Stress, Appraisal, and Coping. New York, New York: Springer Publishing Company.

Lee, Y. (2011). Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective. *Decision Support Systems,* 50(2), 361 – 369.

Lehrer, J. (2009). How We Decide. New York, New York: Houghton Mifflin Harcourt.

Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications. In Berkowitz, L. (Ed). Advances in Experimental Social Psychology (Vol. 5). New York, New York: Wiley.

Lewis, I.M., Watson, B., White, K.M, & Tay, R. (2007). Promoting Public Health Messages: Should We Move Beyond Fear-Evoking Appeals in Road Safety? *Qualitative Health Research,* 17(1), 61 – 74.

Liang, H. & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly,* 33(1), 71 – 90.

Lichtenstein, S., Fischhoff, B., & Phillips, L.D. (1982). Calibration of Probabilities: The State of the Art to 1980. In D. Kahneman, P., P.Slovic, & A. Tversky (Eds.)

Judgment Under Uncertainty: Heuristics and Biases. (pg. 306 – 334.). New York, NY: Cambridge University Press.

Lieberman, M.D. (2000). Intuition: A Social Cognitive Neuroscience Approach. *Psychological Bulletin,* 126, 109-137.

Lipka, M. (February 22, 2012). Rise in Identity Fraud Tied to Smartphone Use. *Reuters.* Retrieved from http://www.reuters.com/article/2012/02/22/us-idtheft-javelin-idUSTRE81L16520120222 on March 14, 2012.

Loibl, C., Cho, S.H., Diekmann, F., Batte, M.T. (2009). Consumer Self-Confidence in Searching for Information. *Journal of Consumer Affairs,* 43(1), 26 – 55.

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.

Marks, I. & Tobeña, A. (1990). Learning and Unlearning Fear: A Clinical and Evolutionary Perspective. *Neuroscience & Biobehavioral Review,* 14(4), 365 – 384.

McMath, B.F. & Prentice-Dunn, S. (2005). Protection Motivation Theory and Skin Cancer Risk: The Role of Individual Differences in Responses to Persuasive Appeals. *Journal of Applied Social Psychology,* 35(3), 621 – 635.

Milne, G.R., Labrecque, L.I. & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *The Journal of Consumer Affairs,* 43(3), 449 – 473.

Monahan, T. (2009). Identity Theft Vulnerability: Neoliberal Governance Through Crime Construction. *Theoretical Criminology,* 13(2), 155 – 176.

Moore, T. & Clayton, R. (2007). Examining the Impact of Website Take-down on Phishing. *Proceedings of the Anti-Phishing Working Group 2nd Annual e-Crime Researchers Summit,* Pittsburgh, PA, 1 - 13.

Moray, N., Inagaki, T., & Itoh, M. (2000). Adaptive Automation, Trust, and Self-Confidence in Fault Management of Time-Critical Tasks. *Journal of Experimental Psychology: Applied,* 6(1), 44 – 58.

Moser, S., Bruppacher, S.E., Mosler, H.J. (2011). How People Perceive and Will Cope with Risks from the Diffusion of Ubiquitous Information and Communication Technologies. *31(5),* 832 – 846.

Mulilis, J.P. & Duval, T.S. (2003). Activating Effects of Resources Relative to Threat and Responsibility in Person-to-Relative to Event Theory of Coping with Threat: An Educational Application. *Journal of Applied Social Psychology,* 33(7), 1437 – 1456.

Munoz, Y., Chebat, J.C., & Suissa,J.A. (2010). Using Fear Appeals in Warning Labels to Promote Responsible Gambling Among VLT Players: The Key Role of Depth of Information Processing. *Journal of Gambling Studies,* 26(4), 593 – 609.

Murphy, S. & Bennett, P. (2004). Health Psychology and Public Health: Theoretical Possibilities. *Journal of Health Psychology,* 9(1), 13 – 27.

Nash, J.R. (1976). Hustlers and Con Men: An Anecdotal History of the Confidence Man and His Games. New York, NY: M. Evans and Company, Inc.

National Research Council. (1994). Learning, Remembering, Believing: Enhancing Human Performance. Washington, D.C.: The National Academies Press.

Neuman, Y. & Levi, M. (2003). Blood and Chocolate: A Rhetorical Approach to Fear Appeal. *Journal of Language and Social Psychology,* 22(1), 22 – 29.

Nunnally, J.C. (1978). Psychometric Theory. New York, NY: McGraw-Hill.

Paine, C., Reips, U.D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'. *International Journal of Human-Computer Studies,* 65(6), 526 – 536.

Petty, R.E. & Cacioppo, J.T. (1990). Involvement and Persuasion: Tradition Versus Integration. *Psychological Bulletin,* 107(3), 367 – 374.

Pinsker, D.M., McFarland, K., & Pachana, N.A. (2010). Exploitation in Older Adults: Social Vulnerability and Personal Competence Factors. *Journal of Applied Gerontology,* 29(6), 740 – 761.

Piper, P.S. (2007). Phish Pharming. *Searcher: The Magazine for Database Professionals,* 15(9), 40 – 47.

Plotnikoff, R.C., Rhodes, R.E., Trinh, L. (2009). Protection Motivation Theory and Physical Activity: A Longitudinal Test Among a Representative Population Sample of Canadian Adults. *Journal of Health Psychology,* 14(8), 1119 – 1134.

Png, I.P.L.& Wang, Q.H. (2009). Information Security: Facilitating User Precautions Vis-à-vis Enforcement Against Attackers. *Journal of Management Information Systems,* 26(2), 97 – 121.

Pratt, T.C., Holtfreter, K., & Reisig, M.D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency,* 47(3), 267 – 296.

Prentice-Dunn, S. & Rogers, R.W. (1986). Protection Motivation Theory and Preventive Health: Beyond the Health Belief Model. *Health Education Research,* 1(3), 153 – 161.

Puhakainen, P. & Siponen, Mikko. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly,* 34(4), 757 – 778.

Rachman, S.J. (1978). Fear and Courage. San Francisco, CA: W.H. Freeman and Company.

Ramamoorti, S. (2008). The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula. *Issues in Accounting Education,* 23(4), 521 – 533.

Regan, T. (2010). "Phishing" Can Fool Even Experts. In Kiesbye, S. (Ed.) Does the Internet Increase Crime? 50 – 53. Farmington Mills, MI: Greenhaven Press.

Ringle, C.M., Wende, S., & Will, A. (2005). SmartPLS 2.0 (beta). www.smartpls.de. Hamburg: SmartPLS.

Rippetoe, P.A. & Rogers, R.W. (1987). Effects of Components of Protection Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat, *Journal of Personality and Social Psychology,* 52(3), 596 – 604.

Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology,* 91(1), 93 – 114.

Rogers, R.W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In Cacioppo, J. & Petty, R. (Eds.) Social Psychophysiology: A Sourcebook. 153 – 176. New York, New York: Guilford.

Rogers, R.W. & Mewborn, C.R. (1976). Fear Appeals and Attitude Change: Effects of a Threat's Noxiousness, Probability of Occurrence, and the Efficacy of Coping Responses. *Journal of Personality and Social Psychology,* 34(1), 54 – 61.

Roskos-Ewoldsen, D.R., Yu, H.J., & Rhodes, N. (2004). Fear Appeal Messages Affect Accessibility of Attitudes Toward the Threat and Adaptive Behaviors. *Communications Monographs,* 71(1), 49 – 69.

Sagarin, B.J., Cialdini, R.B., Rice, W.E., & Serna, S.B. (2002). Dispelling the Illusion of Invulnerability: The Motivations and Mechanisms of Resistance to Persuasion. *Journal of Personality and Social Psychology,* 83(3), 526 – 541.

Sarel, D. & Marmorstein, H. (2006). Addressing Consumers' Concerns About Online Security: A Conceptual and Empirical Analysis of Banks' Actions. *Journal of Financial Services Marketing,* 11(2), 99 – 115.

Sayago, S. & Blat, Josep. (2010). Telling the Story of Older People E-mailing: An Ethnographical Study. *International Journal of Human-Computer Studies,* 68(1-2), 105 – 120.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of CHI Conference on Human Factors in Computing Systems,* Atlanta, GA, 373 – 382.

Shrauger, J.S. (1972). Self-Esteem and Reactions to Being Observed by Others. *Journal of Personality and Social Psychology,* 23(2), 192 – 200.

Simons-Morton, B.G., Hartos, J.L., Leaf, W.A., & Preusser, D.F. (2006). Increasing Parental Limits on Novice Young Drivers: Cognitive Mediation of the Effect of Persuasive Messages. *Journal of Adolescent Research,* 21(1), 83 – 105.

Sinclair, R.C., Gershon, R.R.M., Murphy, L.R., & Goldenhar, L.M. (1996). Operationalizing Theoretical Constructs in Bloodborne Pathogens Training, *Health Education Behavior,* 23(2), 238 – 255.

Slavin, S., Batrouney, C. Murphy, D. (2007). Fear Appeals and Treatment Side-Effects: An Effective Combination for HIV Prevention? *AIDS Care,* 19(1), 130 – 137.

Solomon, M.G. & Chapple, M. (2005). Information Security Illuminated. Sudbury, MA: Jones and Bartlett Publishers.

Spence, H.E. & Moinpur, R. (1972). Fear Appeals in Marketing – A Social Perspective. *Journal of Marketing,* 36(3), 39 – 43.

Stajano, F. & Wilson, P. (2011). Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM,* 54(3), 70 – 75.

Stamatellos, G. (2007). Computer Ethics: A Global Perspective. Mississauga, Ontario: Jones and Bartlett Publishers Canada.

Stuteville, J.R. (1970). Psychic Defenses Against High Fear Appeals: A Key Marketing Variable. *Journal of Marketing,* 34(2), 39 – 45.

Tanner, Jr. J.F., Hunt, J.B., & Eppright, D.R. (1991). The Protection Motivation Model: A Normative Model of Fear Appeals. *Journal of Marketing,* 55(3), 36 – 45.

Taylor, J. (1987). Predicting Athletic Performance with Self-Confidence Somantic and Cognitive Anxiety as a Function of Motor and Physiological Requirements in Six Sports. *Journal of Personality,* 55(1), 139 – 153.

Thaler, R.H. & Sunstein, C.R. (2008). Nudge: Improving Decisions About Wealth, and Happiness. New Haven, CT: Yale University Press.

Tiedens, L.Z. & Linton, S. (2001). Judgment Under Emotional Certainty and Uncertainty: The Effects of Specific Emotions on Information Processing. *Journal of Personality and Social Psychology,* 81(6), 973 – 988.

Titus, R.M., Heinzelmann, F., & Boyle, J.M. (1995). Victimization of Persons by Fraud. *Crime Delinquency,* 41(1), 54 – 72.

Triandis, H.C. (1977). Interpersonal Behavior. Monterey, CA: Brooks/Cole.

Van Wyk, J. & Mason, K.A. (2001). Investigating Vulnerability and Reporting Behavior for Consumer Fraud Victimization: Opportunity as a Social Aspect of Age. *Journal of Contemporary Criminal Justice,* 17(4), 328 – 345.

Vancouver, J.B., Thompson, C.M., Tischner, E.C., & Putka, D.J. (2002). Two Studies Examining the Negative Effect of Self-Efficacy on Performance. *Journal of Applied Psychology,* 87(3), 506 – 516.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, R. (2011). Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability Within an Integrated, Information Processing Model. *Decision Support Systems,* 51(3), 576 – 586.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao,H.R. (2012). Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication,* 55(4), 345-362.

Watson, D. & Clark, L.A. (1994). The PANAS-X Manual for the Positive and Negative Affect Schedule – Expanded Form. Unpublished Manuscript.

Website: www.internetworldstats.com retrieved June 1, 2011.

Weisman, S. (2008). The Truth About Avoiding Scams. Upper Saddle River: FT Press.

White, M.D. & Fisher, C. (2008). Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. *Criminal Justice Policy Review,* 19(1), 3 – 21.

Witte, K. (1991-1992). The Role of Thr eat and Efficacy in Aids Prevention. *International Quarterly of Community Health Education,* 12(3), 225 – 249.

Witte, K. (1992). Putting the Fear Back Into Fear Appeals: The Extended Parallel Process odel. *Communication Monographs,* 59(4), 329 – 349.

Witte, K.(1994). Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM). *Communication Monographs,* 61(2), 113 – 134.

Witte, K. (1998). Fear as Motivator, Fear as Inhibitor: Using the EPPM to Explain Fear Appeal Successes and Failures. In Anderson, P.A. & Guerrero, L.K. (Eds.). 425-450. The Handbook of Communication and Emotion. New York, NY: Academic Press.

Witte, K. & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health Education & Behavior,* 27(5), 591 – 615.

Witte, K., Cameron,K.A., McKeon, J.K., & Berkowitz, J.M. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communication,* 1(4), 317 – 341.

Wood, R. & Bandura, A. (1989). Social Cognitive Theory of Organizational Management.*Academy of Management Review,* 14(3), 361 – 384.

Workman, M., Bommer, W.H., Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior,* 24(6), 2799 – 2816.

Wright, R.T. & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management of Information Systems,* 27(1), 272 – 303.

Wurtele, S.K.& Maddux, J.E. (1987). Relative Contributions of Protection Motivation Theory Components in Predicting Exercise Intentions and Behavior. *Health Psychology,* 6(5), 453 – 466.

Yerkes, R.M. & Dodson, J.D. (1908). The Relation of Strength of Stimulus to Rapidity of Habit-Formation. *Journal of Comparative Neurology & Psychology,* 18(5), 459 – 482.

Zhang, L. & McDowell, W. (2009). Modeling Online Passwords Protection Intention. *AMCIS 2009 Proceedings,* Paper 339.

Zulkosky, K. (2009). Self-Efficacy: A Concept Analysis. *Nursing Forum,* 44(2), 93 – 102.

Biographical Information

Deanna House received her PhD in Information Systems from the University of Texas at Arlington. She holds a Master's degree in Management of Information Systems from the University of Nebraska at Omaha and a Bachelor's degree in Human Resources from Bellevue University. Her current research interests are related to: influences of individual's responses to phishing attacks; global software implementations, and change management. She has published in *The International Journal of Business and Social Research* in addition to proceedings in the *Decision Sciences Institute* and the *Southwest Academy of Management.* She has accepted a position as an Assistant Professor at Ohio University and will begin in the fall.