9-23-2019

Phishing: message appraisal and the exploration of fear and self-confidence

Deanna House
University of Nebraska at Omaha

M. K. Raja

Phishing: message appraisal and the exploration of fear and self-confidence

Deanna House (Center for Ethics, University of Tampa, Tampa, FL, USA; Information and Technology Management, University of Tampa, Tampa, FL, USA) and M. K. Raja (Information Systems, University of Texas, Arlington, TX, USA)

ABSTRACT

Phishing attacks have threatened the security of both home users and organisations in recent years. Phishing uses social engineering to fraudulently obtain information that is confidential or sensitive. Individuals are targeted to take action by clicking on a link and providing information. This research explores fear arousal and self-confidence in subjects confronted by phishing attacks. The study collected data from multiple sources (including an attempted phishing attack). 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 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. The combined data indicated that higher level of fear arousal resulted in a decreased intention to respond to a phishing attack and a decreased actual click behaviour. The research explores how fear of providing login credentials influences both intention to respond and actual response to a phishing attack. When fear arousal is high, individuals are less likely to respond.

ARTICLE HISTORY

Received 22 June 2018
Accepted 8 August 2019

KEYWORDS

Behaviour intention, information security, information security behaviours, fear, self-confidence, EPPM

1. Introduction

The Internet has evolved from an unfettered world of possibilities to a potentially perilous space with hazards such as social engineering, identity theft, viruses, malware and fraud. New threats are propagated in such a rapid manner that it can be difficult for Internet users to stay abreast of the latest risks. One threat, in particular, phishing, continues to be a problem of magnitude. Phishing attacks are an ever-present problem; with attacks still increasing (Olenick). 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 (Jakobsson & Myers 2007). The click of an email link can take users to a fake site requesting login information (Anderson 2013; Caputo et al. 2014). The number of Internet users in the world is around 4.09 billion as of 2018 (Statista 2018) which provides a large population of potential victims to gain identifying information from.

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 and Omoniyi (2006), Internet fraud works and although communications may not be perfectly written, the globalised 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, 2). The messages are designed with the hopes of gaining the attention of a select few potential victims (Wright and 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 and Marmorstein 2006) and can be very deceptive, leaving fakes virtually undetectable by the user (Dhamija, Tygar, and Hearst 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. The social engineering aspects of phishing are described by Easttom and Taylor (2011) as an 'old-fashioned conning' (63) with the social engineer being very adept at manipulating victims by using persuasion and deception (Ramamoorti 2008). As is the case with any scam, those responsible for phishing attacks use all of the basic human needs and desires to manipulate victims including fear and anxiety (Piper 2007; Chiluwa 2009). The use of a fear appeal to motivate a behavioural change and increase the message's persuasiveness is common practice for a phishing campaign. The recipient's judgment can also be clouded because that 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 setup to look like a legitimate company.

An important strategy to protect individuals from falling victim to phishing attacks is to use training to arm users with knowledge to prevent attacks (Kumaraguru et al. 2010). Education is key to prevent individuals from falling victim to social engineering attacks (Easttom and Taylor 2011; Khonji, Iraqi, and Jones 2013). 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). 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. Exploring these relationships will assist with the development of customised user training and impact the prevention of individuals falling victim to phishing attacks. According to a report by Wombat Security, phishing attacks have remained steady with over 76% of companies surveyed experiencing an attack (Wombat Security 2018). While impactful to businesses, there is still little known related to why individuals fall victim to phishing attacks.

2. Literature review

Research related to phishing brings in subject matter from multiple disciplines such as criminology, psychology, fraud, information systems and security. While many of the concepts discussed below have been explored in other disciplines, 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. Recent security research has explored fear appeals and the part they play in user motivation to protect themselves from threats. While the previous research has provided an excellent starting point for this paper, the context of the research focuses on protective measures such as virus protection (Boss et al. 2015); anti-spyware software (Johnston and Warkentin 2010); information security compliance (Vance, Siponen, and Pahnila 2012; Johnston, Warkentin, and Siponen 2015); and preventing password reuse (Jenkins et al. 2014). While protecting oneself from a phishing message is an adequate response to a phishing attack, the researchers focused specifically on the maladaptive and adaptive responses to a phishing message using the theoretical grounding of the Extended Parallel Processing Model (EPPM) (Witte 1992; Witte, Meyer, and Martell 2001) to explore both the message acceptance and message rejection of a fear appeal.

Fear appeals have been studied in psychology research since the early 1950s (Witte and 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, 1983; Witte 1994; Champion et al. 2004; Johnston and Warkentin 2010; Boss et al. 2015; Warkentin et al. 2016). EPPM specifically looks at both message acceptance and message rejection; which the other theories it is derived from (Protection Motivation Theory (Rogers 1975) and Parallel Process Model (Leventhal 1970)) seem to ignore (Witte 1992). The EPPM states that message processing will result in one of two outcomes. These are danger control in which the recipient has the belief that the threat can be averted by performing protective actions and the fear control which results in a defensive avoidance and leads to the message being ignored (Witte, Meyer, and Martell 2001).

If faced with a serious threat, EPPM provides the reasoning that an individual will respond to their fear and take action to reduce it (Witte and Allen 2000). That is, when the level of threat is high, the motivation to act is strong. 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 and Allen (2000), ‘perceived efficacy determines whether people will become motivated to control the danger of the threat or control their fear about the threat’ (594). The perceived threat is defined as thoughts about

danger or harm (Witte 1994). EPPM has been used to explain the reactions that individuals have to a health threat and whether or not they follow the recommended response.

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. The more severe the threat, the more likely the individual will take the recommended action (Das, de Wit, and Stroebe 2003). Additionally, EPPM accounts for message appraisal related to threat and the motivation for processing the message (Witte and Allen 2000). In the case of phishing, the messages are worded with an emotional appeal to fear (Kim and Kim 2013) yet the protective action taken by the message recipient is to respond by providing sensitive information to alleviate the threat.

Fear communications work best when there is an accompanying suggestion of how to cope with the threat (LaRose, Rifon, and Enbody 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 would entail clicking on the link. If the individual provides a user name and password he/she will become a victim to a phishing attack. Communications that threaten the shutdown or lockout of an account are difficult for users to detect as fraudulent (Davinson and Sillence 2010). Therefore, the user is frequently unaware that they are providing sensitive information to a fraudulent source. This situation emphasises the importance of studying both successful and unsuccessful phishing attacks while also educating users on preventative measures.

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 and Taylor 2011). Victims will frequently neglect to report the crime to police; particularly if the financial loss is negligible (White and Fisher 2008). User responses tend to be high during the initial onset of the mass emailing (Moore and Clayton 2007; Kanich et al. 2008; Kanich et al. 2009; Wright and Marett 2010). In fact, while phishing sites are frequently taken down in a hasty manner, Moore and 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).

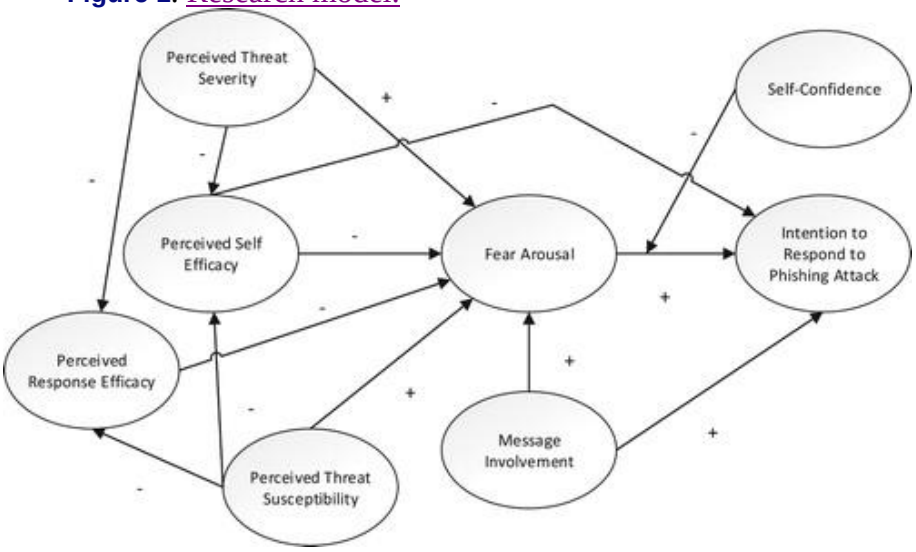
Confidence has a 'stable influence on a person's behavior' (Zulkosky, 2009, 99). Specific to this study, the researchers are interested in how confidence can change the relationship between fear arousal and protection motivation/intention to respond to a phishing attack. Confident subjects will focus less on their fear and have a decreased perception of fear (Carver and Blaney, 1977). Lazarus (1999) found that individuals can address a situation as either a threat or a challenge. Confidence varies among individuals but those that have a high level of confidence are more likely to be challenged in overcoming an obstacle.

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.

3. Model development

This research model, shown in Figure 1, attempts to explore the influence that fear and self-confidence have on an individual's intention to respond to 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. healthcare), they do not specifically address the possible behavioural responses to a phishing attack. More specifically, phishing attacks have the goal of receiving a response. Individuals are that receive a phishing communication click on a link to follow the recommended response and avert the threat by clicking on the link. Conversely, individuals that have self-confidence related to phishing attacks are predicted to respond differently. These individuals will have a decreased likelihood to respond by clicking on the link. Individuals that have self-confidence will moderate the relationship between fear and intention to respond to a phishing attack.

Figure 1. Research model.



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 type of communication has the 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 phishing attack is designed to manipulate victims by using communications that are threatening. The use of words that intend to invoke fear is prevalent. Phrases such as 'urgent reply', 'failure to abide will result in account suspension' and 'permanent suspension' are commonly used. Examples of such attacks that have a high level of fear appeal are email exceeding storage with the threat of inability to send/receive emails or password expiration with the threat of account lockout. Similar threatening phishing communications perceived as a low level of fear could have a request for personal information (with or without a monetary incentive) or provide login information (such as a fraudulent message notification from a site)a communication would be a recently distributed request for 'mystery shopper' participation. This research explores communications that have a fear appeal. Preying upon individual's insecurities using threat is common (Davinson and Sillence 2010) and the researchers seek to gain insight regarding this type of phishing attack.

User response related to phishing attacks can be challenging to gather data that accurately reflect individuals' behavioural responses with just survey data alone. This research collected both experimental and survey data to provide the researchers with a full picture of what occurs when an individual is presented with a phishing attack. The empirical data collected during the experiment provided researchers with data related to how users respond when faced with phishing communication. Collecting both survey and experimental data allow the researchers to explore both individual intention to respond to an attack and click data in response to a phishing message. It is important that researchers learn as much as possible related to what happens during an attempted phishing attack to aid in the development of training and communication to facilitate the prevention of future attacks.

The model below follows a setup similar to Johnston and Warkentin (2010). This model incorporates both self-efficacy and response efficacy from previous research related to 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. Additionally, self-confidence has added as a moderator between fear arousal and intention to respond to a phishing attack.

3.1. Hypotheses

Phishing communications are designed so that users can easily click on a provided link and give out the requested sensitive information. 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, 114). Research has indicated that situations involving high efficacy result in the acceptance of the recommended response (Roskos-Ewoldsen, Yu, and Rhodes 2004).

Self-efficacy is considered 'a person's ability to carry out a recommended response' (Witte 1994, 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 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 phishing communication.

Threats are considered 'harms or losses that have not yet taken place but are anticipated' (Lazarus and Folkman 1984, 32). Users may be aware of potential security threats but this awareness does not necessarily equate to action (Furnell, Bryant, and Phippen 2007; Workman, Bommer, and Straub 2008). Perceived threat severity is defined by Witte (1992) as 'an individual's beliefs about the seriousness of the threat' (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 and 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 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, email account, or education system can be perceived as serious for many individuals. Similar to results found by Wurtele and 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, Adams, and Beyer 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, 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. Thus:

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 the 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 and 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 disbelief in the recommended action's effectiveness (Witte et al. 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 and 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, 194). In addition, those that have a high self-efficacy have a reduction in fear. (Bandura 1977b). An individual can modify his/her behaviour related to his/her abilities in the wake of fear (Marks and 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 and 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 of arousal based on abilities to differentiate between legitimate and illegitimate emails. When an individual has a high level of response efficacy they 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 and Witte 2006). When the perceived threat is elevated, fear is also elevated (Witte 1992; Witte 1998; Witte and Allen 2000). 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 and 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.

Self-Confidence is the 'belief that one can successfully execute an activity' (Feltz 1988, 423). It is a judgment about achieving one's goals (National Research Council 1994). Self-confidence has a strong influence on an individual's behaviour (Bandura 1986; Zulkosky 2009). 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, Hoffrage, and Kleinbolting (1991), self-confidence that is 'immediate and spontaneous rather than a product of

long-term reflection' (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 high self-confidence will focus less on their fear and have a decreased perception of fear (Carver and 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 (Taylor 1987; Feltz 1988). In other words, those that have a high level of self-confidence will not respond to the 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 behaviour' and self-efficacy is something that influences outcomes (Cramer, Neal, and Brodsky 2009, 326). Self-confidence related to general-knowledge tasks has been related to an overconfidence bias such that individuals tend to be confident yet inaccurate (Lichtenstein, Fischhoff, and Phillips 1982; Brenner et al. 1996; Griffin and Brenner 2004; Hoffrage 2004; Koriat 2011). 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).

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 (Confidence, n.d. Merriam-Webster Dictionary online). Research by Cramer, Neal, and Brodsky (2009) 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 and Hall 2004). Self-confidence affects behaviour in the wake of a threatening situation and can give individuals the focus needed to handle the situation effectively (Bandura, Adams, and Beyer 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, Neal, and Brodsky 2009). According to Gigerenzer, Hoffrage, and Kleinbolting (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 and Spiridigliozzi 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 behavioural 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, Prentice-Dunn, and Rogers 2000) which can be related to underlying factors associated with why phishing attacks work. According to Boer and 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 behaviour (De Hoog, Stroebe, and de Wit 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 high fear of 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 phishing communication.

Message involvement entails how important a message is to oneself (Petty and Cacioppo 1990). If individuals find a message to be irrelevant, the message may be deflected (Slavin, Batrouney, and Murphy 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 have heightened fear arousal. It is hypothesised 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 phishing communication.

3.2. 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 (Titus, Heinzelmann, and Boyle 1995; Van Wyk and Mason 2001). Older email users can have difficulty understanding terminology, be intimidated by using technology, and want to avoid making mistakes (Sayago and Blat 2010). They may likely have decreased motor skills and memory yet overconfidence in the knowledge of Internet and computer use (Lam and Lee 2006).

In a study by Pratt, Holtfreter, and Reisig (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, McFarland, and Pachana 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 and 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 themselves (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.

4. Methodology

There is a need for utilising multiple methodologies related to fear appeals research (Crossler et al. 2013). In addition to survey data collected to test the model, the researchers conducted an experiment to collect actual click data in response to a phishing attack.

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, Papadaki, and Furnell 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 behaviour in response to a phishing attack.

4.1. Subjects

The research participants were recruited from students currently taking courses at a university in the southern United States over the course of one semester. The subjects had 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 and were enrolled in the Introduction to Management of Information Systems course. Random sampling of the population minimised threats to external validity. A total of 400 survey emails were sent and 223 surveys were returned resulting in a 56% response rate.

4.2. Survey

The survey items were reviewed by three PhD candidates to ensure face and content validity. The items were reflective indicators as mentioned by Petter, Straub, and Rai (2007). The fourth and fifth items for fear were dropped because they did not apply to the context of fear arousal related to a phishing attack/providing login credentials. 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 .70 or above the range of being acceptable recommended by Nunnally (1978).

The subjects were provided with informed consent related to a study on 'email usage'. The subjects were offered the chance to win a drawing for one of seven $25 Amazon gift cards. It was important for the success of the research that the subjects did not know the training, phishing attempt and survey were related. Therefore, the researchers created an 'opt-out' of future research checkbox so that subjects could be continued to be utilised for the experimental portion of the research. Subjects were assigned a participant number and sent an individual link to the electronic survey via email so that survey data and actual behavioural data could be matched to participants. The researchers used adapted survey instruments for all constructs (see Table 1). The use of instruments adapted from prior research for the survey portion of the research reduced threats to construct validity. The use of surveys in conjunction with experiments has been used to conduct research on phishing response (Downs, Holbrook, and Cranor 2007; Sheng et al. 2010) without putting undue stress on the subjects.

Table 1. Survey measurement items. (Table view)

(All scales were measured using a 7-point Likert scale with 1 = Strongly disagree and 7 = Strongly agree unless otherwise noted).
Self-Efficacy (Adapted from Witte et al. 1996)**:**
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 (Adapted from Witte et al. 1996)**):**

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

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

Response Efficacy (Adapted from Witte et al. 1996)**):**

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 (Adapted from Witte et al. 1996)**:**

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 (from Shrauger and 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 (Adapted from Witte et al. 1996)**:**

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 (Adapted from 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.

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)

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

4.3. Experiment

An experiment was conducted using a subset of the survey population; specifically, those that did not check ‘do not contact me for future research’ during the informed consent process. The experiment was setup so that data could be collected in response to a realistic phishing attack. 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 setup a plausible scenario in which to gain sensitive information, all of the students in the seven sections were given a course-related training assignment. Ideally, studies should involve real-life activities to try to mimic encounters and reduce suspicion (Herzberg and Margulies 2011).

The experiment collected data from subjects faced with a phishing attack attempt. The experiment was setup as a 2X2 (Training, Fear appeal). The students were randomly assigned to one of four experimental treatments prior to receiving training site instructions and prior to additional participation in the study/experiment. The possible combinations were Low Fear/Baseline Training, Low Fear/Advanced Training, High Fear/Baseline Training, High Fear/Advanced Training. The web-based training site was created to provide flexibility in the design of the experiment and treatments. A plausible training url was used to ensure the subjects did not doubt the legitimacy of the site. The instructors were given scripts to introduce the training site as part of the course material and to ensure a consistent message was communicated. All of the students in the course were assigned the task and given training materials that contained the link and instructions on how to setup a username and password. 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. In total, 529 logins were created. Randomly assigning subjects to treatments minimised threats to internal validity.

After setting up the login information, students were shown a training video with either basic (00:01:21 duration) or advanced (00:02:47 duration) 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 but the advanced training contained information specifically pertaining to phishing prevention. Knowledge is a major component in protecting individuals from scams (Weisman 2008). One week after the training task was due; the subjects that provided consent for future contact were sent a phishing email based on their pre-assigned condition of low fear/high fear. 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 and Chapple 2005).

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 1967). 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 and 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.

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 analysed using SmartPLS 2.0 software (Ringle, Wende, and Will 2005). Partial Least Squares (PLS) is more flexible with sample size when compared to Structural Equation Modeling (SEM) (Hair et al. 2010). 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, Gottfredson, and Joo 2013) the total usable sample size was 192. The sample was 50.5% female.

A principle components analysis was performed in SPSS. This resulted in eight 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 two separate items. Confidence items for the first set of questions (items 1, 3 and 7) had the reliability of .7021 and Cronbach's alpha of .6941.

However, items 3 and 7 had very low factor loadings (.146 and −.041). These items were dropped and resulted in 1 item remaining. The second construct (items 2, 4, 5 and 6) had 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. 2010). More details related to self-confidence are explained in the section below.

The constructs were checked for validity, reliability and internal consistency. Table 2 displays Cronbach's alpha and reliability for the constructs. Reliability evaluates the consistency of the measurements of a variable (Hair et al. 2010). As mentioned by Hair et al. (2010) 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, Liehr-Gobbers, and Krafft 2007). The recommended cutoff for composite reliability is .70 (Fornell and Larcker 1981; Gefen and Straub 2005). All of the remaining variables had 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. 2010). The variables range from .6016 to .9754 which fall within the range and indicate no problems with internal consistency.

Table 2. Composite reliability and Cronbach's alpha. (Table view)

	Composite reliability	Cronbach's alpha
Fear arousal	0.8749	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
Confidence	0.7865	0.6560

Next, validity was evaluated. Validity looks at whether a variable represents what it should (Hair et al. 2010). 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, the web experience 1 and response efficacy 1 were removed. The cross loadings for the remaining variables are displayed in Table 3 below. There is no evidence of cross loading on other constructs. The AVEs for the variables are also displayed in Table 3 below. It is recommended that for adequate convergence of items, the AVEs exceed .50 (Hair et al. 2010). All of the AVEs exceeded .50 except for perceived response efficacy which is .402. As mentioned by Fornell and Larcker (1981), if AVE is less than .5 but the composite reliability is greater than .6 convergent validity is acceptable.

Table 3. Exploratory factor loadings and AVE. (Table view)

	Exploratory factor loadings						
	1	2	3	4	5	6	AVE
SE1	0.873						0.702
SE2	0.843						
SE3	0.797						
TSE2		0.854					0.556
TSE3		0.618					
RE2			0.652				0.402
RE3			0.616				
TSU1				0.734			0.512
TSU2				0.766			
TSU3				0.642			
INT1					0.962		0.9
INT2					0.932		
FA1						0.698	0.522
FA2						0.750	
FA3						0.733	
FA6						0.680	
FA7						0.758	
FA8						0.716	

Discriminant validity and internal reliability were assessed by performing exploratory factor analysis. The Kaiser–Meyer–Oklin measure of sampling adequacy was .733 which is above the recommended .6 (Kaiser 1974; Cerny and Kaiser 1977). The initial scree plot (performed with principal components extraction) indicated that there were six factors which provided the value for the next test within the exploratory factor analysis. A promax rotation was first performed, to verify that there were no correlation issues. All six factors loaded properly within the expected constructs with no correlation issues. A varimax rotation was performed next, with all items loading on the expected six factors. The factors explained 62% of the variance and there were no cross loadings above .25. The loadings are shown in Table 3. In addition, to check for issues related to discriminant validity, a correlation matrix should be checked and compared with the square root of the AVE to ensure that the correlation is not greater than the square root of the AVE. The square root of the AVE (on the diagonal in Table 4) is not less than the correlations in the correlation matrix thus indicating that there are not issues with discriminant validity. Tests for collinearity were also run in SPSS using the independent variables. The VIF scores for each variable did not exceed 1.3 which is lower than 5 which is recommended as the lowest tolerable level by Hair et al. (2010). VIFs less than five indicate that there are not problems with multicollinearity.

Table 4. Correlation matrix and square root of average variance extracted (AVE) (on diagonal). (Table view)

	Fear arousal	Intention to respond	Perceived self-efficacy	Perceived response efficacy	Perceived threat severity	Perceived threat susceptibility
Fear arousal	**0.722**					
Intention to respond	−0.020	**0.949**				
Perceived self-efficacy	−0.148	−0.343	**0.837**			
Perceived response efficacy	−0.099	−0.124	0.282	**0.634**		
Perceived threat severity	0.084	−0.033	0.013	0.170	**0.746**	
Perceived threat susceptibility	0.152	−0.093	−0.083	−0.059	0.039	**0.716**

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 hypothesised 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 hypothesised 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 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, Adams, and Beyer 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 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 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 an indication that the items separated into two constructs. When the data was analysed 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 and 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 and 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 increased fear of 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 and Figure 2 below provide a summary of the hypotheses and summarise the results for the hypothesis testing.

Figure 2. Results of the analysis.

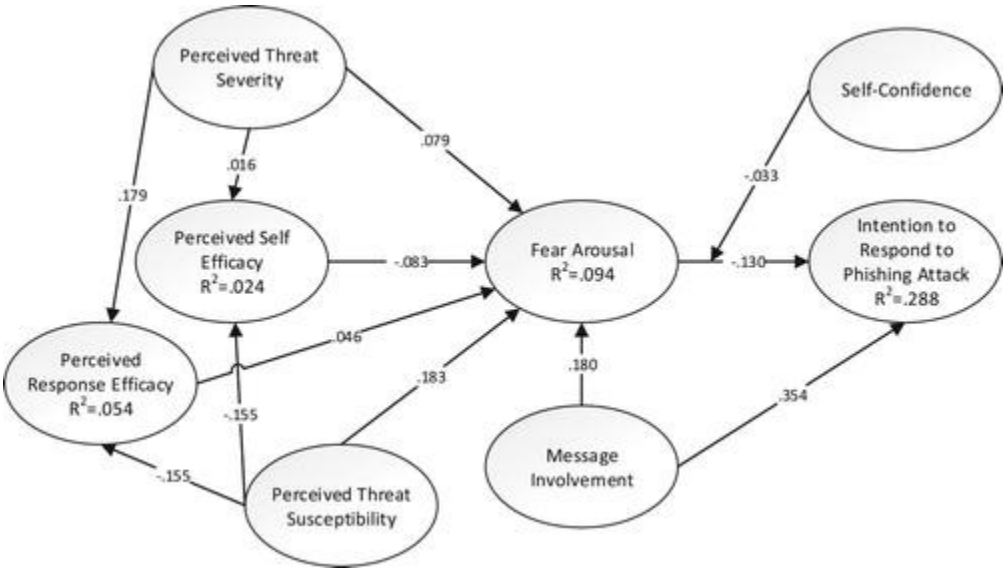


Table 5. Summary of the survey results. (Table view)

	t-statistic	*p*-Value (1-tailed)	
H1: Perceived self-efficacy will decrease the intention to respond to a phishing communication.	4.942	<.0001***	Supported
H2a: Perceived threat severity will have a negative influence on perceived self-efficacy.	0.017	0.4932	Not Supported
H2b: Perceived threat severity will have a negative influence on perceived response efficacy.	2.113	0.0179**	Not Supported (Sig,Opp Dir)
H3a: Perceived threat susceptibility will have a negative influence on perceived self-efficacy.	1.96	0.0257**	Supported
H3b: Perceived threat susceptibility will have a negative influence on perceived response efficacy.	1.96	0.0257**	Supported
H4: Perceived self-efficacy will have a negative influence on fear arousal.	1.246	0.1071	Not Supported
H5: Perceived response efficacy will have a negative influence on fear arousal.	0.557	0.2891	Not Supported
H6: Perceived threat severity will have a positive influence on fear arousal.	0.791	0.2150	Not Supported
H7: Perceived threat susceptibility will have a positive influence on fear arousal.	2.23	0.0135**	Supported
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.	0.382	0.3514	Not Supported
H9: Fear arousal will have a positive influence on the intention to respond to the phishing communication.	2.267	0.0123**	Significant, Opposite Direction
H10: Message involvement will have a positive influence on fear arousal.	2.159	0.0160	Supported
H11: Message involvement will have a positive influence on intention to respond to the phishing communication.	4.864	<.0001***	Supported

*$p < .10$.

**$p < .05$.

***$p < .001$.

5.2.1. Experiment results

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 analysing data with a dichotomous dependent variable is logistic regression (Kutner et al. 2005). The subjects were sent individual links so that the participant number could be preserved. The original experimental dataset consisted of 100 subjects. 18 subjects clicked on the

link. 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 in Table 6 below.

Table 6. Results of the experiment. (Table view)

		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).

5.2.2. Post-hoc analysis

Further analysis was conducted to explore findings related to gender and the web experience, and also analysis for combined survey/click data. An interesting finding was that the web experience resulted in an increased intention to respond to phishing communication. Those with increased the web experience were *more likely* to respond. The web experience had a significant positive influence on intention to respond (.167, $t = 2.370$)

The data was split by gender (Male = 1; Female = 2). Women had a significant negative relationship between fear and intention to respond to a phishing attack. Also of interest is that men had a decreased influence of fear arousal on the intention to respond to a phishing attack. This is interesting because men are taught not to express fear as an emotion (Rachman 1978). Also of interest is that women with a high level of self-confidence were less likely to respond to a phishing attack ($t = -2.113$, *p*-value .037).

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. The results are displayed in Table 7. Perceived self-efficacy, perceived threat severity and fear arousal was significant at the .05 level ($p < .05$). Perceived self-confidence and perceived threat susceptibility were not significant ($p > .10$).

Table 7. DV click with survey data. (Table view)

	B	*p*-Value (1-tailed)
Perceived self-efficacy	−.586	.0290**
Perceived threat severity	1.042	.0455**
Perceived threat susceptibility	.396	.1175
Self-confidence	−.351	.1290
Fear arousal	−.775	.0295**
Message involvement	.556	.302

**$p < .05$.

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

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 were collected using an adapted scale from Van Wyk and Benson (1997). While risk did not significantly influence the intention to respond to a phishing attack (−.006, $t = .131$), the relationship was negative. This is similar to what Van Wyk and Benson (1997) found in their study; risk-taking did not significantly influence fraud victimisation. 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 results are displayed in Table 8. The high risk group had a significant decreased intention to respond when fear arousal was high. This is interesting because Van Wyk and Benson (1997) found that high risk individuals are more open to fraudulent transactions but risk taking did not equate to successful victimisation. This research was in agreement with those findings; risky individuals were less likely to respond out of fear.

Table 8. Risk group high/low. (Table view)

RiskGrp	Model		Coefficients[a] Unstandardized coefficients		Standardized coefficients	*t*	Sig.
			B	Std. error	Beta		
High	1	(Constant)	6.592	1.521		4.335	.000
		Fear arousal	−.213	.127	−.160	−1.674	.097
		Perceived self-efficacy	−.502	.134	−.372	−3.733	.000
		Perceived threat severity	.038	.158	.023	.242	.809
		Perceived threat susceptibility	.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
		Fear arousal	−.041	.112	−.035	−.360	.719
		Perceived self-efficacy	−.233	.105	−.221	−2.219	.029
		Perceived threat severity	.050	.143	.034	.353	.725
		Perceived threat susceptibility	−.102	.099	−.100	−1.035	.303
		Gender	.232	.300	.077	.775	.440
		Age	−.365	.310	−.114	−1.178	.242

[a]Dependent variable: Intention to respond to phishing attack.

The data was split by gender (Male = 1; Female = 2) and displayed in Table 9. For women, fear had a significant negative relationship on the 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 9. Split by gender (1 = Male, 2 = Female). (Table view)

Gender	Model		Coefficients[a] Unstandardized coefficients		Standardized coefficients	*t*	Sig.
			B	Std. error	Beta		
1	1	(Constant)	3.048	1.601		1.904	.060*
		Fear arousal	−.047	.121	−.041	−.388	.699
		Self conf 245	−.078	.116	−.069	−.672	.503
		Perceived self-efficacy	−.447	.143	−.321	−3.129	.002**
		Perceived threat severity	.112	.148	.075	.757	.451

Gender		Model	Coefficients[a] Unstandardized coefficients		Standardized coefficients	*t*	Sig.
			B	Std. error	Beta		
		Perceived threat susceptibility	−.031	.112	−.029	−.278	.781
		Self-confidence 1	.193	.104	.196	1.849	.068*
		Web experience	.270	.151	.177	1.788	.077*
2	1	(constant)	6.475	1.294		5.005	.000***
		Fear arousal	−.186	.111	−.154	−1.667	.099*
		Self Conf 245	−.242	.115	−.206	−2.113	.037**
		Perceived self-efficacy	−.461	.093	−.466	−4.979	.000***
		Perceived threat severity	−.121	.130	−.087	−.930	.355
		Perceived threat susceptibility	−.178	.100	−.165	−1.785	.078*
		Self confidence1	.208	.102	.197	2.036	.045**
		Web experience	.202	.124	.155	1.632	.106

[a]Dependent variable: Intention to respond to phishing attack.

*$p < .10$.

**$p < .05$.

***$p < .001$.

6. Discussions and conclusions

This research explored how fear and self-confidence influenced individuals' response to phishing communication. 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. While the relationship between self-confidence and the intention to respond to a phishing attack was not significant, it is important to maintain education related to the dangers of clicking on links. 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 hypothesised. 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).

Behaviours related to deceptive/fraudulent practices by email and computer-related communications have not been extensively studied (Chiluwa 2009). Research related to phishing is still very exploratory in nature and is lacking strong theoretical grounding. In addition, it can be difficult to collect actual behavioural data. According to Finn and Jakobsson (2007), phishing research can be tricky to setup; particularly in light of the fact that subjects are being deceived into providing sensitive information. However, the researchers were able to obtain both survey data and actual click data. 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. 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). In this study, 18% of individuals *did* click on the link which is higher than the 2% standard. Educating users about the dangers of phishing is still important for the protection of sensitive information such as user names and passwords. Even with education and training in place, there is still a risk that Internet users will lack the skills necessary to prevent sensitive information such as user name and password from being compromised (Hallam-Baker 2008). Some of the limitations of the study are mentioned below.

6.1. 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 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 jeopardised 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 and scripted verbiage on how to introduce the training so that the message was consistent.

> Both the requirement for an informed consent and the requirement for permission for future contact (required for sending the phishing email) had an effect on the sample size for the experiment. A total of 335 individuals participated in the training. Of those, 100 provided informed consent with permission for future contact and were able to be 'phished'. 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 and 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.

It is possible that the high fear email was too strong and the low fear email too weak persuasively. According to Ray and Wilkie (1970) moderate fear arousal may result in the largest response rate. Janis and 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 and 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, Hunt, and Eppright 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 desensitised reaction; thus reducing its effect. In particular, a judgment or beliefs and knowledge can reshape a situation in a manner that no longer is 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 and Agarwal (2010) although this age group is representative of a majority of Internet users, they may have differing opinions on what is persuasive.

The perceived genuineness of the threat could have had an effect on fear arousal. The emails that were chosen for both the survey responses and the phishing experiment contained elements that provided a plausible situation (a database corruption and exceeded email storage). Research by

Algarni, Xu, and Chan (2017) explored dimensions of source credibility and its influence on susceptibility to social engineering victimisation. All of the dimensions significantly influenced susceptibility. The emails that were crafted for this study were sent from an authoritative source. Other studies have explored source credibility (Sussman and Siegal 2003; Dhamija, Tygar, and Hearst 2006; Luo et al. 2012) as an influencer of phishing victimisation. Future research should explore the credibility of the source and also the genuineness of the threat to determine the influence that these constructs have on fear arousal related to phishing messages in this context.

Lastly, the researchers did not explore the influences that computer anxiety and internet anxiety could have on the participants' behaviour related to phishing attacks. Prior studies have explored computer anxiety and negative affectivity (Thatcher and Perrewé 2002), performance in a computing-intensive environment (Buche, Davis, and Vician 2007), and social aversion and institution-based trust (Baker et al. 2014). This construct is related to the level of confidence an individual may have with higher confidence related to lower computer anxiety (Thatcher and Perrewé 2002). Internet anxiety was found to be influenced by both personality and beliefs (Thatcher et al. 2007). Additional studies related to internet anxiety and teachers' anxiety (Ekizoglu and Ozcinar 2011), gender, experience and identification (Joiner et al. 2005; Joiner et al. 2012), and as a comparison across generations (Joiner et al. 2013). Internet anxiety can hinder individuals' use of the Internet and is closely related to computer anxiety (Thatcher et al. 2007).

6.2. Contributions to research and practice

Detecting deceitful emails is difficult for users (Kim and Kim 2013). As mentioned by Guo et al. (2011), education and training related to security risk can sometimes be vague and problematic in preventing violations. Training with specific prevention mechanisms such as this (do not click on links in emails) may be a start to implementing simple prevention mechanisms. 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. In this case, a very threatening fear appeal caused subjects to shut down and 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 organisation. Hackers will continue to exploit security loopholes such as providing false IP addresses to redirect Internet traffic to fraudulent websites (Schneider and Burstein 2009). 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 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 organisations (Brenner 2010).

Disclosure statement

No potential conflict of interest was reported by the authors.

References

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

Algarni, A., Y. Xu, and T. Chan. 2017. "An Empirical Study on the Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook." *European Journal of Information Systems* 26 (6): 661–687. Crossref.

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

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

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

Baker, E. W., J. B. Thatcher, M. Gundlach, and D. M. McKnight. 2014. "The Influence of Social Aversion and Institution-Based Trust on Computer Self-Efficacy, Computer Anxiety, and Antecedents to IT Use." *Journal of Organizational and End User Computing* 26 (1): 1–26. Crossref.

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

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

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

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

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

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

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

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

Boer, H., and E. R. Seydel. 1996. "Protection Motivation Theory." In *Predicting Health Behaviour*, edited by M. Connor and P. Norman, 95–120. Buckingham: Open University Press.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors." *MIS Quarterly* 39 (4): 837–864. Crossref.

Brenner, S. W. 2010. *Cybercrime: Criminal Threats From Cyberspace*. Santa Barbara, CA: Praeger.

Brenner, L., D. Koehler, V. Liberman, and A. Tversky. 1996. "Overconfidence in Probability and Frequency Judgments: A Critical Examination." *Organizational Behavior and Human Decision Processes* 65 (3): 212–219. Crossref.

Buche, M. W., L. R. Davis, and C. Vician. 2007. “A Longitudinal Investigation of the Effects of Computer Anxiety on Performance in a Computing-Intensive Environment.” *Journal of Information Systems Education* 18 (4): 415–423.
Butler, R. 2007. “A Framework of Anti-Phishing Measures Aimed at Protecting the Online Consumer’s Identity.” *The Electronic Library* 25 (5): 517–533. Crossref.
Byrne, J. A. 2004. “Why Courage?” *Fast Company* 86: 16.
Caputo, D. D., S. L. Pfleeger, J. D. Freeman, and M. E. Johnson. 2014. “Going Spear Phishing: Exploring Embedded Training and Awareness.” *IEEE Security & Privacy* 12 (1): 28–38. Crossref.
Carver, C. S., and P. H. Blaney. 1977. “Perceived Arousal, Focus of Attention, and Avoidance Behavior.” *Journal of Abnormal Psychology* 86 (2): 154–162. Crossref. PubMed.
Cauberghe, V., P. De Pelsmacker, W. Janssens, and N. Dens. 2009. “Fear, Threat, and Efficacy in Threat Appeals: Message Involvement as a Key Mediator to Message Acceptance.” *Accident Analysis and Prevention* 41: 276–285. Crossref. PubMed.
Cerny, C. A., and H. F. Kaiser. 1977. “A Study of a Measure of Sampling Adequacy for Factor-Analytic Correlation Matrices.” *Multivariate Behavioral Research* 12 (1): 43–47. Crossref. PubMed.
Champion, V. L., C. S. Skinner, U. Menon, S. Rawl, R. B. Giesler, P. Monahan, and J. Daggy. 2004. “A Breast Cancer Fear Scale: Psychometric Development.” *Journal of Health Psychology* 9 (6): 753–762. Crossref. PubMed.
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. Crossref.
Chiluwa, I. 2009. “The Discourse of Digital Deceptions and ‘419’ Emails.” *Discourse Studies* 11 (6): 635–660. Crossref.
Confidence. n.d. In *Merriam-Webster Dictionary* online. http://www.merriam-webster.com/dictionary/confidence.
Connor, M., and P. Norman. 1995. “The Role of Social Cognition in Health Behaviours.” In *Predicting Health Behaviour. pg*, edited by M. Connor and P. Norman, 1–22. Buckingham: Open University Press.
Cramer, R. J., T. M. S. Neal, and S. L. Brodsky. 2009. “Self-Efficacy and Confidence: Theoretical Distinctions and Implications for Trial Consultation.” *Consulting Psychology Journal: Practice and Research* 61 (4): 319–334. Crossref.
Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. 2013. “Future Directions for Behavioral Information Security Research.” *Computers & Security* 32: 90–101. Crossref.
Das, E. H. H. J., J. B. F. de Wit, and W. Stroebe. 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. Crossref. PubMed.
Davinson, N., and E. Sillence. 2010. “It Won’t Happen to Me: Promoting Secure Behaviour Among Internet Users.” *Computers in Human Behavior* 26 (6): 1739–1747. Crossref.
De Hoog, N., W. Stroebe, and J. B. F. de Wit. 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. Crossref.
Dhamija, R., J. D. Tygar, and M. Hearst. 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.
Dinev, T., and Q. Hu. 2007. “The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies.” *Journal of the Association for Information Systems* 8 (2): 386–408. Crossref.
Downs, J. S., M. Holbrook, and L. F. Cranor. 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., and J. Taylor. 2011. *Computer Crime, Investigation, and the Law*. Boston, MA: Course Technology.
Ekizoglu, N., and Z. Ozcinar. 2011. “A Study of Developing an Anxiety Scale Towards the Internet.” *Procedia Social and Behavioral Sciences* 15: 3902–3911. Crossref.

Feltz, D. L. 1988. “Self-Confidence and Sports Performance.” *Exercise and Sport Sciences Reviews* 16 (1): 423–458. PubMed.
Finn, P., and M. Jakobsson. 2007. “Designing Ethical Phishing Experiments.” *IEEE Technology and Society Magazine* 26 (1): 46–58. Crossref.
Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers. 2000. “A Meta-Analysis of Research on Protection Motivation Theory.” *Journal of Applied Social Psychology* 30 (2): 407–429. Crossref.
Fornell, C., and D. F. Larcker. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.” *Journal of Marketing Research* 18 (1): 39–50. Crossref.
Furnell, S. M., P. Bryant, and A. D. Phippen. 2007. “Assessing the Security Perceptions of Personal Internet Users.” *Computers & Security* 26 (5): 410–417. Crossref.
Gefen, D., and D. Straub. 2005. “A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example.” *Communications of the Association for Information Systems* 16: 91–109. Crossref.
Giaquinto, S., and C. Spiridigliozzi. 2007. “Possible Influences of Spiritual and Religious Beliefs on Hypertension.” *Clinical and Experimental Hypertension* 29 (7): 457–464. Crossref. PubMed.
Gigerenzer, G., U. Hoffrage, and H. Kleinbolting. 1991. “Probabilistic Mental Models: A Brunswikian Theory of Confidence.” *Psychological Review* 98 (4): 506–528. Crossref. PubMed.
Gotz, O., K. Liehr-Gobbers, and M. Krafft. 2007. “Evaluation of Structural Equation Models Using Partial Least Squares (PLS) Approach.” In *Handbook of Partial Least Squares*, 691–711. Berlin: Springer-Verlag.
Green, E. C., and K. Witte. 2006. “Can Fear Arousal in Public Health Campaigns Contribute to the Decline of HIV Prevalence?” *Journal of Health Communication* 11 (3): 245–259. Crossref. PubMed.
Griffin, D., and L. Brenner. 2004. “Perspectives on Probability Judgment Calibration.” In *Blackwell Handbook of Judgment and Decision Making*, edited by D. J. Koehler, and N. Harvey, 177–198. Malden, MA: Blackwell. Crossref.
Guo, K. H., Y. Yuan, N. Archer, and C. Connelly. 2011. “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model.” *Journal of Management Information Systems* 28 (2): 203–236. Crossref.
Hair, J., W. Black, B. Babin, and R. Anderson. 2010. *Multivariate Data Analysis*. Upper Saddle River, NJ: Prentice Hall.
Hallam-Baker, P. 2008. *The DotCrime Manifesto: How to Stop Internet Crime*. Boston, MA: Pearson Education.
Herzberg, A., and R. Margulies. 2011. “Forcing Johnny to Login Safely.” In *European Symposium on Research in Computer Secuirty: ESORICS 2011*. Vol. 6879., edited by V. Atluri and C. Diaz, 452–471. Berlin: Springer. Crossref.
Hoffrage, U. 2004. “Overconfidence.” In *Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgment, and Memory*, edited by R. F. Pohl, 235–254. Hove, England: Psychology Press.
Hollenbeck, G. P., and D. T. Hall. 2004. “Self-confidence and Leader Performance.” *Organizational Dynamics* 33 (3): 254–269. Crossref.
Jakobsson, M., and S. Myers. 2007. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Hoboken, NJ: John Wiley & Sons, Inc.
James, L. 2005. *Phishing Exposed*. Syngress Publishing.
Janis, I. L. 1967. “Effects of Fear Arousal on Attitudinal Change: Recent Developments in Theory and Experimental Research.” In *Advances in Experimental Social Psychology*. Vol. 3, edited by L. Berkowitz, 166–225. New York, NY: Academic Press. Crossref.
Janis, I. L., and S. Feshbach. 1953. “Effects of Fear-Arousing Communications.” *Journal of Abnormal Psychology* 48 (1): 78–92. Crossref. PubMed.
Jenkins, J. L., M. Grimes, J. G. Proudfoot, and P. B. Lowry. 2014. “Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals.” *Information Technology for Developoment* 20 (2): 196–213. Crossref.
Johnston, A. C., and M. Warkentin. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study.” *MIS Quarterly* 34 (3): 549–566. Crossref.

Johnston, A. C., M. Warkentin, and M. Siponen. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric." *MIS Quarterly* 39 (1): 113–134. Crossref.
Joiner, R., J. Gavin, M. Brosnan, J. Cromby, H. Gregory, J. Guiller, P. Maras, and A. Moon. 2012. "Gender, Internet Experience, Internet Identification, and Internet Anxiety: A Ten Year Followup." *Cyberpsychology, Behavior, and Social Networking* 15 (7): 370–372. Crossref. PubMed.
Joiner, R., J. Gavin, M. Brosnan, J. Cromby, H. Gregory, J. Guiller, P. Maras, and A. Moon. 2013. "Comparing First and Second Generation Digital Natives' Internet Use, Internet Anxiety, and Internet Identification." *Cyberpsychology, Behavior, and Social Networking* 16 (7): 549–552. Crossref. PubMed.
Joiner, R., J. Gavin, J. Duffield, M. Brosnan, C. Crook, A. Durndell, P. Maras, J. Miller, A. J. Scott, and P. Lovatt. 2005. "Gender, Internet Identification, and Internet Anxiety: Correlates of Internet Use." *CyberPsychology & Behavior* 8 (4): 371–378. Crossref. PubMed.
Kahneman, D. 2011. *Thinking, Fast and Slow*. New York, NY: Farrar, Straus, and Giroux.
Kaiser, H. 1974. "An Index of Factor Simplicity." *Psychometrika* 39 (1): 31–36. Crossref.
Kanich, C., C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. 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., C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. 2009. "Spamalytics: An Empirical Analysis of Spam Marketing Conversion." *Communications of the ACM* 52 (9): 99–107. Crossref.
Khonji, M., Y. Iraqi, and A. Jones. 2013. "Phishing Detection: A Literature Survey." *IEEE Communications Surveys & Tutorials* 15 (4): 2091–2121. Crossref.
Kim, D., and J. H. Kim. 2013. "Understanding Persuasive Elements in Phishing E-Mails: A Categorical Content and Semantic Network Analysis." *Online Information Review* 37 (6): 835–850. Crossref.
Koriat, A. 2011. "Subjective Confidence in Perceptual Judgments: A Test of the Self-Consistency Model." *Journal of Experimental Psychology: General* 140 (1): 117–139. Crossref. PubMed.
Kumaraguru, P., S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. 2010. "Teaching Johnny Not to Fall for Phish." *ACM Transactions on Internet Technology* 10 (2): 1–31. Crossref.
Kutner, M. H., C. J. Nachtsheim, J. Neter, and W. Li. 2005. *Applied Linear Statistical Models*. Boston, MA: McGraw-Hill/Irwin.
Lam, J. C. Y., and M. K. O. Lee. 2006. "Digital Inclusiveness–Longitudinal Study of Internet Adoption by Older Adults." *Journal of Management of Information Systems* 22 (4): 177–206. Crossref.
LaRose, R., N. J. Rifon, and R. Enbody. 2008. "Promoting Personal Responsibility for Internet Safety." *Communications of the ACM* 51 (3): 71–76. Crossref.
Lazarus, R. S. 1966. *Psychological Stress and the Coping Process*. New York: McGraw-Hill Book.
Lazarus, R. S. 1999. *Stress and Emotion: A New Synthesis*. New York: Springer.
Lazarus, R. S., and S. Folkman. 1984. *Stress, Appraisal, and Coping*. New York: Springer.
Lehrer, J. 2009. *How We Decide*. New York: Houghton Mifflin Harcourt.
Leventhal, H. 1970. "Findings and Theory in the Study of Fear Communications." In *Advances in Experimental Social Psychology*, Vol. 5. edited by L. Berkowitz. New York: Wiley. Crossref.
Lichtenstein, S., B. Fischhoff, and L. D. Phillips. 1982. "Calibration of Probabilities: The State of the Art to 1980." In *Judgment Under Uncertainty: Heuristics and Biases*, edited by D. Kahneman, P. Slovic, and A. Tversky, 306–334. New York: Cambridge University Press. Crossref.
Luo, X. R., W. Zhang, S. Burd, and A. Seazzu. 2012. "Investigating Phishing Victimization with the Heuristic-Systematic Model: A Theoretical Framework and an Exploration." *Computers & Security* 38 (1): 28–38.
Marks, I., and A. Tobeña. 1990. "Learning and Unlearning Fear: A Clinical and Evolutionary Perspective." *Neuroscience & Biobehavioral Review* 14 (4): 365–384. Crossref. PubMed.
Moore, T., and R. Clayton. 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.
Nash, J. R. 1976. *Hustlers and Con Men: An Anecdotal History of the Confidence Man and His Games*. New York: M. Evans and Company.
National Research Council. 1994. *Learning, Remembering, Believing: Enhancing Human Performance*. Washington, DC: The National Academies Press.

Nunnally, J. C. 1978. *Psychometric Theory*. New York: McGraw-Hill.
Olenick, D. 2017. Email Malware, Phishing and Spam Attempts Hit New Highs for 2017. *SC Media*, August 7, 2017.
Paine, C., U. D. Reips, S. Stieger, A. Joinson, and T. Buchanan. 2007. "Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'." *International Journal of Human-Computer Studies* 65 (6): 526–536. Crossref.
Petter, S., D. Straub, and A. Rai. 2007. "Specifying Formative Constructs in Information Systems Research." *MIS Quarterly* 31 (4): 623–656. Crossref.
Petty, R. E., and J. T. Cacioppo. 1990. "Involvement and Persuasion: Tradition Versus Integration." *Psychological Bulletin* 107 (3): 367–374. Crossref.
Pinsker, D. M., K. McFarland, and N. A. Pachana. 2010. "Exploitation in Older Adults: Social Vulnerability and Personal Competence Factors." *Journal of Applied Gerontology* 29 (6): 740–761. Crossref.
Piper, P. S. 2007. "Phish Pharming." *Searcher: The Magazine for Database Professionals* 15 (9): 40–47.
Pratt, T. C., K. Holtfreter, and M. D. Reisig. 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. Crossref.
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. Crossref.
Ray, M., and W. Wilkie. 1970. "Fear: The Potential of an Appeal Neglected by Marketing." *Journal of Marketing* 34 (1): 54–62. Crossref.
Ringle, C. M., S. Wende, and A. Will. 2005. SmartPLS 2.0.M3. Hamburg: SmartPLS. http://www.smartpls.de.
Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change." *Journal of Psychology* 91 (1): 93–114. Crossref. PubMed.
Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation." In *Social Psychophysiology: A Sourcebook*, edited by J. Cacioppo, and R. Petty, 153–176. New York: Guilford.
Roskos-Ewoldsen, D. R., H. J. Yu, and N. Rhodes. 2004. "Fear Appeal Messages Affect Accessibility of Attitudes Toward the Threat and Adaptive Behaviors." *Communications Monographs* 71 (1): 49–69. Crossref.
Sagarin, B. J., R. B. Cialdini, W. E. Rice, and S. B. Serna. 2002. "Dispelling the Illusion of Invulnerability: The Motivations and Mechanisms of Resistance to Persuasion." *Journal of Personality and Social Psychology* 83 (3): 526–541. Crossref. PubMed.
Sarel, D., and H. Marmorstein. 2006. "Addressing Consumers' Concerns About Online Security: A Conceptual and Empirical Analysis of Banks' Actions." *Journal of Financial Services Marketing* 11 (2): 99–115. Crossref.
Sayago, S., and Josep Blat. 2010. "Telling the Story of Older People E-Mailing: An Ethnographical Study." *International Journal of Human-Computer Studies* 68 (1–2): 105–120. Crossref.
Schneider, F. B., and A. Burstein. 2009. "Trustworthiness as a Limitation on Network Neutrality." *Federal Communications Law Journal* 61 (3): 591–623.
Sheng, S., M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs. 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. Crossref. PubMed.
Shrauger, J. S., and M. Schohn. 1995. "Self-Confidence in College Students: Conceptualization, Measurement, and Behavioral Implications." *Assessment* 2: 255–278. Crossref.
Slavin, S., C. Batrouney, and D. Murphy. 2007. "Fear Appeals and Treatment Side-Effects: An Effective Combination for HIV Prevention?" *AIDS Care* 19 (1): 130–137. Crossref. PubMed.
Solomon, M. G., and M. Chapple. 2005. *Information Security Illuminated*. Sudbury, MA: Jones and Bartlett Publishers.
Stamatellos, G. 2007. *Computer Ethics: A Global Perspective*. Mississauga, Ontario: Jones and Bartlett.

Statista. 2018. “Global Digital Population as of April 2018.” https://www-statista-com.leo.lib.unomaha.edu/statistics/617136/digital-population-worldwide/.
Sussman, S. W., and W. S. Siegal. 2003. “Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption.” *Information Systems Research* 14 (1): 47–65. Crossref.
Tanner, J. F., J. B. Hunt, and D. R. Eppright. 1991. “The Protection Motivation Model: A Normative Model of Fear Appeals.” *Journal of Marketing* 55 (3): 36–45. Crossref.
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. Crossref. PubMed.
Thatcher, J. B., M. L. Loughry, J. Lim, and D. M. McKnight. 2007. “Internet Anxiety: An Empirical Study of the Effects of Personality, Beliefs, and Social Support.” *Information & Management* 44 (4): 353–363. Crossref.
Thatcher, J. B., and P. L. Perrewe. 2002. “An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy.” *MIS Quarterly* 26 (4): 381–396. Crossref.
Titus, R. M., F. Heinzelmann, and J. M. Boyle. 1995. “Victimization of Persons by Fraud.” *Crime Delinquency* 41 (1): 54–72. Crossref.
Vance, A., M. Siponen, and S. Pahnila. 2012. “Motivating IS Security Compliance: Insights From Habit and Protection Motivation Theory.” *Information & Management* 49 (3-4): 190–198. Crossref.
Van Wyk, J. L., and M. Benson. 1997. “Fraud Victimization: Risky Business or Just Bad Luck?” *American Journal of Criminal Justice* 21 (2): 163–179. Crossref.
Van Wyk, J., and K. A. Mason. 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. Crossref.
Vishwanath, A., T. Herath, R. Chen, J. Wang, and R. Rao. 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. Crossref.
Wang, J., T. Herath, R. Chen, A. Vishwanath, and H. R. Rao. 2012. “Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email.” *IEEE Transactions on Professional Communication* 55 (4): 345–362. Crossref.
Warkentin, M., A. C. Johnston, E. Walden, and D. W. Straub. 2016. “Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination.” *Journal of the Association for Information Systems* 17 (3): 194–215. Crossref.
Weisman, S. 2008. *The Truth About Avoiding Scams*. Upper Saddle River: FT Press.
White, M. D., and C. Fisher. 2008. “Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts.” *Criminal Justice Policy Review* 19 (1): 3–24. Crossref.
Witte, K. 1991–1992. “The Role of Threat and Efficacy in Aids Prevention.” *International Quarterly of Community Health Education* 12 (3): 225–249. Crossref. PubMed.
Witte, K. 1992. “Putting the Fear Back Into Fear Appeals: The Extended Parallel Process Model.” *Communication Monographs* 59 (4): 329–349. Crossref.
Witte, K. 1994. “Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM).” *Communication Monographs* 61 (2): 113–134. Crossref.
Witte, K. 1998. “Fear as Motivator, Fear as Inhibitor: Using the EPPM to Explain Fear Appeal Successes and Failures.” In *The Handbook of Communication and Emotion*, edited by P. A. Anderson, and L. K. Guerrero, 425–450. New York: Academic Press.
Witte, K., and M. Allen. 2000. “A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns.” *Health Education & Behavior* 27 (5): 591–615. Crossref. PubMed.
Witte, K., K. A. Cameron, J. K. McKeon, and J. M. Berkowitz. 1996. “Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale.” *Journal of Health Communication* 1 (4): 317–342. Crossref. PubMed.
Witte, K., G. Meyer, and D. Martell. 2001. *Effective Health Risk Messages: A Step-by-Step Guide*. Thousand Oaks, CA: Sage Publications.
Wombat Security. 2018. “2018 State of the Phish.” https://www.wombatsecurity.com/state-of-the-phish.

Wood, R., and A. Bandura. 1989. “Social Cognitive Theory of Organizational Management.” *Academy of Management Review* 14 (3): 361–384. Crossref.
Workman, M., W. H. Bommer, and D. Straub. 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. Crossref.
Wright, R. T., and K. Marett. 2010. “The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived.” *Journal of Management of Information Systems* 27 (1): 273–303. Crossref.
Wurtele, S. K., and J. E. Maddux. 1987. “Relative Contributions of Protection Motivation Theory Components in Predicting Exercise Intentions and Behavior.” *Health Psychology* 6 (5): 453–466. Crossref. PubMed.
Yerkes, R. M., and J. D. Dodson. 1908. “The Relation of Strength of Stimulus to Rapidity of Habit-Formation.” *Journal of Comparative Neurology & Psychology* 18 (5): 459–482. Crossref.
Zulkosky, K. 2009. “Self-Efficacy: A Concept Analysis.” *Nursing Forum* 44 (2): 93–102. Crossref.