A Personality Based Model for Determining Susceptibility to Phishing Attacks

James L. Parrish, Jr.

University of Arkansas at Little Rock, 2801 S. University Ave., Little Rock, AR 72204-1099
Phone: 501-569-3293 Fax: 501-683-7021
jlparrish@ualr.edu

Janet L. Bailey

University of Arkansas at Little Rock, 2801 S. University Ave., Little Rock, AR 72204-1099
Phone: 501-569-8851 Fax: 501-683-7021
jlbailey@ualr.edu

James F. Courtney

Louisiana Tech University, P.O. Box 10318, Ruston, LA 71272
Phone: 318-257-3804
Courtney@latech.edu

ABSTRACT

Phishing is a type of social engineering attack that attempts to gain information from a computer user by sending a message under the guise of a trustworthy entity. These attacks have been increasing at an alarming rate and cause damage to both individuals and organizations. Recent research has determined that some individuals are more apt to fall prey to these types of attacks than others. This paper seeks to further examine the reason by proposing a conceptual framework that utilizes the Big-Five personality traits as a possible way to explain why some people are more susceptible than others to phishing attacks.

INTRODUCTION

Social engineering attacks are security exploits that prey on the vulnerable attributes of humans rather than of technology. They stem from the fact that some criminals have found it easier to obtain the information needed to execute illegal activities from the people that operate the computers via some sort of social interaction than it is from the computers themselves (Microsoft Corporation, 2007; Winkler & Dealy, 1995). These attacks can come in many forms ranging from telephone calls under the guise of a help desk technician or other entity that needs the

information to "assist" them in some way to sending out massive amounts of email requesting information from what appears to be a legitimate sourcesuch as a bank or Internet service provider.

A recent Gartner Group study has revealed that 19% of respondents admitted to clicking on links in phishing emails, and 3% of the respondents gave up personal information to the attackers (Jagatic, Johnson, Jakobsson, & Menczer, 2007). Even groups of experienced Internet users have shown that they are vulnerable to these types of attacks. For example, recent research by Bailey and Jensen (2008) found that college students were alarmingly susceptible to email phishing attacks. Their findings are important because college students are for the most part computer literate and should have awareness of these types of social engineering exploits.

Regardless of how the attacks come, they all seem to target certain human traits to gain access to the desired information. This leads to the question posed in this study: What qualities make some individuals more susceptible to phishing attacks than others? Recent work using behavior constructs found that persons high in normative commitment feel more obligated to give up information when offered something in exchange. The same study also found that individuals with different personality traits were more receptive to different lures. For example, an individual who exhibits greater tendencies to obey authority might be more susceptible to a scam purporting to be from a financial institution whereas someone more focused on greed and fear of a missed opportunity might be more receptive to a scam that appears to be a "first-come first-serve" offer such as one from a young woman who needs help getting her family's fortune out of her country before it is taken from her (Workman, 2008).

This research examines the phishing issue further by proposing a framework that links the level of social engineering security-exploit susceptibility to an individual's personality traits. The benefit of this type of holistic view is that it provides the mechanism to potentially reveal relationships responsible for user behavior.

Openness, conscientiousness, extraversion, agreeableness, and neuroticism are frequently referred to as the "Big-Five" personality traits (Gosling, Rentfrow, & Swann Jr., 2003). Numerous studies have used these traits as a predictor for human behavior with high validity. The framework presented in this paper proposes the Big-Five as an applicable lens from which to study the phenomena of phishing susceptibility.

PHISHING: NATURE AND VICTIMS

Jagatic, Johnson, et. al. (2007, p. 94) define phishing as "a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity." These attacks usually come in the form of an email that is transmitted to many different individuals that are unknown to the attacker under the guise of a notice from a large financial institution, online marketing firm, or a popular email site. Despite the fact that the attacker does not actually know whether or not individual victims are actually affiliated with the supposed "sender", the sheer volume of emails transmitted coupled with the immense

popularity of the "sender" allows the attacker to reach many targets that are (Jagatic, Johnson, Jakobsson, & Menczer, 2007). Attacks are not always of such a blanket nature however. Context aware phishing is a more sophisticated type of phishing attack whereby the attacker gains knowledge of the actual sites a victim visits and bases their attack on that knowledge. This type of attack is much more effective in gaining information from the victim (Robila & Ragucci, 2006). In fact some studies that leveraged social context have reported success rates of 70-80% (Jagatic, Johnson, Jakobsson, & Menczer, 2007; Robila & Ragucci, 2006).

Regardless of the context, most phishing attacks have three components: the hook, the lure and the catch. The hook is the legitimate looking email form, website, or mechanism that the phisher uses to collect confidential information. The lure is the social engineering incentive the phisher uses to trick the potential victim into providing them with the desired information. Finally, the catch is the information acquired in the attack that the criminal can then capitalize on (Jakobsson & Myers, 2007). The fact that phishing and other similar forms of social engineering attacks leverage how humans interact with technology makes this area a rich avenue of research in which, to date, exploration has just begun.

Phishing is big business. The first six months of 2008 saw a 47 percent increase in the number of phishing attacks (Websense Security Labs, 2008) – a frightening statistic when taking into account the fact that $3.2 billion was lost to phishing in 2007 (Litan, 2007) up $500 million from 2006 (Keizer, 2007). Furthermore, phishing attacks were listed as the top cyber security incident for the first three quarters of the 2008 fiscal year. Table 1 shows the percentage of incident types reported to United States Computer Emergency Readiness Team (US-CERT) for this time period.

Type of Incident	Q1	Q2	Q3
Phishing	45%	72.5%	76.3%
Non Cyber	10.9%	5.4%	5.3%
Malicious Web Site	9.4%	4.5%	4.2%
Policy Violation	9.4%	4.4%	3.7%
Equipment Theft/Loss	7.1%	3.8%	2.9%
Other	18.2%	9.4%	7.5%

Table 1: Percentage of Incidents Reported to US-Cert in FY'08 (United States Computer Emergency Readiness Team, 2008).

One of the major reasons phishing attacks have become so popular is the high ROI to criminals. An investment of less than $200 will allow a criminal to send tens of thousands of emails. With a response rate of as little as 1 percent, the criminal stands to net hundreds of thousands of

dollars (Singh, 2007). In fact, although the overall damages resulting from phishing are not as large as that of viruses or spyware, the average amount of damage to the victim exceeds those damages eight times over (Singh, 2007). Additionally in cases where acquired information allows a phisher to fraudulently obtain funds from a victim's bank or credit card account(s), the financial institutions are often left covering much of the monetary damages incurred (Bailey, Mitchell, & Jensen, 2008). This makes phishing not only an individual problem, but an organizational problem as well with a ripple effect of higher costs to consumers as the institutions attempt to cover expenses caused by losses.

In addition to the direct monetary costs associated with the attack, there are also indirect costs such as the time and effort spent to reclaim one's identity. These costs also spill over to organizations in the form of increased calls to customer service, changing login credentials, freezing and recreating accounts, and investigations to ensure that a phishing attack did indeed take place (Jakobsson & Myers, 2007). Organizations must also deal with the opportunity costs of phishing attacks in the form of suspicion or refusal to use online services. If customers of an organization refuse to use online services out of the fear of phishing, then the organization has no choice but to have staff that might not be otherwise needed in the absence of this fear, available to service their customers (Jakobsson & Myers, 2007).

Phishing susceptibility is defined in this study as the likelihood that a person will respond to a phishing attack. Recent research has revealed differences in the types of people that fall prey to phishing attacks. For example, Bailey, Mitchell and Jensen (2008) found in a study of student vulnerabilities to phishing that female students were more susceptible than their male counterparts and students that had jobs were less susceptible to the attacks than those that attended university classes full-time. Differences responses to phishing between sexes were also found in an Indiana University study that used social context methods to gain information about student victims. The Indiana study also found females were more susceptible than males. However, it also found if the message was from a member of the opposite sex, the likelihood of the success of the attack increased. This effect was more pronounced in males than females (Jagatic, Johnson, Jakobsson, & Menczer, 2007). The study also found that much of the success was achieved in the first twelve hours after the message was sent and there were significant differences in vulnerability rates between students in different courses of study (Jagatic, Johnson, Jakobsson, & Menczer, 2007).

How can we account for these differences in individuals? Personality researchers have determined that males and females have gender differences in personality traits (Costa Jr., Terracciano, & McCrae, 2001). A difference in the time the majority of the success was achieved suggests a possible link to other personality-related factors. Additionally, the fact that attacks in a social context are more successful may also relate to the personality of the victim.

FRAMEWORK DEVELOPMENT

The Big-Five framework is one of the most widely used models for personality and has considerable support amongst personality researchers (Gosling, Rentfrow, & Swann Jr., 2003).

The model consists of five broad, bipolar factors that represent personality at the highest level of abstraction that proponents of the model believe can classify differences in the personalities of individuals. These factors summarize more specific facets which are themselves made up of traits (Gosling, Rentfrow, & Swann Jr., 2003).

The five broad personality domains are Neuroticism, Extraversion, Openness to experience, Agreeableness, and Conscientiousness. Neuroticism is the tendency to feel that reality is a problem and to experience readily unpleasant emotions. People that possess high levels of neuroticism are generally sad and sometimes hot tempered (Rolland, 2002; Weiner & Greene, 2008). Extraversion is the tendency to seek out the company of others and reflects energy and positive emotions in one's personality. Extraverted personalities often seek excitement and tend to be dominant (Rolland, 2002; Weiner & Greene, 2008). Openness is the desire to seek out new experiences without anxiety and an appreciation of different ideas and beliefs. Individuals that exhibit high levels of openness revel in fantasy and appreciate art and nature (Rolland, 2002; Weiner & Greene, 2008). Agreeableness is a measure of the quality of the relationships a person has with others. If a person has a high level of agreeableness, they are compassionate and cooperative rather than antagonistic and suspicious. They believe that people they interact with are generally good intentioned and honest (Rolland, 2002; Weiner & Greene, 2008). Finally, conscientiousness focuses on self-discipline, dutiful action, and a respect for standards and procedures. These people are known for their prudence and common sense (Rolland, 2002; Weiner & Greene, 2008). The five domains and the facets corresponding to them are found in Table 2.

Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Fantasy	Competence	Warmth	Trust	Anxiety
Aesthetics	Order	Gregariousness	Straightfor-wardness	Hostility
Feelings	Dutifulness	Assertiveness	Altruism	Depression
Actions	Achievement Striving	Activity	Compliance	Self-Consciousness
Ideas	Self-Discipline	Excitement Seeking	Modesty	Impulsiveness
Values	Deliberation	Positive Emotion	Tender-mindedness	Vulnerability to Stress

Table 2: Facets and Domains of the NEO PI-R Personality Inventory (Costa and McCrae, 1985).

The framework presented in this paper leverages the Big-Five personality factors to explain the differences found in current empirical literature between types of individuals with regards to their susceptibility to phishing attacks and to provide a structure for future research. The framework consists of four main groups of factors: personal, experiential, personality profile, and phishing susceptibility. In phishing studies, the personal and experiential factors contain

aspects that reveal differences in individuals with regards to the success or failure of phishing attacks.

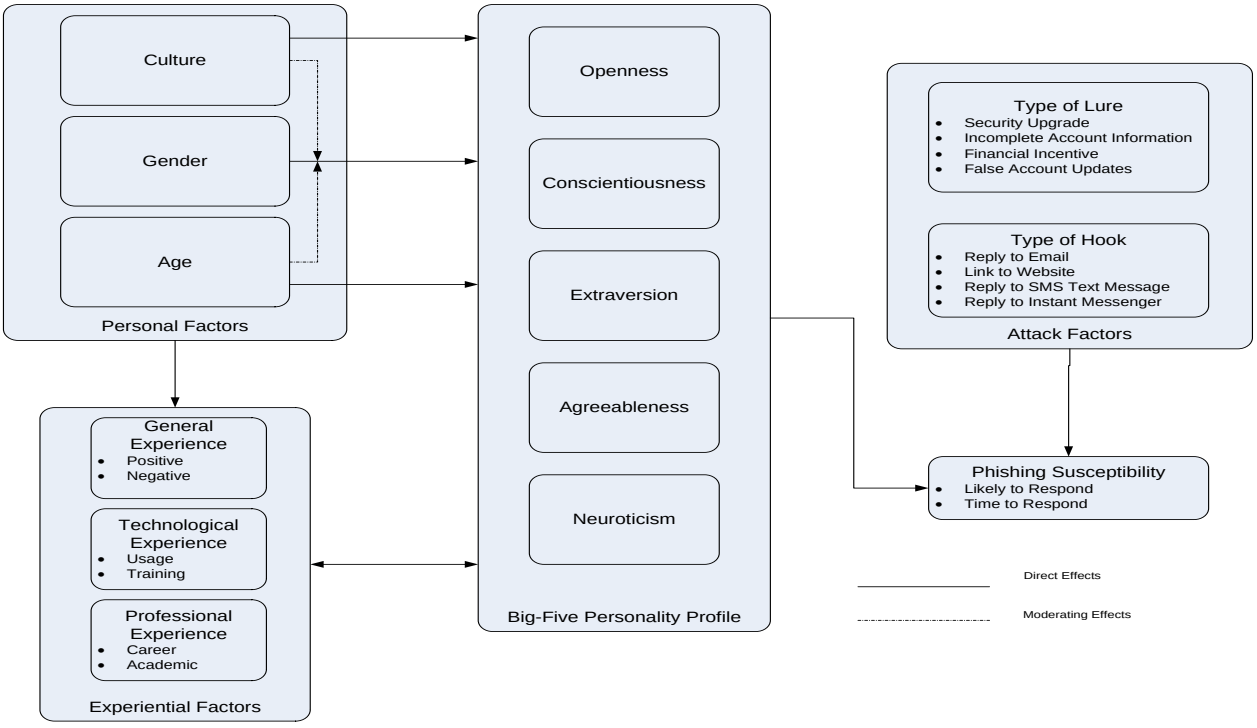

Figure 1: Phishing Susceptibility Framework

Personal factors are those that either cannot be changed or are extremely difficult to change and include gender, culture, and age. Experiential factors are those that shape an individual's personality because of a past event or experience. The Big-Five personality profile classifies the personality differences of individuals among five broad factors as previously discussed. The framework proposes that each of these factors has a role to play with regards to the susceptibility of an individual to a phishing attack.

Some of the factors also affect the development of other factors. For example, personal factors directly influence the types of experience an individual may have. Certain attributes of the personal factors also affect the relationship other personal factors have on the Big-Five personality traits. Prior studies have shown that age and culture both have moderating effects on the development of personalities in the different genders (Costa Jr., Terracciano, & McCrae, 2001; Srivastava, John, Gosling, & Potter, 2003; Rolland, 2002).

Regardless of their effects on each other, both personal and experiential factors play a play in the development of personality. Some of the effect is biological and can be related to the individual's gender or age, while some is environmental and can be related to the experiences of the individual and the culture in which they are immersed.

Personal Factors

As mentioned earlier in this paper, multiple studies (Bailey, Mitchell, & Jensen, 2008; Jagatic, Johnson, Jakobsson, & Menczer, 2007) have found a difference in susceptibility to phishing attacks between males and females which could be related to personality differences between the genders. In a study of over 23,000 participants across multiple studies, females scored consistently higher in Neuroticism and Agreeableness than their male counterparts. There was no consistent difference with regards to Openness, Extraversion, and Conscientiousness (Costa Jr., Terracciano, & McCrae, 2001).

Culture has also been found to have an impact on the personality traits of individuals. In an examination of cross-cultural generalizability of the Big-Five traits across 16 cultures, one study found that Agreeableness and Extraversion were found to be sensitive to the cultural background of the individual, while Neuroticism, Openness and Conscientiousness were fairly generalizable (Rolland, 2002). Additionally, personality differences have been found to be more pronounced in cultural settings where traditional sex roles were minimized (Costa Jr., Terracciano, & McCrae, 2001).

One phishing study found that older students were less likely to fall prey to phishing attacks than younger ones (Bailey, Mitchell, & Jensen, 2008). It was once believed that the "hard plaster" theory of personality held true where personality traits became fixed after age 30. Recent studies, however, have shown that our personalities do change beyond this age. Another study by Srivastava, Gosling, and Potter (2003) found that Conscientiousness and Agreeableness changed through early and middle adulthood. They also found that Neuroticism declined in females over time, while staying relatively stable in males. They report that their findings could be attributed to a variety of developmental influences such as experience in different areas that correlate with attainment of certain ages.

Experiential Factors

Sometimes life experiences result in personality changes, such as getting a more responsible job that causes an individual to become more conscientious to meet the requirements of the new situation. Alternatively, a change in conscientiousness brought on by maturity may cause the individual to seek the experience of a more responsible job (Srivastava, John, Gosling, & Potter, 2003). Many experiences are affected by age, such as individuals in early adulthood entering the workforce and climbing the corporate ladder, those starting families and others at an age where they may be looking at retirement. There are three main categories of experiential factors: general experiences, technological experiences, and professional experiences.

General experiences are those not related to an individual's encounters with technology or their profession. These experiences could be positive, such as having children, an event that has been shown to promote Agreeableness (Srivastava, John, Gosling, & Potter, 2003). They can also be negative, such as being victimized by a scam or going through a difficult financial position. While there is no empirical evidence at this time to link negative experiences directly

to personality, research shows prior victimization to scam attacks does decrease certain aspects of an individual's vulnerability to susceptibility to subsequently falling prey when examined through the lens of consumer behavior (Workman, 2008). This suggests negative experiences may have a negative impact on Agreeableness as well as on phishing susceptibility.

Technological experience includes prior technological use as well as training in the proper use of technology. Training is one of the main countermeasures against social engineering and phishing attacks and, one would hope, be negatively correlated with phishing susceptibility. In the sense of experiential effects on personality, a properly trained individual should be more suspicious of incoming emails which could, in turn, have a negative effect on the Agreeableness of the individual in the computing context or could lead to a sense of paranoia about email thus having a positive effect on Neuroticism.

Neuroticism may also have an effect on the technological experience of the individual as it has been linked to computer anxiety (Woszczynski, Roth, & Segars, 2002). Those with computer anxiety may not have the same types of experiences with technology that persons with less anxiety may have. Openness also has impacts on technological experience in that it has been correlated with the optimum stimulation level (OSD) of individuals. Persons with higher OSD levels are more exploratory and thus spend more time engaging in exploratory behaviors with technology to reach their level of optimum stimulation (Woszczynski, Roth, & Segars, 2002).

Professional experience in this framework includes experiences that are associated with the individual's career, professional or academic. Differences in professional and academic experience have been shown to correlate with phishing susceptibility. Professionally, this is seen in studies that show that students who worked full-time were less susceptible to phishing than their counterparts (Bailey, Mitchell, & Jensen, 2008). In the academic sense, studies show that some academic disciplines are more susceptible to phishing than others (Jagatic, Johnson, Jakobsson, & Menczer, 2007).

As previously stated, the impact of professional experience can be seen in its effects on, and how it is affected by, Conscientiousness. The relationship could be posited as a transactional one where an individual's level of Conscientiousness causes them to seek out (or avoid) professional experiences that reinforce (or break down) that same individual's level of Conscientiousness (Srivastava, John, Gosling, & Potter, 2003).

The Big-Five Personality Traits

As stated earlier, the Big-Five model classifies the personality differences of individuals among five broad factors. This research framework proposes that each of these factors has a role to play with regards to an individual's susceptibility to a phishing attack.

Openness

Openness is relevant on two fronts dependent on which aspects of Openness the person exhibits most. On one hand, the technological experience and computer proficiency that has been hypothesized by Woszczynski, Roth, and Segars (2002) to be associated with Openness could lead to reduced susceptibility to phishing attacks. However, a general openness to all experiences and a tendency toward fantasy could play right into the criminal's hands. Especially considering many of the lures that are used in phishing attacks could have come right out of a Hollywood movie (i.e. the disposed dictator that needs your help to claim his fortune).

Conscientiousness

Conscientiousness may be the personality trait most negatively correlated with phishing vulnerability, especially for those individuals that have had some training in security or for those that have workplace policies in place designed to curb phishing – assuming those policies have been communicated. It stands to reason that the higher levels of Conscientiousness would result in individuals more likely to follow training guidelines and less likely to break security policies. There is support for this position in a study by Salgado (2002) that found low levels of Conscientiousness predicted deviant workplace behavior such as breaking rules, or behaving irresponsibly.

Extraversion

Extraverted persons wish to surround themselves with others and to be the center of attention. While generally this is a positive trait, in the context of phishing it can lead to increased vulnerability. The literature supports this assertion. Workman (2008) found that high affective commitment, which can be roughly equated to Extraversion, led to people giving up sensitive information because they wanted to gain acceptance or to belong to some social group while Weirich and Sasse (2001) found that people that did not disclose their passwords were thought of as unsociable and not team players.

Agreeableness

If Conscientious is the personality trait least associated with phishing vulnerability, then Agreeableness is possibly the personality trait that is most associated with it. When divulging information to a phisher, trust is generally the key criterion for doing so (Weirich & Sasse, 2001). Trust is one of the facets of Agreeableness. Other facets of this domain also targeted directly by phishers include altruism (the email from the dying lady that needs your information to access her money to give aid to the poor) and compliance (the email from the bank that says you need to provide information about your account or it will be frozen).

Neuroticism

Neuroticism may get an underserved reputation as a personality trait that is always negative. One study in particular showed that people with negative self-images and self admitted paranoia were more inclined not to share their personal information in some circumstances. This could be because they feel that they could be considered a suspect in the event a breach in security did happen (Weirich & Sasse, 2001). The association that Neuroticism has with computer anxiety may also prove to help protect the individual in regards to phishing. If computer anxiety has reduced their technical experience then they may be less likely to be online or have fewer online accounts than less neurotic counterparts. This is important because most phishing attacks achieve success within 12 hours of the time the attack is deployed (Jagatic, Johnson, Jakobsson, & Menczer, 2007) leading to the possibility people who are online more frequently are more vulnerable by default.

Attack Factors

The attack factors portion of the framework is comprised of two dimensions. The "type of lure" dimension encompasses the various social engineering lures that criminals use to attract the victim. The "type of hook" is related to the vehicle the criminal uses to collect the information. Collectively, these factors and the Big-Five personality profile influence an individual's phishing susceptibility – in both the likelihood of and time to be caught.

Phishing Susceptibility

Phishing susceptibility is examined along two dimensions. The first dimension is the likelihood that an individual will respond to a phishing attack by being lured in and interacting with the hook. The second dimension, time to respond, is a measure of the time that it will take for a person to interact with the hook.. This dimension is important because the majority of people that fall prey to phishing attacks do so within twelve hours of receiving the lure. As the time period between receiving the lure and interaction with the hook increases, so does the probability that the hook has been subject to a *takedown*, the process of rendering a hook non-operational (Jagatic, Johnson, Jakobsson, & Menczer, 2007; Jakobsson & Myers, 2007). In the event of a takedown, the potential to gain information from the victim is greatly diminished.

CONCLUSION

Phishing is one of the most widespread security threats today. It causes damage to both individuals and organizations in the form of monetary damages, indirect costs, and opportunity costs. Unlike security threats that can be mitigated primarily through the use of technology, phishing and other social engineering exploits require intervention on the human level as well. Effective intervention on this level requires not only understanding of the technology used in the attack, but also understanding of the roles individuals and organizations play in the success or failure of the attack. MIS researchers are in a position to make a significant contribution in the

fight against these types of exploits. The Big-Five personality traits have proven useful in many areas arenas for predicting different aspects of human behavior. Their validity in the context of predicting an individual's susceptibility to various forms of phishing attacks is still unclear and will require further research. The purpose of the framework proposed in this paper is to provide a structure to assist researchers in their quest for answers. Reasons for susceptibilities need to be identified before effective measures to mitigate those vulnerabilities can be taken.

REFERENCES

Bailey, J., Mitchell, R., & Jensen, B. (2008). Analysis of Student Vulnerabilities to Phising. *Proceedings of the Fourteenth Americas Conference on Information Systems* (pp. 1-10). Toronto: Association of Information Systems.

Barrick, M., & Mount, M. (2005). Yes, Personality Matters: Moving on to More Important Matters. *Human Performance , 18* (4), 359-372.

Costa Jr., P., Terracciano, A., & McCrae, R. (2001). Gender Differences in Personality Traits Across Cultures: Robust and Surprising Findings. *Journal of Personality and Social Psychology* , 322-331.

Costa, P., & McCrae, R. (1992). *NEO PI-R professional manual.* Odessa: Psychological Assessment Resources.

Dunn, W., Mount, M., Barrick, M., & Ones, D. (1995). Relative Importance of Personality and General Mental Ability in Managers' Judgments of Applicant Qualifications. *Journal of Applied Psychology* , 500-509.

Emigh, A. (2005, October). *Online Identity Theft: Phishing technology, chokepoints, and countermeasures.* Retrieved October 10, 2008, from ITTC Report on Online Identity Theft Technology and Countermeasures: http://www.anti-phishing.org/Phishing-dhs-report.pdf

Gosling, S., Rentfrow, P., & Swann Jr., W. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in Personality* , 504-528.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM* , 94-100.

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

Keizer, G. (2007, 12 18). *Phishers pinch billions from consumer' pockets.* Retrieved 2 25, 2008, from Computerworld UK: www.computerworlduk.com/management/security/cybercrime/news-analysis/index

Litan, A. (2007). *Phishing attacks escalate, morph and cause considerable damage.* ".

Microsoft Corporation. (2007, January 16). *What is social engineering?* Retrieved October 5, 2008, from Social Engineering, Phishing, and Email Hoaxes - Microsoft Security: http://www.microsoft.com/protect/yourself/phishing/engineering.mspx

Robila, S. A., & Ragucci, J. W. (2006). Don't be a phish: steps in user education. *ACM SIGCSE Bulletin* , 237-241.

Rolland, J.-P. (2002). The Cross-Cultural Generalizability of the Five Factor Model of Personality. In R. McCrae, & J. Allik, *The Five-Factor Model of Personality Across Cultures* (pp. 7-28). New York: Springer.

Rubin, A. d. (2002). Security considerations for remote electronic voting. *Communications of the ACM* , 39-44.

Salgado, J. (2002). The Big Five Personality Dimensions and Counterproductive Behaviors. *International Journal of Selection and Assessment* , 117-125.

Saulsman, L., & Page, A. (2004). The five-factor model and personality disorder empirical literature: A meta-analytic review. *Clinical Psychology Review* , 1055-1085.

Singh, N. (2007). Online Frauds in Banks with Phishing. *Journal of Internet Banking and Commerce* , 1-27.

Srivastava, S., John, O., Gosling, S., & Potter, J. (2003). Development of Personality in Early and Middle Adulthood: Set Like Plaster ofr Persistent Change? *Journal of Personality and Social Psychology* , 1041-1053.

United States Computer Emergency Readiness Team. (2008, February 20). *Quarterly Trends and Analysis Report.* Retrieved October 14, 2008, from US-CERT Publications: http://www.us-cert.gov/press_room/trendsandanalysisQ108.pdf

United States Computer Emergency Readiness Team. (2008, May 28). *Quarterly Trends and Analysis Report.* Retrieved October 14, 2008, from US-CERT Publications: http://www.us-cert.gov/press_room/trendsandanalysisQ208.pdf

United States Computer Emergency Rediness Team. (2008, August 25). *Quarterly Trends and Analysis Report.* Retrieved October 14, 2008, from US-CERT Publicatons: http://www.us-cert.gov/press_room/trendsandanalysisQ308.pdf

Vollrath, M., & Torgersen, S. (2003). Who takes health risks? A probe into eight personality types. *Personality and Individual Differences* , 1185-1197.

Websense Security Labs. (2008). *State of Internet Security.* http://www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf: Websense.

Weiner, I., & Greene, R. (2008). *Handbook of Personality Assessment.* Hoboken: John Wiley & Sons.

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: a first step towards effective password security in the real world. *Proceedings of teh 2001 workshop on New Security paradigms* (pp. 137-143). Cloudcroft: ACM.

Winkler, I. S., & Dealy, B. (1995). Information Security Technology?...Don't Rely on It: A Case Study in Social Engineering. *Proceedings of the Fifth USENIX UNIX Security Symposium* (pp. 1-6). Salt Lake City: USENIX.

Workman, M. (2008). Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society of Information Science and Technology* , 662-674.

Woszczynski, A., Roth, P., & Segars, A. (2002). Exploring the theoretical foundations of playfulness in computer interactions. *Computers in Human Behavior* , 369-388.