COMBATTING CYBER SOCIAL ENGINEERING IN THE DIGITAL AGE

A Master Thesis

Submitted to the Faculty

of

American Military University

by

Nicholas Ryan McLarty

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

November 2017

American Military University

Charles Town, WV

DEDICATION

I dedicate this thesis to my parents, my wife, and my daughter. Without their encouragement, support, sacrifice, understanding, and love, I would not have been able to accomplish this momentous achievement of my life.

ACKNOWLEDGEMENTS

I wish to thank the faculty of the American Public University System, and in particular Dr. Ronald Booth, for their wonderful guidance and support throughout this program. The cybersecurity studies graduate program has been an excellent experience and has provided directly relevant knowledge that I will use for many years to come.

I would also like to express my gratitude to the Texas A&M University System, Texas A&M Transportation Institute, and my supervisor, Bradley Hoover. Their unwavering support of my desire to pursue a master's degree has greatly facilitated this opportunity for me, and the daily work experience I have gained directly contributed to my success in this degree program.

ABSTRACT OF THE THESIS

COMBATTING CYBER SOCIAL ENGINEERING IN THE DIGITAL AGE

by

Nicholas Ryan McLarty

American Public University System, September 16, 2017

Charles Town, West Virginia

Dr. Ronald Booth, Thesis Professor

Efforts made to reduce or eliminate the threat of social engineering have not been effective in addressing the lack of security awareness exhibited by users of cyber resources. Success combatting social engineering attacks requires a new approach to user education and improvements to anti-social engineering technology. This study incorporates existing research with surveys designed to identify trends of online Internet behavior and defensive posture from social engineering attacks. The research found that cultures which promote trusting and open social relationships are the most vulnerable,

while skeptical individuals will be more likely to detect or avoid a social engineering attack. The research also found younger subjects exhibit online Internet behaviors that place them at greater risk, and social engineering prevention training in the enterprise does not translate easily to the personal setting. Recommendations include training specific to social engineering, delivered regularly and in small doses rather than one large course annually, and educating users to recognize the tactics employed by social engineers. Additional emphasis must be placed on mobile device security and researching new avenues for delivery of social engineering prevention training.

Table of Contents

Introduction....1
Background of the Study....1
Statement of the Problem....2
Definition of Key Terms....3
Theoretical Framework....4
Hypotheses....4
Literature Review....6
Introduction....6
Correlation between human behavior and susceptibility to social engineering attacks....8
Workplace social engineering prevention and training challenges to individual protection against social engineering attacks....13
Better methods or delivery mechanisms for social engineering prevention....19
Research Methodology....26
Research Questions....26
Identification and Operationalization of Variables....27
Population and Sampling Plan....28
Data Collection/Sources....29
Summary of Analysis Procedures....29
Limitations of the Study....29
Assumptions....30
Results of the Study....31

Objective Results....31
Subjective Results....37
Significance and Interpretation of Results....48
Gender....48
Age Range....51
Level of Education....51
Discussion....55
References....58

List of Tables

Table 1. Survey responses by desktop/laptop anti-malware product.....36

Table 2. Survey responses by mobile anti-malware product.....36

List of Figures

Figure 1. Survey response distribution by age range 31
Figure 2. Survey response distribution by gender 32
Figure 3. Survey response distribution by average online Internet usage 32
Figure 4. Survey response distribution by highest level of education 33
Figure 5. Survey response distribution by location/method of accessing the Internet 34
Figure 6. Survey response distribution by location/method of accessing email 35
Figure 7. Heat map of survey responses to PayPal phishing email 38
Figure 8. Heat map of survey responses to realty company notice to vacate 39
Figure 9. Heat map of survey responses to PayPal phishing website 40
Figure 10. Survey response distribution by actions in response to phishing email in work/school mailbox 41
Figure 11. Survey response distribution by actions in response to phishing email in home/personal mailbox 42
Figure 12. Survey response distribution by actions in response to accessing a phishing website at work/school 43
Figure 13. Survey response distribution by actions in response to accessing a phishing website at home 44
Figure 14. Survey response distribution by actions in response to disclosing a password to a phishing website at work/school 45
Figure 15. Survey response distribution by actions in response to disclosing a password to a phishing website at home 46
Figure 16. Survey response distribution by self-evaluated level of computer competency 47

Figure 17. Survey response distribution by previous formal instruction in social engineering prevention/protection.....47

Figure 18. Survey response distribution by level of comfort to respond appropriately to a social engineering attack 48

Figure 19. Survey response distribution by amount of time spent online in an average week, by gender 49

Figure 20. Survey response distribution by location/method of accessing the Internet, by gender 50

Figure 21. Survey response distribution by amount of time spent online in an average week, by level of education 52

Figure 22. Survey response distribution by desktop/laptop anti-malware product, by level of education.....53

Figure 23. Survey response distribution by mobile anti-malware product, by level of education.....53

Combatting Cyber Social Engineering in the Digital Age

Introduction

Background of the Study

Despite the attention and investment into educating users of consumer and enterprise information technology about the persistent threats stemming from social engineering by malicious actors, social engineering continues to be one of the most effective means of exploiting users and infiltrating systems for nefarious purposes. While a balanced strategy of addressing an organization's approach to systems security and introducing modern technologies can reduce the effectiveness of malicious actors to compromise an organization via social engineering, the human element will remain one of the most vulnerable elements of a cyber network should any social engineering campaigns circumvent an organization's technical controls.

Enterprises and similar organizations with mature internal information technology departments may employ the necessary tools and training to protect and educate users against social engineering as a matter of sound business practice. However, in the case of consumers and small to medium businesses, the organization providing the user's cyber connectivity (typically an Internet service provider) may use varying degrees of protection through strategies such as content blocking and spam filtering, but is not under any obligation to do so, and rarely will provide tools and training directly to users. Therefore, the baseline for human-centric social engineering protection across a population is particularly low when considering the lowest common denominator of exposure to social engineering awareness campaigns.

Statement of the Problem

The summary of a 2016 Herjavec Group report on the subject of social engineering and cybercrime states "a common thread [of] this entire report is a lack of security awareness on the part of corporate executives, small business owners, employees at organizations of all sizes, and consumers" (Morgan, 2016). It is clear that social engineering awareness measures to date have not been wholly successful at thwarting social engineering, and further research is necessary to tackle this challenge, specifically addressing the human element, in a fashion that can scale to all users of cyber resources.

While most Internet search results for social engineering point to news or resources relating to businesses, very little can be found about how to protect yourself as an individual against such attacks. An average company with 10,000 employees spends $3.7 million per year addressing phishing attacks (Ponemon Instiute, LLC, 2015), while the investment in protecting individuals from social engineering is either at their own expense or provided as a common good by service providers. The result includes users falling victim to ransomware at a sum of over $24 million in 2015 (Turkel, 2016), compromising credit card and other financial information, or revealing login information to sensitive websites such as online banking or payroll that can result in the diversion of money into the criminal's control. In nearly all of these cases, a social engineering tactic provided the attackers with the opportunity to exploit the victim.

If users are to be better protected from social engineering attacks, an improved and consistent approach by which users are informed of legitimate requests for information, trained to recognize malicious solicitation, and equipped to protect themselves before, during and after social engineering attacks is necessary to mitigate this enduring threat.

Definition of Key Terms

Enterprise information technology--hardware and software designed to meet the demands of a large organization (Rouse & Wigmore, 2013).

Internet service provider--a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting (Rouse, 2006).

Malicious actor--an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security (Rouse & Wigmore, 2016).

Phishing--a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels (Rouse & Cobb, 2015).

Ransomware--malicious code that is used by cybercriminals to launch data kidnapping and lock screen attacks (Rouse, 2016).

Spear phishing--an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information (Rouse & Bacon, 2017).

Social engineering--(as applied to cybersecurity) an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures (Rouse & Bacon, 2016).

Theoretical Framework

Social engineering is defined as the "application of principles, techniques, methods, and findings of social sciences to the solution of identified social problems, especially with respect to effecting change" (Chumbow, 2012). Chumbow (2012) goes on to define social engineers as "one who tries to influence popular attitudes, social behaviors, and resource management on a large scale." With these two definitions applied to the context of a cyber actor engaging in a manipulative enterprise, a cyber social engineer can be construed as "one who applies principles, techniques, methods, and findings of social sciences to effect change in the furtherance of their goals."

During a keynote speech at InfoSec Europe 2016, Dr. Jessica Barker attributed the success of social engineering attacks (while noting that phishing attacks are at a 12-year high) to elements of human nature such as reciprocity, social obligation, curiosity, naivety, overconfidence, and narcissism (Barker, 2016). This study theorizes that because social engineering leverages fundamental human behavior to be successful, there is a natural limit to how effective technical solutions can be in deterring these attacks. Additionally, there is resistance in training users to disregard natural instincts in an attempt to prevent social engineering.

Given the dependence of social engineering attacks on natural human behavior, this study intends to prove the following hypotheses:

Hypotheses

H1. Social engineering attacks are effective because the engineers exploit their victims' emotions and behaviors to elicit a favorable response.

H2. Younger age groups of online Internet users have a higher susceptibility to social engineering attacks because of their more limited life experience and developed risk-based decision-making.

H3. Young and mid-aged professionals, and Internet users with a higher regular utilization of online services are less susceptible to social engineering attacks because of their recent and frequent exposure to modern technology and awareness of common issues affecting users on the Internet.

H4. Workplace training on social engineering prevention does not reduce susceptibility to personal social engineering attacks because users are not regularly trained to correlate risks in the workplace with personal risk and to apply the same level of scrutiny in their personal social interactions as they do in the workplace.

Literature Review

This study aims to analyze existing research on the subject of social engineering awareness and current practices for educating users of social engineering tactics and strategies for protecting themselves, and to explore options for improving the technical and human measures employed to minimize exposure to social engineering attacks. This literature review will examine various sources of existing research, industry best practices, training material, and other publicly available information relating to social engineering and its prevention. After exploring previous literature on the subject, gaps will be identified and discussed.

Introduction

Many online resources on the subject of social engineering are tailored for corporate organizations as a means to protect the organization from risk exposure caused by social engineering (see PCI Security Standards Council, LLC, 2015; Ponemon Instiute, LLC, 2015; Rader & Rahman, 2015). Few organizations, primarily non-profit and governmental, provide awareness resources for "protecting yourself online" (see Center for Cyber Safety and Education, 2017; U.S. Department of Homeland Security, 2017), but those resources often fall short by briefly highlighting common indicators of social engineering and then move on to other protective measures.

Of the various types of social engineering attacks, phishing and spear phishing are among the most popular with phishing attacks at a 12-year high (Barker, 2016), and is consistently a leading vector in cyberattacks and online identity theft (Gharibi, 2012). Social engineering has also been observed on social media sites (Algarni, Xu, Chan, & Tian, 2013), as they are a treasure trove of information on potential victims, particularly when the default privacy settings

are in place (Wilcox & Bhattacharya, 2015), as well as via the Short Message Service (SMS) on mobile phones (Rader & Rahman, 2015).

"Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels" (Rouse & Cobb, 2015), whereas a spear phishing email is crafted for and sent to an individual or small group of recipients. Spear phishing emails also contain more specific, contextual information that is intended for the recipient, such as information relating to personal or business interests, as a means to successfully capture the victim's attention and solicit a response to the phishing attack (Rouse & Bacon, 2017). Phishing attacks are perpetrated by criminals of financial crimes, corporate spies stealing proprietary information, and hacktivists to draw attention their cause (Butavicius, Parsons, Pattinson, & McCormac, 2016).

Phishing attacks manipulate recipients into providing information or access to an information system (Butavicius et al., 2016; Dhinakaran, Nagamalai, & Lee, 2011) while allowing the attacker to bypass technical controls that would otherwise prevent them from gaining remote access to that system (Rader & Rahman, 2015). Phishing attacks may be used to compel a victim to disclose sensitive personal information such as a password, or inadvertently provide access to a computer or network through acquired malware delivered as part of the phishing attack (Butavicius et al., 2016), and they are always done remotely allowing the attacker to remain anonymous and relatively free from risk of prosecution (Rader & Rahman, 2015; Wilcox & Bhattacharya, 2015).

Depending on the nature and target, phishing attacks often result in the loss of proprietary information (commonly referred to as data breaches), the financial impact to an individual or an

organization, and the corruption of sensitive data using tools such as ransomware (Butavicius et al., 2016).

Correlation between human behavior and susceptibility to social engineering attacks

A variety of human characteristics contributes to a person's susceptibility to social engineering attacks--demographics, experience, and simple human nature. This portion of the literature review focused on discovering what correlations have been made in this area. While there is extensive research on the relationship between psychology and susceptibility to social engineering attacks, there are few publicly available studies regarding any correlation between demographic groups of Internet users and their susceptibility to social engineering attacks.

Many of the studies that address the psychology of social engineering agree that these attacks are successful because of their ability to take advantage of human nature, considered the weakest link in information security (Algarni et al., 2013; Barker, 2016; Dhinakaran et al., 2011; Rader & Rahman, 2015; Wilcox & Bhattacharya, 2015), with minimal use of technology beyond being used to collect information about potential victims and as a means to communicate with the victims.

Hasan (2010) establishes that social engineering campaigns form a pattern consisting of four phases – information gathering, relationship development, exploitation, and execution. The information gathering and relationship development phases may be curtailed or deeply planned, depending on the nature of the social engineering attack (Nyirak, n.d.). In cases of spear phishing, the attacker must spend the time to learn about the individuals and the environment to craft an email tailored to the individuals targeted for the attack (Butavicius et al., 2016); whereas, in traditional phishing, the message is generic for any victim. In any case, social engineers often target cultures which promote social interaction that forms trusting and open social relationships

(Wilcox & Bhattacharya, 2015); Australia was cited as one example of a culture that fits well into this category.

The studies also agree that social engineering manipulates six emotions of human behavior and that social engineering attackers leverage one or more of these six emotions during the relationship development and exploitation phase of their phishing campaigns (Thapar, n.d.). The first, curiosity, allows attackers to exploit a victim's natural curiosity by sending a phishing email that contains a link to a purported interesting video or another type of Internet site that peaks the interest of the victim (Barker, 2016; Rader & Rahman, 2015). The second, fear, persuades the victim to act in a certain way by sending a phishing email that appears to originate from an organization or person who has influence over the victim, such as the Internal Revenue Service (IRS), the victim's bank, or an executive at the victim's place of work. The third, empathy, involves impersonating a friend or other acquaintance of the victim and claiming to be in an emergent need for money, such as being stranded overseas on vacation (Rader & Rahman, 2015). The fourth, social proof, entices victims by creating the perception that the purported offer in the phishing email has been taken up by others and therefore must be legitimate. The fifth, scarcity, creates a sense of urgency by claiming that an offer in the phishing email is rare or limited and must be acted upon soon to take advantage of the offer. The last, authority, suggests that people will comply with a request if it appears that it came from someone in a position of authority (Butavicius et al., 2016; Rader & Rahman, 2015).

The ability to respond proactively to an attempted social engineering attack depends significantly on the personality of the targeted individual. Personality traits such as skepticism and patience, combined with a familiarity with computers and especially a knowledge of social engineering, influences how successfully that person will respond, while higher levels of

impulsiveness have been associated with lower performance detecting phishing emails because of the eagerness to take advantage of the content presented in the phishing email (Butavicius et al., 2016).

Arachchilage's (2014) research focuses on the evaluation of concepts or procedures of anti-phishing behavior as being the most effective for computer users. Arachchilage observes that cyber-attacks may be motivated, not only by the typical factors discussed above, but also by social gain. To illustrate the value of social gain, Arachchilage cites a BBC News report that found "one in four young Britons attempts to access the Facebook accounts of their friends just for fun" (BBC News, 2010).

Arachchilage also notes that as the workplace has become more connected, employees have been enabled to either work from home or bring work home with them, and home networks may not have the same infrastructure or security controls in place to protect their IT assets that they would find in the workplace, exacerbated by the fact that most computer users lack an awareness of security education or training. One study cited by Arachchilage found that 23% of participants ignored all cues of a web browser (address bar, status bar, and security indicators) that warn against illegitimate websites (Dhamija & Tygar, 2005). A lack of technical security controls afforded in an ill-designed home network, compounded with a lack of awareness to consider security warnings presented by a web browser, create a high-risk environment for social engineering.

The Arachchilage study concluded that when a threat, such as a phishing attack, can be avoided given a user's level of technical knowledge, the user may take a problem-solving focused approach to coping with the threat; however, when the threat cannot be avoided completely due to a lack of technical knowledge or understanding, the user may take an

emotional coping behavior approach. The user's self-efficacy, or confidence in their ability to achieve intended results, has a significant importance to "enhance their avoidance behavior to thwart phishing threats" (Arachchilage & Love, 2014).

Arachchilage concluded that a combination of conceptual and procedural knowledge has a positive effect on a user's self-efficacy, which contributes to the user's phishing threat avoidance behavior. The study also identified that computer users are susceptible to phishing attacks due to a lack of knowledge empowering them to prevent phishing threats.

Barker's (2016) presentation discusses the elements of human nature and societal norms that make humans susceptible to social engineering attacks. As discussed above, social engineering exploits characteristics of human behavior to obtain information or access to information systems from someone who is entrusted with valid access to that system. Attackers play on the desire for reciprocity and curiosity to exploit their victims.

Barker references the drastic growth in the use of social media over the past decade, notably with 20% of the world's population on Facebook, and the potentially correlating increase in narcissistic personality traits among younger Internet users. Barker cites research that suggests young people with narcissistic traits desire to have as many friends as possible and have those friends know what they are doing, which plays into a "perfect breeding ground for social engineering attacks" (Barker, 2016). In addition, the growth of the fast-paced lifestyle has contributed to users neglecting rational decision-making when faced with subtle social engineering attacks such as the phishing email that plays on the emotions discussed above. An example cited in Barker is the business professional that hurriedly checks emails on a mobile device while in-between meetings, where pressing through a backlog of emails takes a higher priority to carefully scrutinizing the content of each email from a security-conscious perspective.

Sheng (2010) provides useful data that supports the expected results of this thesis regarding the correction of demographics with social engineering attacks. In particular, Sheng found that generally speaking, women are more susceptible to phishing than men. In an Indiana University study (Jagatic, Johnson, Jakobsson, & Menczer, 2007), researchers discovered that before social engineering education, 77% of the female study participants fell for spear phishing attacks, versus 65% of the male participants. Similarly, in the same study, participants between the ages of 18 to 25 were more susceptible to phishing than other age groups. The reason was concluded to be that older study participants had prior exposure to phishing, more years of experience as users of the Internet, additional education, and a perceived financial risk from phishing attacks. Sheng also determined that participants that had started but not completed formal post-secondary education were at highest risk (approximately 35%) for being victimized by phishing attacks than any other education-based cohort.

The Sheng study was accomplished through a roleplay survey that was administered to 1,001 online respondents solicited using the Amazon Mechanical Turk service, and used to study the relationship between demographics and phishing susceptibility, and the effectiveness of anti-phishing educational materials. The survey offered questions to determine the respondent's background and knowledge about phishing, and then assessed their behavioral susceptibility to phishing through a roleplay task. Based on the assessment, the respondent was assigned one of several forms of training, and then administered a second roleplay task to identify reductions in their susceptibility to phishing and any changes in their tendencies towards being suspicious of legitimate emails. The respondents were randomly assigned to a control condition or one of four experimental conditions that varied depending on the training to which they were exposed. The roleplay task showed the respondents 14 images of emails in context and then asked the

respondents to indicate how they would respond to the emails if they had received them in their mailbox.

The biases in the findings from this study include the source of survey respondents--participants of Amazon Mechanical Turk. Users of the Mechanical Turk service are younger, more educated, and have more technical knowledge than the general public. As such, the study results will be biased towards this group of users. Also, because the roleplay provides a controlled environment for the respondents free from the risk of actual phishing, there is a lack of direct consequences for a respondent's decision which may invite more risky behavior than the respondent would normally accept in an actual social engineering situation.

Summary. The review of literature analyzing the correlation between human behavior and susceptibility to social engineering attacks indicates that humans have natural tendencies towards emotions that can be leveraged by social engineers to persuade a potential victim in a phishing attack. The literature finds that by combining training that instills a greater sense of skepticism, caution, and diligence when reviewing potential phishing emails, and empowering users with increased awareness and training to recognize behaviors that may be associated with social engineering, users will be more resilient to attempts at social engineering.

Workplace social engineering prevention and training challenges to individual protection against social engineering attacks

Typical social engineering awareness programs do not give any insight into the motives or methodologies of social engineers (Rader & Rahman, 2015). As a result, users do not understand the motivation of social engineering, but rather are only instructed to recognize the indicators of a social engineering attack and respond accordingly. Best-in-class anti-phishing software creates up to 50% false positive alerts for phishing email (Dhinakaran et al., 2011),

which suggests that objective tell-tale indicators are not reliable enough and users cannot depend on them solely to make determinations of a potential phishing email. At the same time, employees are spending an average of 4.1 hours each year responding to phishing scams (Ponemon Instiute, LLC, 2015), suggesting that the combination of technology and training in place today is not adequate to reduce the threat of phishing attacks.

Meanwhile, social media continues to rise as an emerging vector for social engineering attacks. These online services have become a view into the diaries of people's lives, broadcast for everyone to read including social engineers who can construct targeted phishing scams using the personal information available on social media profiles. Some users also make their email address and phone number publicly available, giving social engineers the information needed to conduct a phishing or smishing (phishing over SMS) attack (Rader & Rahman, 2015). As mentioned above, social media continues to rise particularly with the business-related use of services such as Facebook and LinkedIn, yet less than 30% of global organizations have social media usage policies in place and very few organizational policies offered any guidance for securing social media technology. This absence of policy suggests that organizational users lack awareness of, and thus an appropriate level of precaution, for social engineering activities operating within social media networks (Wilcox & Bhattacharya, 2015).

There are a variety of strategies available to social engineers for leveraging an attack that could go reasonably undetected by even a security-conscious user. Transparent proxies create spoofed copies of legitimate websites and then intercept all information provided by the victim to the purported legitimate website. DNS cache poisoning corrupts a name server table and directs a victim accessing a legitimate host to a malicious address. Browser proxy configuration hijacking changes the proxy setting on the user’s web browser, directing all traffic through a

man-in-the-middle proxy server designed to capture all information. URL obfuscation attacks and third-party URL shortening services convince a victim to click a link that appears to be similar to a legitimate website but instead takes the victim to a malicious site. Lastly, cross-site scripting attacks manipulate legitimate websites by injecting malicious code to collect data provided to the legitimate site (Rader & Rahman, 2015). While Google reports that 9,500 websites are blacklisted daily (Goodin, 2012), social engineers adapt their strategies in response, and phishing attacks become more sophisticated each day (Arachchilage & Love, 2014).

The Ponemon Institute (2015) study, as the title implies, studies the organizational costs resulting from a phishing attack, and the value that proactive employee training to counter social engineering brings to the organization thereby reducing the financial impact of phishing. Ponemon found through a survey of 377 IT and information security practitioners that effective social engineering prevention training can produce a cost savings of $188.40 per user, compared to an extrapolated annual cost of phishing for a typically sized organization approaching $3.77 million per year, mostly related to lost employee productivity.

Ponemon's research indicates the average cost to contain manually is $1.9 million per year, with the highest expense associated with the costs of cleaning and fixing damage resulting from malware, followed by the time and effort to investigate reported malware incidents; malware introduced via a phishing attack accounts for 11% of total malware incidents. Ponemon also calculates the potential cost of malware that was not contained by automated processes or personnel at $105.9 million per year, based on a probable maximum loss to the organization. By extrapolating the percentage of total malware incidents introduced by phishing against the total probable maximum loss, Ponemon calculates that the total cost attributable to phishing attacks at $338,098 per year.

As mentioned above, one of the highest costs is associated with lost employee productivity. Ponemon estimates that "employees waste an average of 4.16 hours annually due to phishing scams" (Ponemon Instiute, LLC, 2015). Assuming an average organization with 9,552 employees, the loss of 4.16 hours of work translates to approximately $1.8 million of lost revenue per year per organization, solely related to the lost productivity from phishing attacks.

Ponemon's research estimates that four credential compromises per year originate from phishing attacks. Assuming one compromise results in 1,540 hours of a technician's time to investigate and respond to the credential compromise, the total cost to the organization solely in technician time and effort is $381,920 per year.

The research concluded by Ponemon reflects that social engineering attacks, and phishing, in particular, represent a substantial financial risk to organizations regarding lost productivity and other direct monetary losses from data breaches. As has been consistent throughout the literature, improved user awareness training is the single most effective mitigation strategy to reduce organizational risk from social engineering, and Ponemon can place a valuation on such a strategy.

Rader (2015) considers how organizations have made heavy investments into technical controls intended to mitigate and reduce the potential risk of damage that may be caused by outsider attacks, including phishing and other methods of social engineering, yet the information assurance training provided to users "lacks enough depth and creativity to keep the trainee engaged" (Rader & Rahman, 2015). Rader proposes to reduce the "shotgun" approach of phishing awareness programs that cover a broad spectrum of information at once into a "rifle shot" approach where the audience is more focused and information presented is more detailed.

Rader equates the modern state of information security to the settlement of Troy, a fortified city that was able to withstand ten years of Greek assault given its perimeter defenses, but a single act of social engineering--that is, the disguised Trojan horse containing Greek soldiers--was brought into the city by Trojans themselves and let to the assault and fall of Troy. In information security terms, penetrating firewalls may take an extraordinary amount of time but convincing someone with access to let them in takes very little comparative effort. The only way to counter these risks is by developing and sustaining a "wary and well-educated staff."

Rader also observes that while the typical social engineering awareness program typically covers aspects of social engineering such as dumpster diving and phishing, they often do not touch on the practices of social engineers nor give insight into their motives and methodologies. As a result, employees do not develop a vigilant defense against the practice of social engineering itself, but rather are trained to simply observe the objective indicators of a social engineering attack such as a phishing email.

By eliminating the current approach to social engineering awareness training--one that is most often a small block of a larger information assurance training program--and creating small, focused chunks of training, users will be more conscious to the subject of social engineering as a singular threat.

Wilcox (2015) focuses on the threat of social engineers that are targeting social media platforms as a precursor to an attack on organizations. As has been established elsewhere, traditional information security strategies that protect the boundary of organizational information systems are not able to adapt to the changes in employee behavior, such as the proliferation of social media, that are creating emerging threats to the organization.

Wilcox underscores that the line of separation between business and personal use of social media technology has become blurred and that social engineers are now shifting their effort away from conventional email phishing to social media platforms to target large volumes of potential victims. Wilcox cites a Symantec report ("Spam decreasing, but social media phishing soaring says Symantec," 2010) that lists the top three issues related to social media negatively impacting organizations as employees disclosing too much information, the loss of confidential organizational information, and increased exposure to litigation.

Global and domestic organizations are adopting social media and other emerging technologies to create new business opportunities, but these technologies also present a significant organizational risk. Wilcox's review of existing organizational policies around social media found a general inconsistency and lack of clarity as to how organizations should legally and ethically address these risks. In 2010, governments in the United States and Australia created initiatives allowing for more open and transparent communications with its constituents; however, to date, there is still uncertainty as to how governments should establish boundaries for government employees' personal, professional, and official agency use of social media. Within the workplace, the government model which may serve as an example for other organizations, has generally established social media policy in one of three ways: (1) controlling the number of and types of employees that may access social media sites, (2) limiting the types of sites that are approved for employees to access, or (3) creating a customized social media platform or using a purpose-built closed social media service (e.g., Socialcast, Workplace, Yammer) for internal use.

In addition to policy considerations, Wilcox noted that traditional network security techniques (using technology to block or filter content) must be augmented with the vigilance of monitoring and social engineering penetration testers to connect a human element with the

collected data of the automated systems. There is an existing gap between social media policy development and lack of advice and awareness provided for employees as to how they can protect themselves and the organization from social engineering attacks.

Employee use of social media and the intermingling of personal and professional online presence continues to grow steadily. Organizations are well positioned to address this trend through policy and awareness training that enables employees to participate in the online social experience and promote their organization's message, while still able to protect organizational interests, by clearly defining permissible behaviors for all employees.

Summary. Organizations are faced with new challenges in the era of social media that create conflict between organizational risk and employee freedoms. The reviewed literature consistently echoes a lack of consistent organizational policy to address these challenges and the importance to begin any effort towards addressing those challenges with a sound policy that is accepted by an organization's executive-level management. With an accepted policy in place, organizations can undertake measures to pursue technical controls and much-needed awareness education and training to reduce the risk to the organization while protecting its employees from exposure to social engineering.

Better methods or delivery mechanisms for social engineering prevention

To improve social engineering awareness, and in turn, the success of prevention, a combination of technical and training solutions must be identified and employed. Several studies mutually agree that, from a technical perspective, a multi-layered approach to host-based firewalls, anti-malware software, and email filters will reduce the volume of phishing emails with which a user must contend (Dhinakaran et al., 2011; Gharibi, 2012; PCI Security Standards Council, LLC, 2015). However, the effectiveness of any email filter depends on the ability for

the filter's policies to be refined, trained, and regularly updated, to remain aware of current phishing strategies (Gharibi, 2012). Studies also recommend users regularly check their operating systems, web browsers, and security software to ensure the latest security patches and updates have been applied, and verify the website the user is accessing is correct before downloading any software or updates, or providing any sensitive personal information (PCI Security Standards Council, LLC, 2015).

Beyond the technical recommendations, a significant amount of effort must be afforded to awareness and training for users. Social engineering prevention training has been shown to reduce susceptibility to phishing attacks between 40% (Sheng et al., 2010) to 64% (Ponemon Instiute, LLC, 2015), yet the current business practice is focused on creating employee awareness at a fundamental academic level, and existing training programs lack the depth and creativity necessary to keep the audience engaged (Rader & Rahman, 2015); the consensus is that collaboration from government, and the private sector is needed to increase cybersecurity effectiveness (Wilcox & Bhattacharya, 2015).

Studies that have evaluated user training recommend that to be effective, the audience must remain engaged, and the training should provide historical examples combined with technical examples of common attacks (Rader & Rahman, 2015). The training should focus on behavior modification to make users aware of and able to recognize the phishing threat (Barker, 2016), such as educating users of the six human behaviors discussed above that social engineers exploit and to resist the urge to follow links or open attachments in suspicious emails despite how appealing the email may seem (PCI Security Standards Council, LLC, 2015).

Government organizations have begun to lead initiatives towards building citizen awareness of the social engineering threat, including the *10 steps to cyber security* awareness

campaign in the United Kingdom (National Cyber Security Centre, 2016), *Cyber Security Awareness Campaign* in India (Data Security Council of India, n.d.), *Go Safe Online* in Singapore (Cyber Security Awareness Alliance, n.d.), and *Stop.Think.Connect.* in the United States (U.S. Department of Homeland Security, 2017) (Wilcox & Bhattacharya, 2015). These awareness campaigns create an ideal venue for driving the awareness message out from corporate and organizational boundaries, and to the general public.

The concept of dynamic security skins was recommended in other literature, and the Dhamija (2005) paper allowed for a more in-depth analysis of the proposed technology.

The dynamic security skin scheme builds upon the Secure Remote Password (SRP) protocol (Wu, n.d.) and renders a trusted browser window with username and password prompts, combined with an individualized photographic image specific to the user, to create a personalized login window per user. Dhamija proposes that because the visual image represents a trusted connection with the remote server, a less complex username and password may be used. To indicate secure connections with a remote server, Dhamija evaluates options for a user interface such as a border graphic that is only rendered during a secure session, and expects that users may find image matching to be less cumbersome than inspecting an HTTPS certificate.

Throughout the research, Dhamija found that phishing attacks "exploit the human tendency to trust certain brands, logos and other trust indicators" (Dhamija & Tygar, 2005) by falsely representing a trusted organization and creating a sense of urgency to take an action to protect the user's relationship with that organization--for example, informing the user they must update their password or perform a similar account function. This exploitation lends itself to ten problems users face: (1) users are unable to reliably determine a sender's identity from a received email, (2) users are unable to reliably distinguish legitimate email and websites from

illegitimate content with a similar "look and feel", (3) users are unable to reliably evaluate domain names for legitimacy, (4) users are unable to distinguish actual hyperlinks from image representations of a hyperlink, (5) users are unable to distinguish a browser's interface from a web page with content that creates a similar appearance, (6) users are unable to identify legitimate browser security indicators from those presented on a web page, (7) users do not understand the intended meaning of a browser's HTTPS lock icon, (8) users do not consistency notice the absence of a security indicator, (9) users are unable to reliably distinguish between multiple browser windows and their associated attributes, and (10) users do not consistency understand the purpose, function, and application of [HTTPS] certificates.

While many of the challenges above continue to be prevalent today, there have been significant improvements to browser security (namely user-friendly warning windows that appear and require the user to explicitly acknowledge) that mitigate the impact of these challenges. Also, the dynamic security skin proposal requires browser support, website support, and added user effort to adopt this scheme.

After discussing the elements of human behavior that makes us susceptible to social engineering, Barker's (2016) presentation concluded by providing recommendations to organizations that can be used to mitigate existing social engineering threats.

First, Barker recommends organizations have a robust cybersecurity culture where the staff is empowered to challenge and prioritize security appropriately. Further, awareness training should focus on changing behaviors and highlighting the most prevalent threats. Organizations should also implement procedures to ensure that sensitive financial transactions required approval from more than one person, strictly enforced physical security procedures particularly

concerning visitors, a mandatory visual identification policy within organizational buildings, and a social media policy which includes provisions for responding to social engineering attacks.

Barker's presentation is notable in that it specifically discusses empowering users to take personal responsibility for security, and developing training that focuses on behavior modification, rather than solely developing an awareness program.

Gharibi (2012) studies, discusses and proposes technologies for detection of phishing sites and provides recommendations to prevent phishing for consumers and business, which provides relevant information to identify opportunities for bridging the gap between organizational training and applicability to individual consumers.

Gharibi acknowledges that cyber threats are becoming more dangerous for individual consumers as they are being targeted for personal information such as login credentials and credit card numbers to be used in identify theft, and social engineering tactics are easier to employ rather than attempting to hack into a system containing the information. According to Gharibi (2012), "by 2007 social engineering techniques became the number one method used by insiders to commit e-crimes."

Gharibi observes in his study that many anti-phishing solutions have been proposed, and some of those solutions attempt to address phishing at the e-mail level similar to those approaches used in anti-spam technology. However, because anti-spam technology is not used by the majority of Internet users, a burden is placed on e-mail providers to implement protections at the server level as an augmentation to endpoint security. A solution that does not involve the use of e-mail filtering is to build the logic of phishing domain blacklisting directly into web browsers rather than depend on a third-party add-on--a technology that has been demonstrated by Apple in their Safari browser, Google in their Chrome browser, Mozilla in their Firefox browser,

and Microsoft marginally with the Internet Explorer, and more recently improved with the release of their Edge browser.

Gharibi recommends for corporations that provide Internet-based services to consumers to create policies that govern acceptable e-mail content to ensure that e-mail cannot be mistaken for phishing, provide stronger authentication measures to allow the consumer to validate the legitimacy of any e-mails they receive purporting to be from that company, and implement blocking at the corporate website gateway to prevent phishing sources from accessing the legitimate website (seen in man-in-the-middle and proxy attacks and website scraping). For consumers, Gharibi recommends anti-spam, -malware, and -spyware tools to protect against any malicious content from being introduced to the computer via a phishing email, a balance of other countermeasures to minimize the phishing attacks introduced to a consumer, and continued education to maintain awareness of social engineering techniques and the ability to recognize a phishing attack. One recommendation that was not observed in any other literature is that Gharibi encourages consumers to be aware of how legitimate entities will communicate with them via e-mail, which requires corporations to proactively inform its customers of the corporation's electronic communication strategies.

To reduce the risks in the workplace presented by social engineering, Rader suggests that reduction begins at the senior management level of the organization. Executive buy-in and effective policies must be implemented that places an appropriate emphasis on information security at the senior management and executive level, and promotes an atmosphere among all members of the organization, to begin working towards minimizing breaches resulting from social engineering.

Once policies are in place and supported by management, training is one of the most important ingredients to improve awareness of phishing scams. Rader suggests combining an awareness program with interactive tools that expose users to actual phishing attacks to develop skills for recognizing various phishing attack vectors. One common thread that runs continuously through Rader is that awareness training must be informative, relevant, and keep the audience engaged.

Summary. Moving the effective level of awareness and ability for Internet users to counter social engineering threats requires improved mechanisms in both terms of technical protections and training. Technical protections have been developed and in-place for quite some time, and they continue to evolve in response to emerging threats on the Internet. However, technical protections are not efficient in countering social engineering and are not capable of detecting threat campaigns that make use of dynamic technology, such as those seen with growing and increasing frequency. To close the gap between what technical solutions afford and total protection, user awareness and vigilance is essential. The recommendations in the literature all point towards emphasis training specific to the fundamentals of social engineering, including the motivating behaviors and tactics used by social engineers, to enable Internet users to recognize attacks as early as possible in the attack chain. One area that was not discussed in the reviewed literature, however, is how to improve the delivery of the training for those users that do not receive organizational training through an employer or academic institution.

Research Methodology

This study incorporates a qualitative analysis of existing research and resources on the subject of social engineering, combined with the collection of quantitative data from anonymous online self-completion surveys designed to identify trends of online Internet behavior and defensive posture from social engineering attacks. This section focuses on the nature of the research, provides a description of the methods used to carry out this study as well as the variables considered during the phases of study, and discuss the research design to include the population used, the sampling technique that was selected, data collection procedures, analysis of the collected data, and the instruments used during the study.

The purpose of conducting the survey portion of research is to gather a real-world sampling of online Internet behaviors from typical users under normal conditions, and establish whether there were any consistencies identified among the sample population that could be used to develop generalized behavior trends. The qualitative research involves a thorough review of published literature, including existing research, industry best practices, training material, and other publicly available information to provide background context for the current state of social engineering awareness and to identify underserved areas of research on the subject.

Research Questions

This study intends to explore the challenges of effective social engineering awareness by considering the following question:

MQ. How can individuals better protect themselves from being exploited by cyber-related social engineering attacks?

To reach an answer to this overarching question, the research in this study addresses the following specific questions by evaluating existing approaches to social engineering awareness training:

Q1. Is there a correlation between human behavior and susceptibility to social engineering attacks?

Q2. Are any specific demographic groups particularly susceptible to social engineering attacks?

Q3. Does workplace training on social engineering prevention benefit an individual's protection against social engineering attacks in the personal/consumer setting?

As existing approaches are evaluated, a fourth question will also be considered:

Q4. What methods or delivery mechanisms of social engineering prevention education may be more effective than is currently available today?

Identification and Operationalization of Variables

The variables considered in the hypotheses of this study include:

V1. Age ranges of those surveyed (measured as groups from 18-24 years of age, and then ten-year increments from 25 through 85 years of age).

V2. Gender of those surveyed (measured as self-identified male, female, or other).

V3. Utilization of online services of those surveyed within an average week (measured as groups of less than 5 hours per week, 5-14 hours, 15-28 hours, 29-56 hours, and over 56 hours per week).

V4. Level of education of those surveyed (measured as groups of less than high school, high school graduate, some college, 2-year degree, 4-year degree, or doctorate).

V5. Formal social engineering awareness training of those surveyed (measured as yes or no).

The age range (V1) and level of education variables (V4) are used to frame hypotheses that relate age to a degree of susceptibility to social engineering attacks (H2), and recency of formal education to a degree of susceptibility to social engineering attacks (H3). Gender (V2) is used to determine whether expected responses to suspected social engineering has any notable variance based on the subject's gender. Formal social engineering awareness training (V5) is used to frame the hypothesis that discounts relation of workplace training to personal social engineering susceptibility (H4).

Population and Sampling Plan

The survey portion of this study will collect the variables identified above, combined with background questions to gather typical Internet usage patterns (location, devices, methods, anti-malware product usage, etc.), and scenario-based questions to determine the subject's reactionary behavior when presented with a social engineering attack. The survey is a referral sampling intended to solicit at least 100 responses to capture a variety of subjects, and intentionally targets a random audience of online Internet users to represent the Internet's distributed nature and to avoid bias towards a particular geographic or demographic segment. Participation criteria required the subject to be at least 18 years of age and an Internet user. Expected variations in survey responses include abandoned surveys, inaccurately recorded responses, and subjects electing to not answer a particular question. These variations are expected to be minimal and not have a notable effect on the results.

Data Collection/Sources

The primary data source for this study consists of self-completion surveys that were distributed to online Internet users and analyzes collected research data to identify common trends in behavior among demographic groups and educational cohorts.

The secondary data source of this study is a review of the literature including previous research on the correlation of human behavior and social engineering, online information covering industry evaluations and recommendations of social engineering prevention practices, and historical and online information detailing actual workplace strategies for social engineering prevention training.

Summary of Analysis Procedures

Because of the results of the study, aside from those variables identified above, are subjective responses, they will not be normalized. Results will be represented as percentages of the total responses to the survey, or total responses for the respective segment. Some survey questions provide the option for the subject to give an open-ended answer, in which case those responses will be coded to create a uniform set of responses. The variables listed above will be used to create cross-section results to answer the hypotheses under consideration.

Limitations of the Study

Given the limited time available to complete this study, extensive observation into the effectiveness of any recommendations presented is not possible. Recommendations presented in this study are conceptually based in part on industry best practice for preventing and countering social engineering efforts, and further research is needed to determine actual effects of the recommendations presented herein.

This study is also limited by the amount of publicly available information relating to the impact of social engineering attacks on individuals and organizations. To protect reputation or ongoing operations, organizations may choose to not publicly disclose occurrences of being a victim to social engineering. Information relating to impacts on individuals and organizations may be conceptualized to illustrate the overall impact of social engineering.

Assumptions

The research presented in this study assumes that malicious actors use current, well-known tactics, techniques and procedures to carry out social engineering attacks, such as phishing and spear-phishing emails, and poisoned web ads or search results. This study also assumes that service providers use fundamental industry best practices to protect users and organizations from general computer security attacks, such as anti-malware and content filtering. This study will focus on more sophisticated protection strategies specific to social engineering campaigns.

Results of the Study

Objective Results

A total of 101 subjects responded to the online self-completion survey. Age ranges (V1) were responded to by 86 subjects and are distributed as follows: 34.88% were between 18-24 year of age, 26.74% were between 45-54, 22.09% were between 35-44, and the remainder of age groups accounted for less than 10% each (see figure 1).

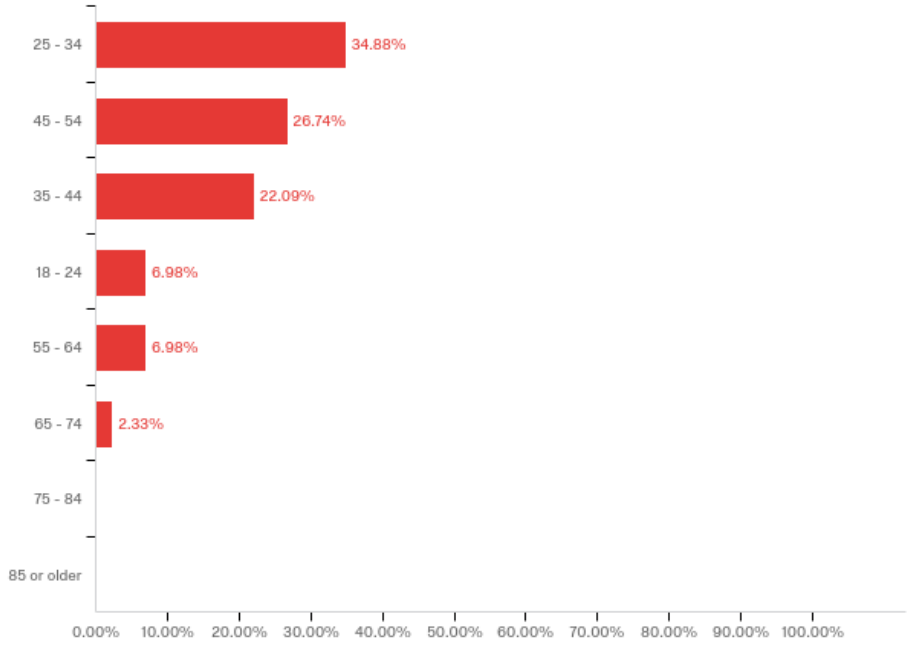

Figure 1. Survey response distribution by age range.

Gender (V2) was also responded to by 86 subjects and is distributed as follows: 50.00% identified as female, 48.84% identified as male, and 1.16% identified as other (see figure 2).

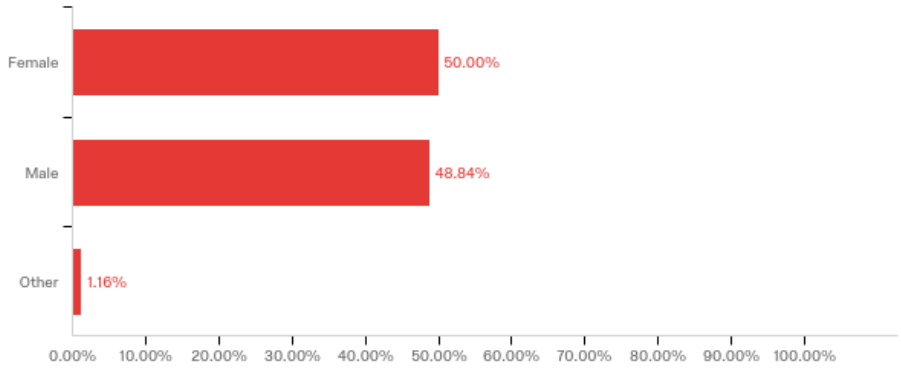

Figure 2. Survey response distribution by gender.

Online Internet usage (V3) was responded to by 100 subjects and is distributed as follows: 29.00% ranged between 29-56 hours per week, 27.00% ranged between 5-14 hours per week, 22.00% ranged between 15-28 hours per week, 18.00% exceeded 56 hours per week, and 4.00% were less than 5 hours per week (see figure 3).

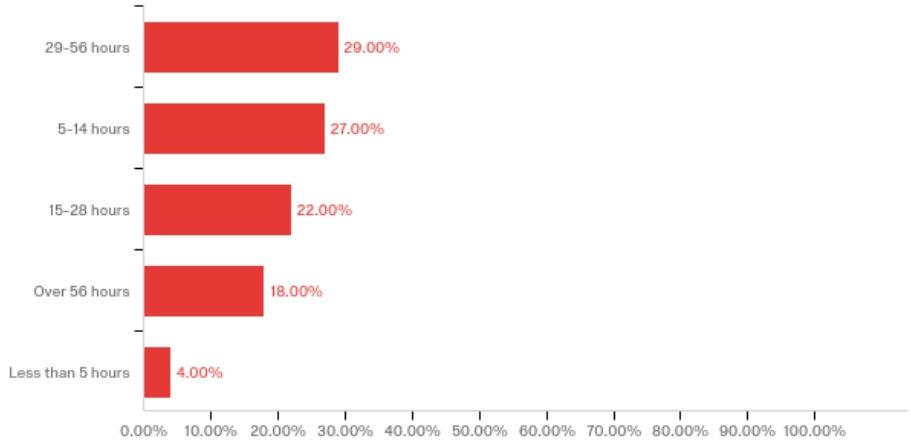

Figure 3. Survey response distribution by average online Internet usage.

Highest level of education completed (V4) was responded to by 62 subjects and is distributed as follows: 54.84% completed a four-year degree, 16.13% completed a four-year degree, 16.13% had some college, 9.68% completed a doctorate, and 3.23% received a high school diploma (see figure 4).

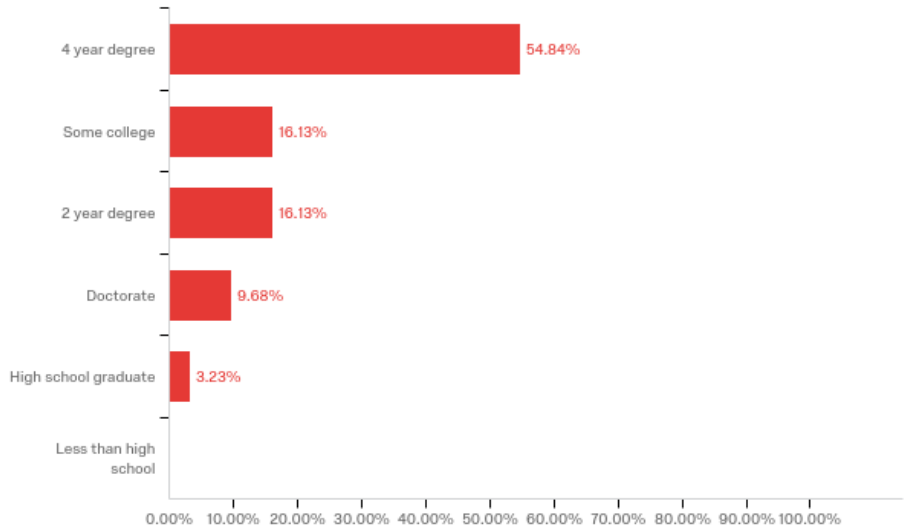

Figure 4. Survey response distribution by highest level of education.

The subjects were asked to identify the devices and in which settings they routinely access the Internet (see figure 5). This question is intended to identify the most common scenarios for gaining Internet connectivity (by device, connection, and any technical controls in place to filter access to the Internet [e.g., corporate content filter/firewall, home router, mobile device with restricted execution policy]). The highest responses included a mobile device connected to Wi-Fi while at home (92.93%), mobile device connected to cellular provider in public spaces and while traveling (91.14% and 90.12%, respectively), desktop/laptop computer while at work (84.34%), and desktop/laptop computer while at home (62.63%).

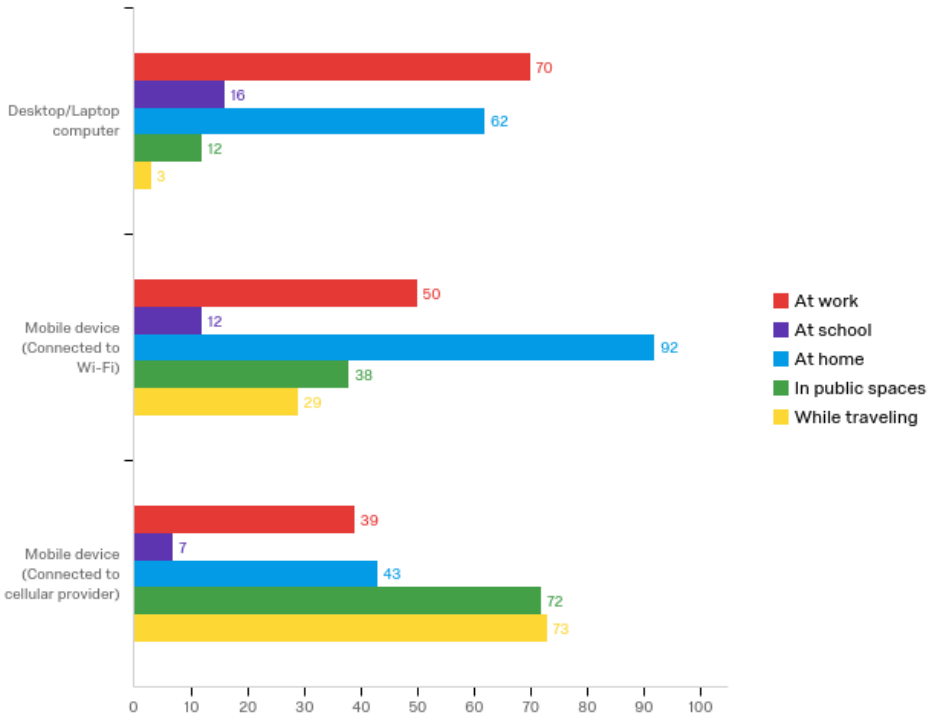

Figure 5. Survey response distribution by location/method of accessing the Internet.

Subjects were then asked to identify the settings, using the same options as provided in the previous question, in which they access their email (see figure 6). This question is an extension of the previous question in that its purpose is to identify the degree of phishing email protection available to a user in their various settings, and to also validate responses from the previous question since accessing email is a common and frequent Internet behavior. The highest responses included a mobile device connected to cellular provider while traveling and in public spaces (91.30% and 89.71%, respectively), desktop/laptop computer while at work (88.16%), mobile device connected to Wi-Fi while at home (85.11%), and desktop/laptop computer while at home (60.64%).

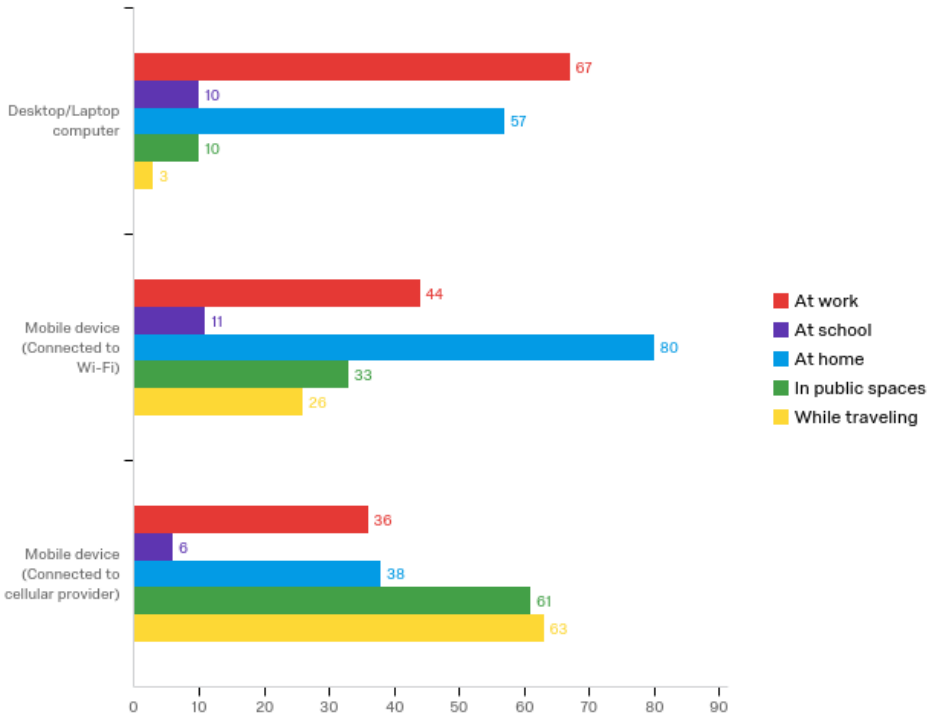

Figure 6. Survey response distribution by location/method of accessing email.

The last series of questions before entering the subjective portion of the survey was for the subject to identify whether they used any anti-malware or other Internet security product on their desktop or laptop computer or their mobile device. 81.01% of the 79 responses indicated they did use an anti-malware or Internet security product on their desktop or laptop computer, while only 29.47% of the 95 responses indicated they use an anti-malware/Internet security product on their mobile device.

Of the subjects that did identify that they used an anti-malware or Internet security product on their desktop/laptop computer (see table 1), several data points were provided. The first is that the majority of responses (18.18%) used a product that is available by default in Microsoft Windows (either Windows Defender or Microsoft Security Essentials)[1]. Another is

[1] References to specific products does not constitute an endorsement of the product or service.

that 9.09% did not know what the product was, just that something was installed on the computer (particularly in cases of corporate-owned computers).

Table 1. Survey responses by desktop/laptop anti-malware product.

Anti-Malware Product	**# of Responses**
Windows Defender	12
Norton	9
McAfee	9
Avast	6
Malwarebytes	5
Webroot	4
AVG	4
ESET	3
Symantec	2
Sophos	2
Clam AV	1
Spybot	1
Kaspersky	1
Trend Micro	1
Unknown	6
Grand Total	**66**

The responses to anti-malware or Internet security products on mobile devices is much less definitive (see table 2). 15.00% of the 20 responses identified a VPN client as their Internet security product. Another 15.00% did not know what the product was but believed to have one installed.

Table 2. Survey responses by mobile anti-malware product.

Anti-Malware Product	**# of Responses**
Personal VPN	2
Lookout	2
Avast!	2
Super Anti-Spyware	1
AVG	1
Symantec/Norton	1
Avira	1

ESET	1
Symantec	1
VPN unlimited	1
Webroot	1
McAfee	1
Apple	1
Malwarebytes	1
Unknown	3
Grand Total	**20**

Subjective Results

The subjective portion of the survey is divided into three sections. In the first section, the subjects were presented with two sample phishing emails and one phishing website and asked to identify the portions thereof that they believed were indicators of a social engineering attack. The results are presented in figures 7, 8, and 9 as heat maps.

In figure 7, a sample PayPal phishing email, the largest concentration of responses identified as suspicious a mistyped expiration of a security notification (27%), followed by the mismatch between the printed URL and the hyperlinked text, the generic greeting, and the printed URL itself. Other noted suspicious items included the mistyping of “PayPal” with proper capitalization and the generic reference to “online service” rather than “PayPal.”

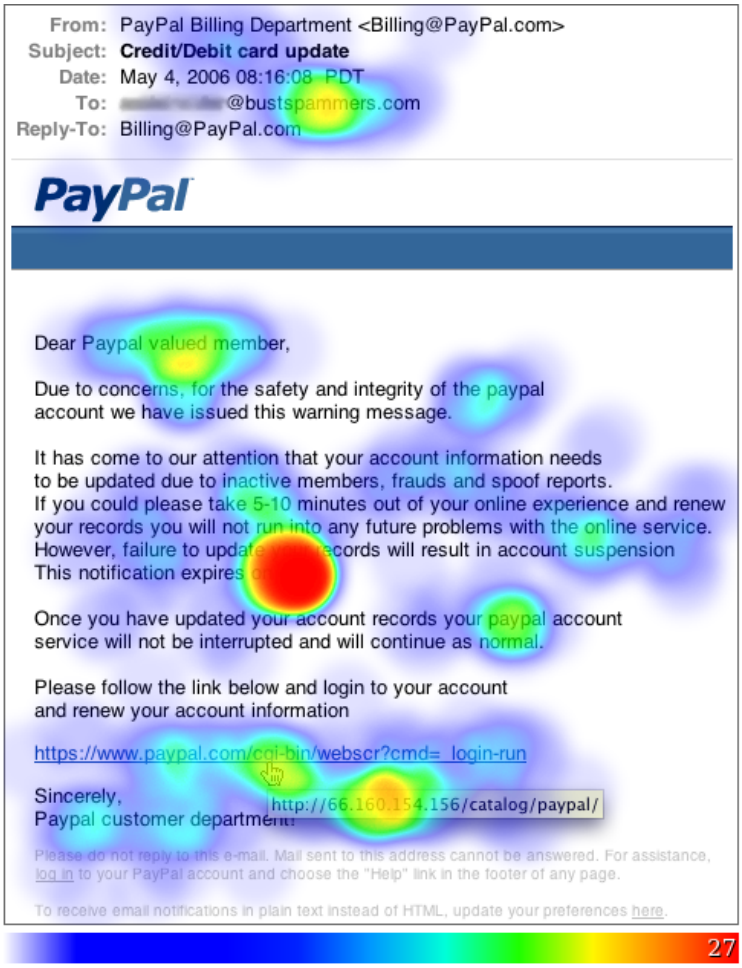

Figure 7. Heat map of survey responses to PayPal phishing email.

In figure 8, a sample notice to vacate email, the largest concentration of responses identified as suspicious a .zip attachment to the email (15%), followed by non-standard English language, and the unknown sender domain.

Figure 8. Heat map of survey responses to realty company notice to vacate.

In figure 9, a sample PayPal phishing website, the largest concentration of responses was the browser's address bar indicating a URL not consistent with PayPal's legitimate address (15%), followed by an out of date copyright.

Figure 9. Heat map of survey responses to PayPal phishing website.

In the second section, the subjects were given hypothetical scenarios and asked to choose, from a list of actions, which action would they take in response. The first scenario presented was "in the event that you discover a social engineering (phishing) email in your work/school mailbox, which actions would you take?" (see figure 10). The highest responses were to delete the email (63.22%), contact the help desk or information security/awareness group to report the email (48.28%), and move/flag the email as junk/spam (36.78%).

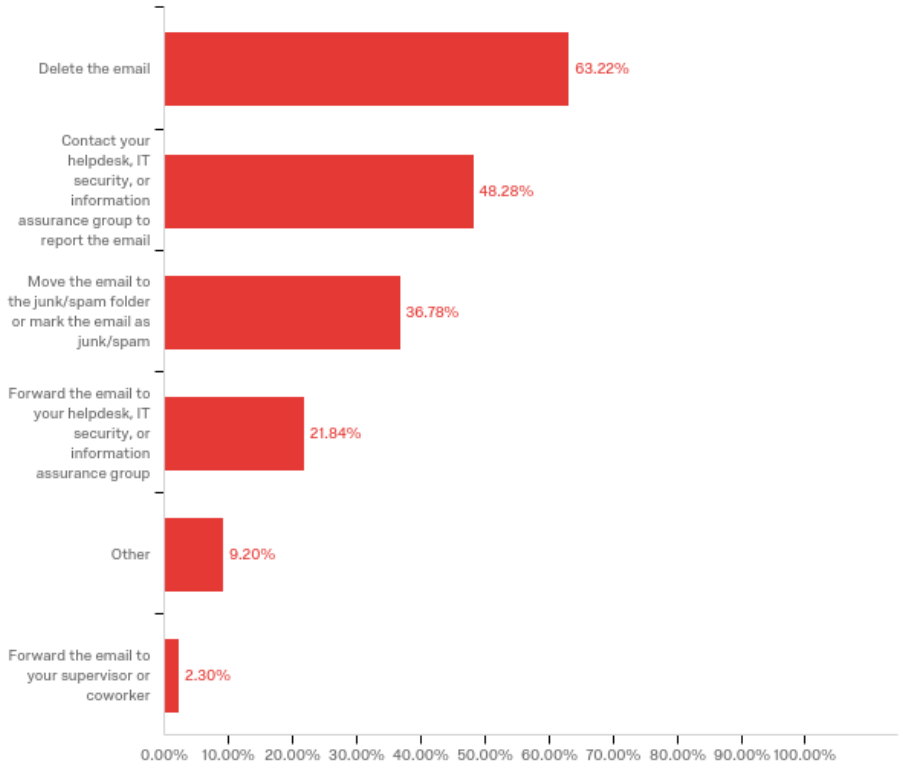

Figure 10. Survey response distribution by actions in response to phishing email in work/school mailbox.

The second scenario presented was the same as the first, but in the context of a home/personal mailbox (see figure 11). The highest responses were to delete the email (79.31%) and move/flag the email as junk/spam (48.28%).

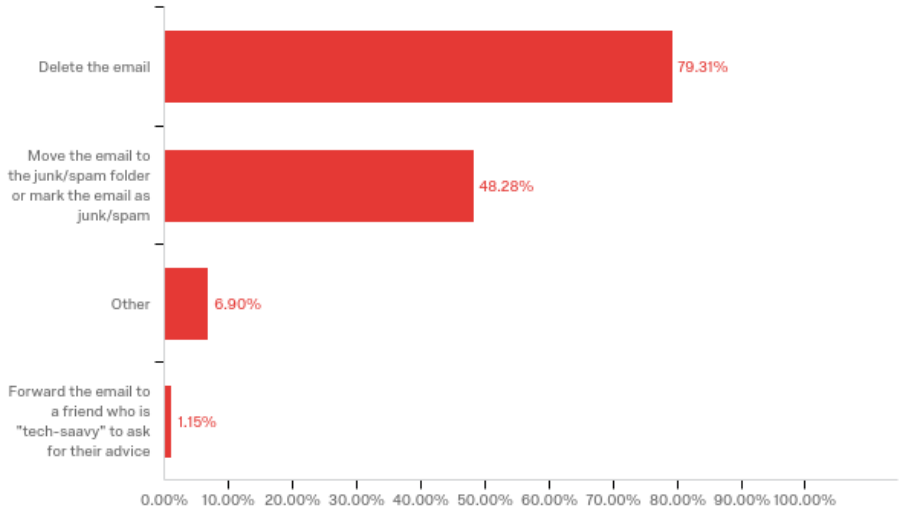

Figure 11. Survey response distribution by actions in response to phishing email in home/personal mailbox.

The third scenario presented was "in the event that you arrive at a phishing website on a work/school computer after clicking a link, which actions would you take?" (see figure 12). The highest responses were to close the web browser (56.32%) and contact the help desk or information security/assurance group to report the incident (51.72%).

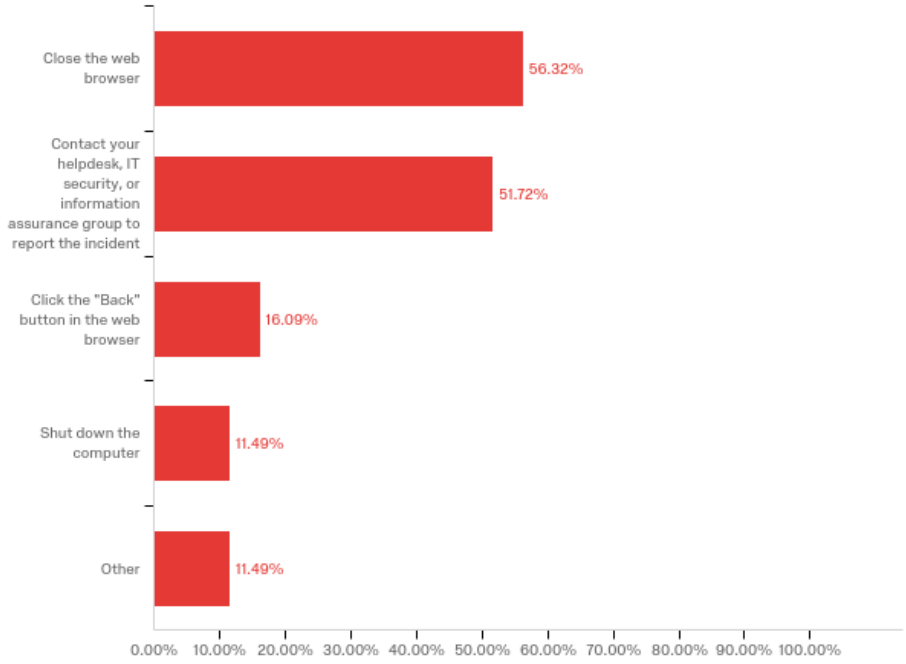

Figure 12. Survey response distribution by actions in response to accessing a phishing website at work/school.

The fourth scenario presented was the same as the previous, but in the context of a home/personal computer (see figure 13). The highest responses were to close the web browser (72.09%), shut down the computer (27.91%), and click the “back” button on the browser (23.26%).

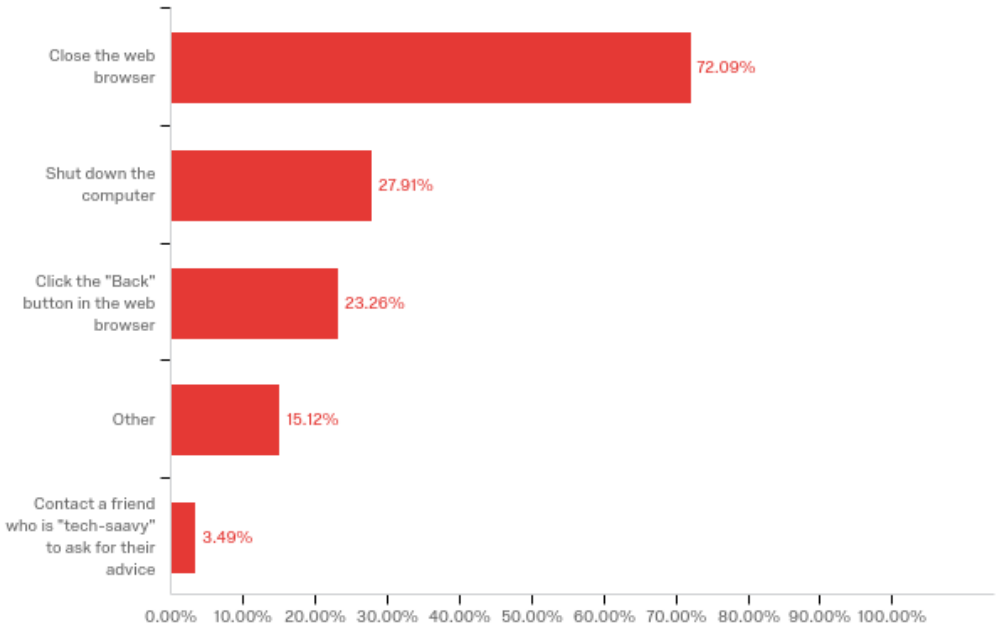

Figure 13. Survey response distribution by actions in response to accessing a phishing website at home.

The fifth scenario presented was "in the event that you inadvertently enter your password into a phishing website on a work/school computer, which actions would you take?" (see figure 14). The highest responses were to change your password (82.76%) and contact the help desk or information security/awareness group to report the incident (65.52%).

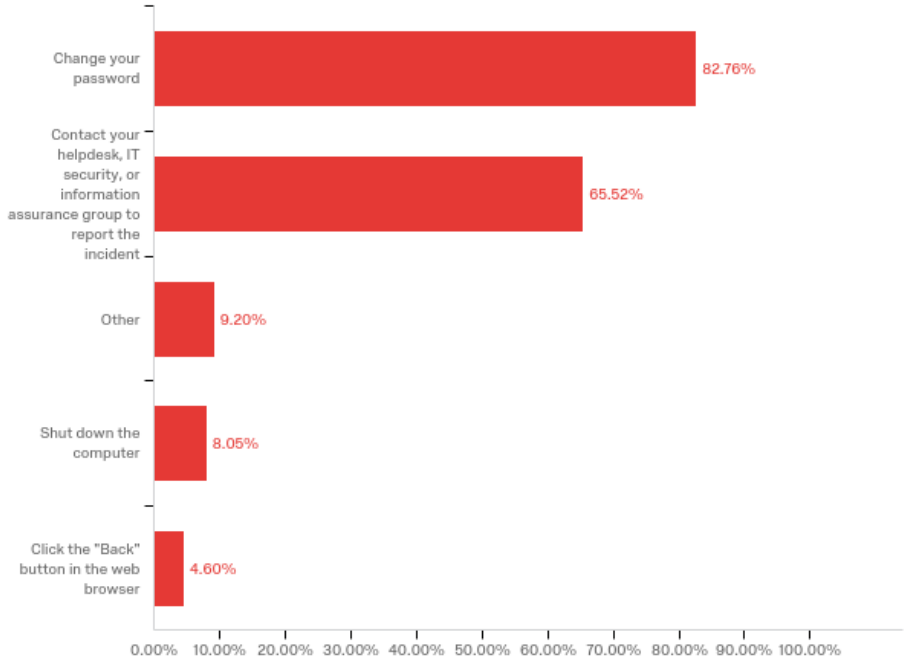

Figure 14. Survey response distribution by actions in response to disclosing a password to a phishing website at work/school.

The last scenario presented was the same as the previous, but in the context of a home/personal computer (see figure 15). The highest responses were to change your password (88.37%) and shut down the computer (19.77%).

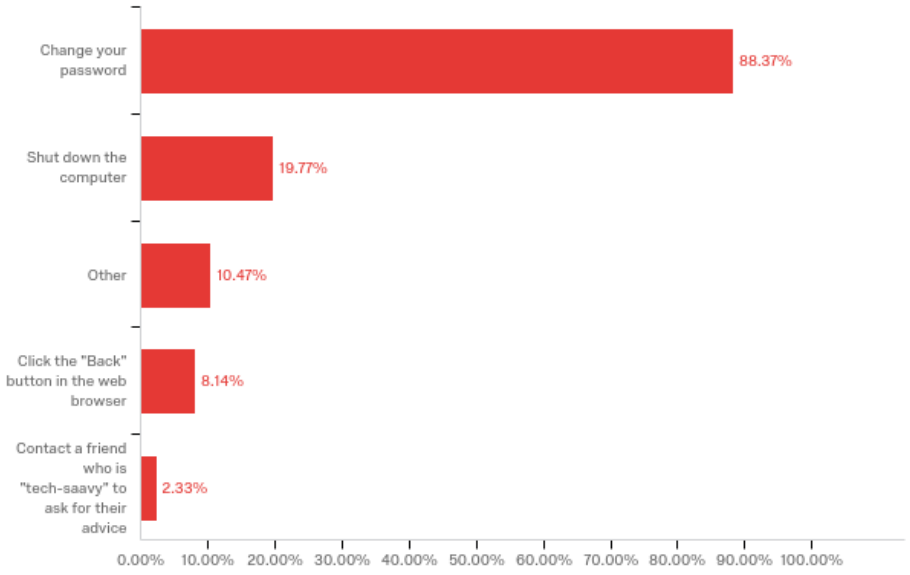

Figure 15. Survey response distribution by actions in response to disclosing a password to a phishing website at home.

In the third and final section, the subjects were asked to self-evaluate their level of competency with computers, any previous exposure to formal instruction relating to protecting against social engineering attacks, and confidence to respond appropriately to a social engineering attack. When asked to rate their level of competency with computers, 87 subjects responded to the question (see figure 16). Of those, 35.63% rated themselves as somewhat above average, 32.18% rated as average, and 25.29% rated as far above average.

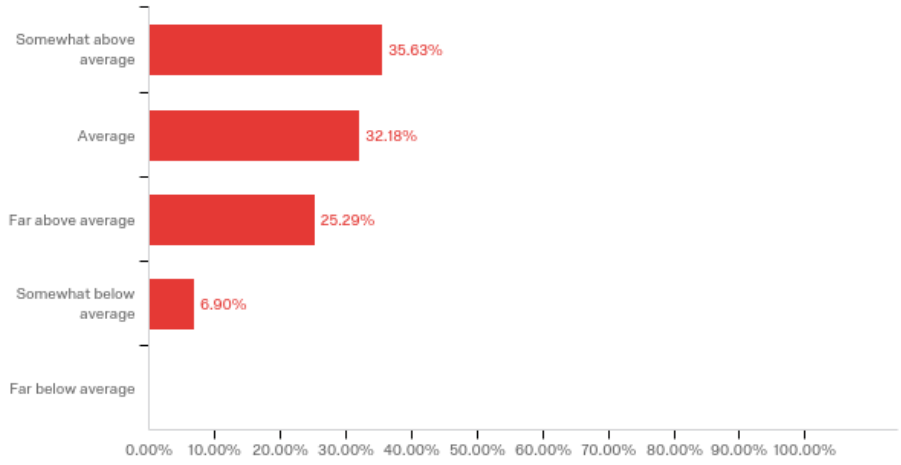

Figure 16. Survey response distribution by self-evaluated level of computer competency.

When asked whether they had any previous exposure to formal instruction relating to protecting against social engineering attacks, 87 subjects responded to the question (see figure 17). Of those, 47.13% responded "no," 42.53% responded "yes," and 10.34% responded "maybe."

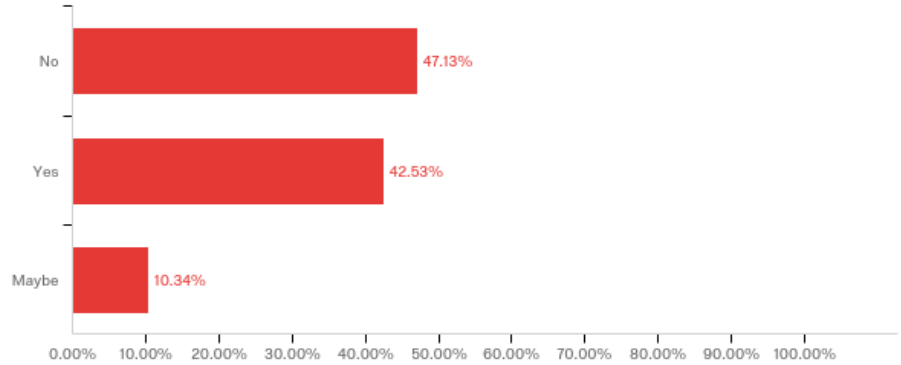

Figure 17. Survey response distribution by previous formal instruction in social engineering prevention/protection.

The last question asked the subjects how confident they were to respond appropriately to a social engineering attack. 87 subjects responded to the question (see figure 18). Of those,

37.93% responded as somewhat comfortable, 26.44% were extremely comfortable, and 19.54% were neither comfortable nor uncomfortable.

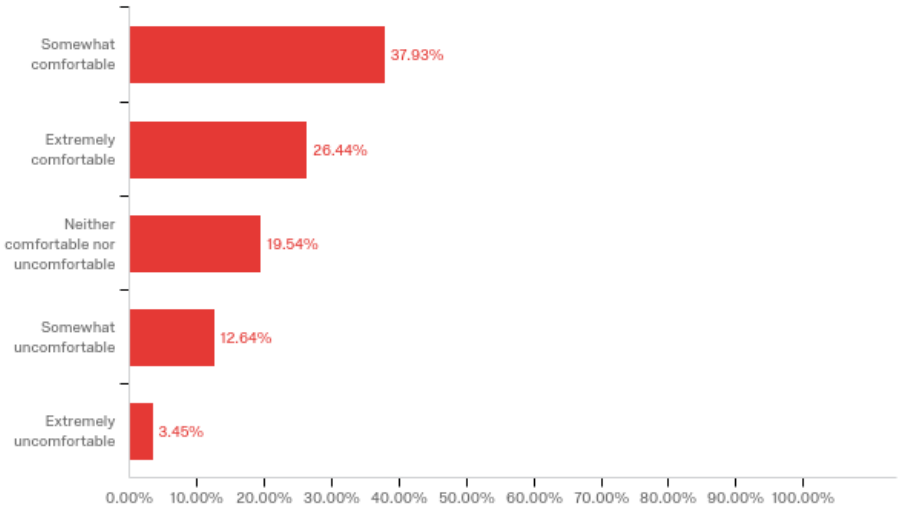

Figure 18. Survey response distribution by level of comfort to respond appropriately to a social engineering attack.

Significance and Interpretation of Results

To answer research questions Q2 and Q3, several segments of the survey results were considered. Q2 asks whether any specific demographic groups are particularly susceptible to social engineering attacks, which requires analysis of the survey's responses by a cross-section of gender, age range, and level of education.

Gender. When considering how much time subjects spend online in an average week, there is a significantly greater segment of males who spend over 56 hours per week (30.95%) than females (11.63%), and more females who spend 15-28 hours per week (32.56%) than males (11.90%) (see figure 19).

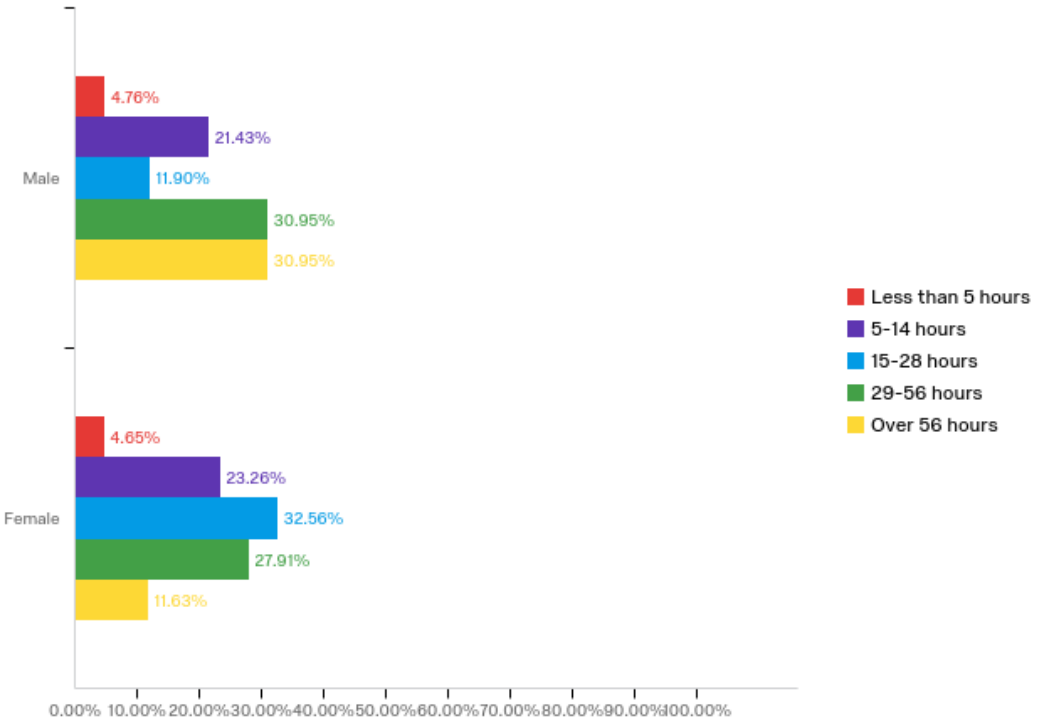

Figure 19. Survey response distribution by amount of time spent online in an average week, by gender.

When considering in which settings subjects routinely access the Internet, there is a significantly greater segment of males that use mobile devices connected to Wi-Fi at work (28.09%) than females (16.16%), and of females that use mobile devices connected to Wi-Fi while traveling (e.g., on foot or in a vehicle/train/subway) (19.19%) than males (7.87%) (see figure 20).

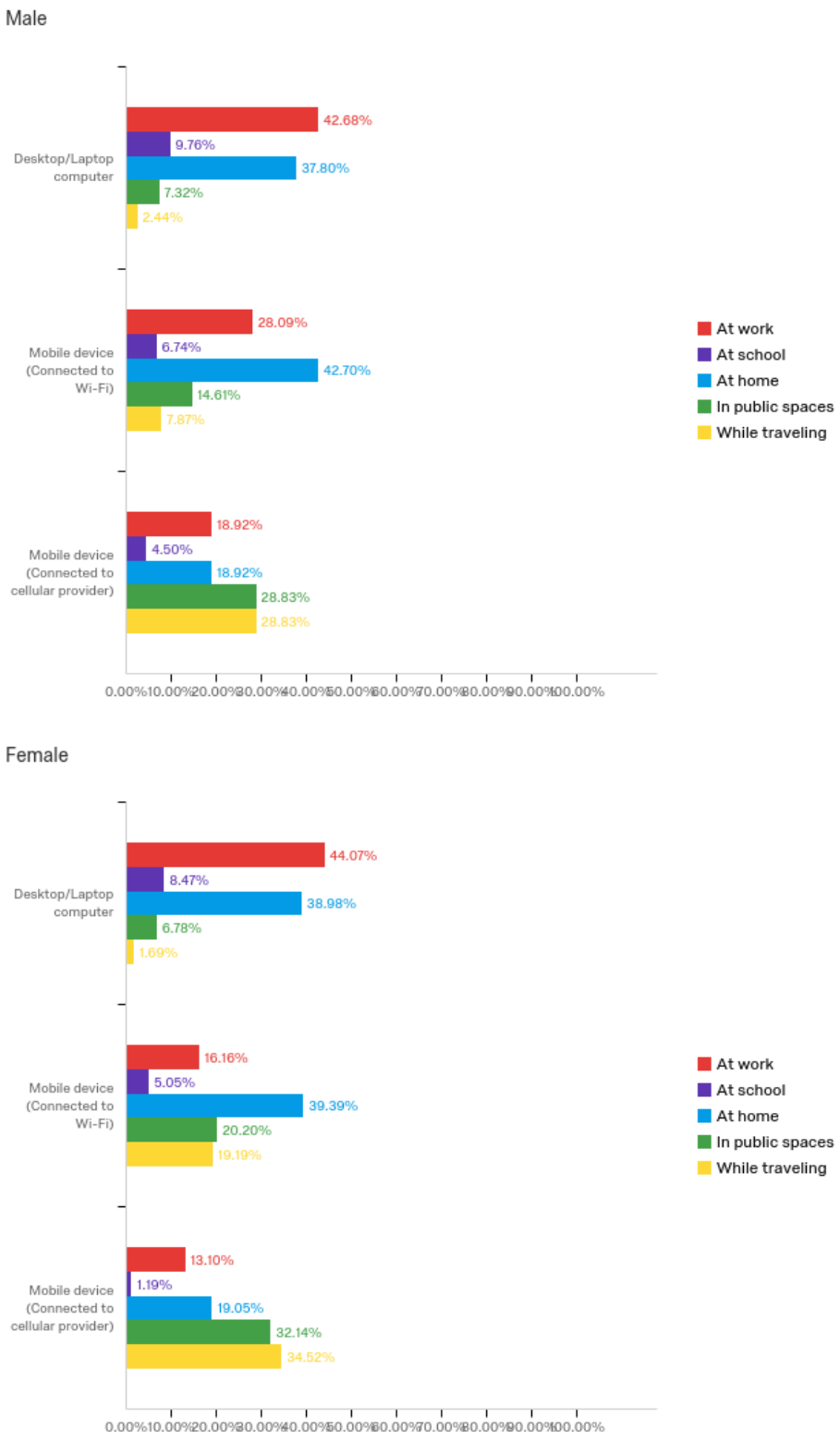

Figure 20. Survey response distribution by location/method of accessing the Internet, by gender.

When asked if the subjects use an anti-malware or other Internet security product on their desktop or laptop computer, or on their mobile device, 92.11% of males responded they did use an anti-malware or Internet security product on their desktop and/or laptop computer compared to 66.67% of females, while 45.24% of males responded they use an anti-malware/Internet security product on their mobile device compared to 11.90% of females.

Concerning the various scenario-based subjective questions, there was very much parity between male and female responses to each of the scenarios with no more than a 12% variance between any of the presented options across all scenarios.

Age Range. When considering the responses to the various questions across age range segments, there were no evident trends consistent with age. Lifestyle and work, school, or other commitments appear to dictate the settings for the use of the Internet more than age.

Level of Education. When considering the relationship between the amount of time spent online and level of education, four-year degree recipients are the highest users of the Internet (70.00% of those that responded 29-56 hours per week, and 60.00% of those that responded over 56 hours per week, completed a four-year degree). The level of education for those that use the Internet for 5-28 hours per week fluctuated, but those that reported using the Internet less than 5 hours per week were evenly distributed across all levels of education except doctorate (see figure 22).

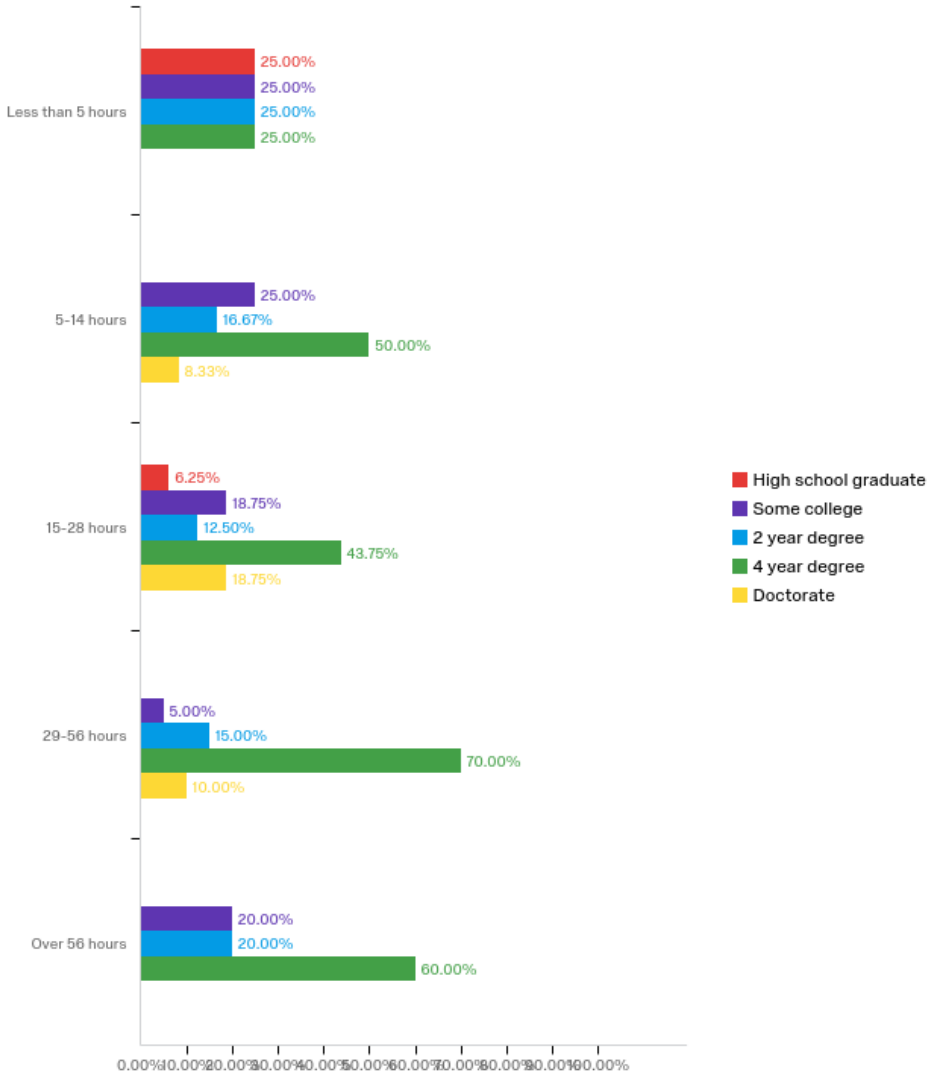

Figure 21. Survey response distribution by amount of time spent online in an average week, by level of education.

When considering in which settings subjects routinely access the Internet, there is a consistent response across all levels of education. There is a sharp increase in the use of an anti-malware or other Internet security product on desktop or laptop computers by those that have earned an associate or higher degree (from 83.33% to 87.50%, compared to 62.50% for those with some college) (see figure 22). The use of an anti-malware or other Internet security product on mobile devices does not follow the same trend, with 50% of those completing a two-year

degree responding they use such a product, compared to only 26.47% of those completing a four-year degree (see figure 23).

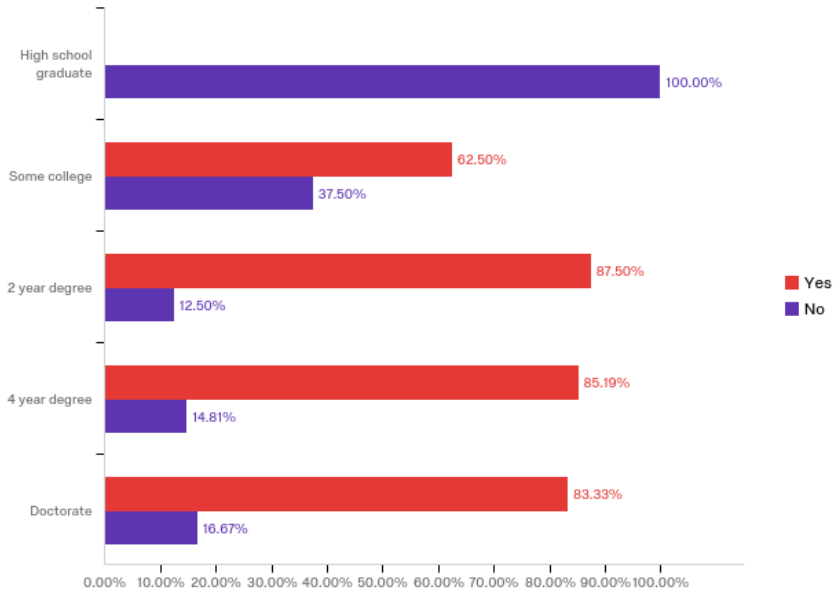

Figure 22. Survey response distribution by desktop/laptop anti-malware product, by level of education.

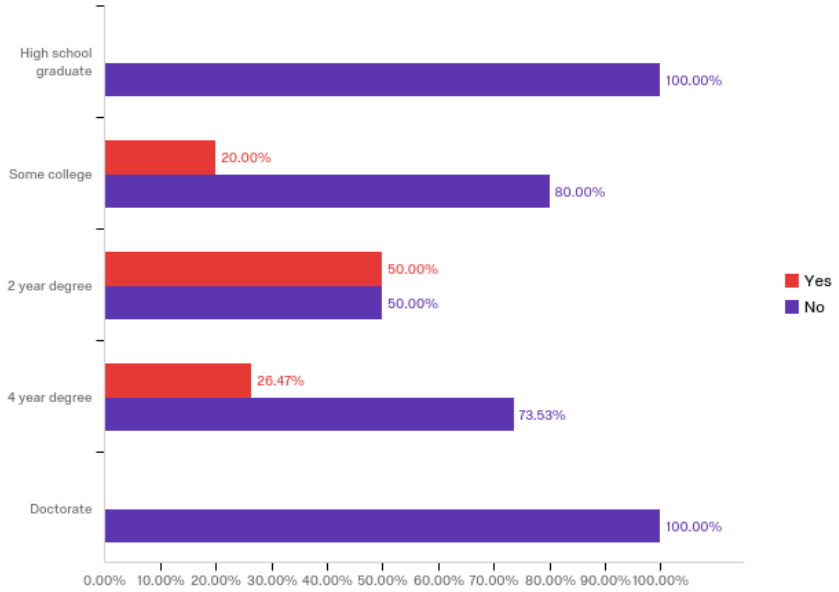

Figure 23. Survey response distribution by mobile anti-malware product, by level of education.

Q3 asks whether workplace training on social engineering prevention benefits an individual's protection against social engineering attacks in the personal/consumer setting, which requires analysis of the survey's scenario-based responses by a cross-section of those who responded that they have previously received formal training on social engineering prevention.

A review of the scenario-based responses finds that those subjects with prior formal training for social engineering prevention tend to respond to email-based social engineering attacks in their work/school use of the Internet by officially reporting the incident to their help desk or information security/awareness group (70.27% of those who have prior training) rather than simply deleting the email (70.73% of those who have not received prior training). The results do show, however, that formal training does not necessarily influence behavior when reacting to the same attack in their personal email; 81.08% of those with formal training would delete the email compared to 85.37% of those without formal training.

Discussion

The research put forth in this study seeks to determine how individuals can better protect themselves from being exploited by cyber-related social engineering attacks. To better understand the effects of social engineering, a combination of researching existing literature and a survey was used to conclude each of the specific questions.

Several of the research sources in the literature review (Algarni et al., 2013; Barker, 2016; Dhinakaran et al., 2011; Rader & Rahman, 2015; Thapar, n.d.; Wilcox & Bhattacharya, 2015) agree with the assertion that there is, in fact, a correlation between human behavior and the susceptibility to social engineering attacks. In particular, successful social engineers specifically target natural human behavior to solicit the desired response from their victims. Cultures which promote social interaction that forms trusting and open social relationships are the most vulnerable, and therefore most targeted (Wilcox & Bhattacharya, 2015). On the other hand, targeted individuals that are skeptical and scrutinize unsolicited contacts will be more likely to detect or avoid a social engineering attack (Butavicius et al., 2016).

The research in this study found that certain demographic groups exhibited online Internet behaviors that could place them at an elevated risk for victimization by social engineering. Younger subjects indicated high average Internet usage (50.00% of 18-24 year olds are online an average of 29-56 hours per week), using mobile devices as their primary Internet access, when 66.67% of the same subjects indicated they do not use an anti-malware or other Internet security product on their mobile device. This setting provides an opportunity for social engineering to be successful given the access to the audience and less preventive measures in place to avoid such an attack.

When evaluating whether workplace training on social engineering prevention benefits an individual's protection against social engineering attacks in the personal/consumer setting, the research found that behaviors between those who did and did not have previous training were fairly consistent (81.08% of this with prior training would delete a suspicious email, compared to 85.37% without any training; 64.06% with training would flag the email as spam or junk, compared to 39.02% without any training). Only 2.44% of subjects without prior training reported they would take a less desirable course of action (forward the email to a "tech-savvy" friend for advice). This data concludes that while social engineering prevention training benefits the enterprise by shaping desired behaviors in the workplace, these behaviors do not necessarily transfer to the personal setting.

As the research data was gathered for this study, one consideration that persisted was to determine if any methods or delivery mechanisms of social engineering prevention training could be designed to be more effective than what is currently available today. Research from Barker (2016) and Rader (2015) suggests the best approach is to provide training specific to social engineering as opposed to general "information security" training, deliver the training regularly and in small doses rather than one large course annually, and educate users to recognize the tactics employed by social engineers instead of simply teaching to identify the characteristics of a phishing website or email. The data collected in this study also suggests that additional emphasis must be placed on mobile device security as users are not applying the same degree of protection to their mobile devices as their desktop and laptop computers.

In addition to the recommendations above of how to improve the content of social engineering prevention training, there must also be a greater emphasis placed on delivery of the training. Presently, the majority of Internet users receive their training through their place of

work or academic institution. While various governments have campaigns that attempt to deliver the message, they tend to only reach those in the public that are actively looking for the information. Recommendations for improved distribution include organizations that are frequent touch points for average consumers such as financial institutions and utility companies, where they can provide short awareness topics during customer logins to their website and include messages in paper bills or statements.

For the human solutions to be effective, there must also be a technical solution that eliminates the bulk of social engineering attempts before they reach the end user. All email providers must strive to identify and block phishing and other social engineering emails before they are delivered to the user. Internet service providers and browser manufacturers should continue to block or warn users attempting to access social engineering websites, particularly as a result of following a link from an email. Mobile device manufacturers should seek to either embed added security into the device's operating system or built-in browser that provides phishing and social engineering protection, or provide guidance to users on the necessity for, and how to utilize, third-party services that offer phishing and social engineering protection.

Further research is recommended in evaluating the efficiency of suggestions provided in this study to determine whether there is any notable improvement in awareness and avoidance of social engineering attacks, as well as the optimal recurrence and method of social engineering prevention training delivery. Research into other potential partners and sources for training delivery that provides the greatest audience to effort ratio is also recommended.

References

Algarni, A., Xu, Y., Chan, T., & Tian, Y. C. (2013). Social engineering in social networking sites: Affect-based model (pp. 508–515). Presented at the 2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013, IEEE. http://doi.org/10.1109/ICITST.2013.6750253

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. http://doi.org/10.1016/j.chb.2014.05.046

Barker, J. (2016). How to hack a human. Presented at the InfoSecurity Europe 2016.

BBC News. (2010, March 18). Hacking "fun" for British teens. Retrieved July 30, 2017, from http://news.bbc.co.uk/2/hi/technology/8574259.stm

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016, May 28). Breaching the human firewall. *arXiv.org*.

Center for Cyber Safety and Education. (2017). Internet security education.

Chumbow, B. S. (2012). Social Engineering Theory: A Model for the Appropriation of Innovations with a Case Study of the Health MDGs. In *Social Sciences and Cultural Studies - Issues of Language, Public Opinion, Education and Welfare*. InTech. http://doi.org/10.5772/37677

Cyber Security Awareness Alliance. (n.d.). GoSafeOnline. Retrieved July 30, 2017, from https://www.csa.gov.sg/gosafeonline/

Data Security Council of India. (n.d.). Cyber security awareness. Retrieved July 30, 2017, from https://www.dsci.in/taxonomypage/349

Dhamija, R., & Tygar, J. D. (2005). The battle against phishing: Dynamic Security Skins.

Proceedings of the 2005 symposium on Usable ... (pp. 77–88). ACM. http://doi.org/10.1145/1073001.1073009

Dhinakaran, C., Nagamalai, D., & Lee, J. K. (2011, August 7). Multilayer approach to defend phishing attacks. *arXiv.org*.

Gharibi, W. (2012, January 4). Some recommended protection technologies for cyber crime based on social engineering techniques -- phishing. *arXiv.org*.

Goodin, D. (2012, June 19). Google bots detect 9,500 new malicious websites every day. Retrieved July 30, 2017, from https://arstechnica.com/information-technology/2012/06/google-detects-9500-new-malicious-websites-daily/

Hasan, M., Prajapati, N., & Vohara, S. (2010, June 19). Case study on social engineering techniques for persuasion. *arXiv.org*. http://doi.org/10.5121/jgraphoc.2010.2202

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. http://doi.org/10.1145/1290958.1290968

Morgan, S. (2016, August 17). Hackerpocalypse: A Cybercrime Revelation - Herjavec Group. Retrieved June 25, 2017, from https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/

National Cyber Security Centre. (2016, August 4). 10 Steps to cyber security. Retrieved July 30, 2017, from https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Nyirak, A. (n.d.). The attack cycle. Retrieved July 30, 2017, from https://www.social-engineer.org/framework/attack-vectors/attack-cycle/

PCI Security Standards Council, LLC. (2015). Defending against phishing and social engineering attacks. *pcisecuritystandards.org*.

Ponemon Instiute, LLC. (2015). *The cost of phishing and value of employee training*.

Rader, M., & Rahman, S. (2015, November 30). Exploring historical and emerging phishing techniques and mitigating the associated security risks. *arXiv.org*. http://doi.org/10.5121/ijnsa.2013.5402

Rouse, M. (2006, February). What is ISP (Internet service provider)? Retrieved July 9, 2017, from http://searchwindevelopment.techtarget.com/definition/ISP

Rouse, M. (2016, April). What is ransomware? Retrieved July 9, 2017, from http://whatis.techtarget.com/definition/ransomware-cryptovirus-cryptotrojan-or-cryptoworm

Rouse, M., & Bacon, M. (2016, February). What is social engineering? Retrieved July 9, 2017, from http://searchsecurity.techtarget.com/definition/social-engineering

Rouse, M., & Bacon, M. (2017, March). What is spear phishing? Retrieved July 9, 2017, from http://searchsecurity.techtarget.com/definition/spear-phishing

Rouse, M., & Cobb, M. (2015, October). What is phishing? Retrieved July 9, 2017, from http://searchsecurity.techtarget.com/definition/phishing

Rouse, M., & Wigmore, I. (2013, June). What is enterprise IT? Retrieved July 9, 2017, from http://searchcio.techtarget.com/definition/enterprise-IT-enterprise-class-IT

Rouse, M., & Wigmore, I. (2016, January). What is threat actor? Retrieved July 9, 2017, from http://whatis.techtarget.com/definition/threat-actor

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? Presented at the CHI 2010, Atlanta.

Spam decreasing, but social media phishing soaring says Symantec. (2010). Spam decreasing, but social media phishing soaring says Symantec. *Infosecurity*, *7*(6), 6. http://doi.org/10.1016/S1754-4548(10)70096-6

Thapar, A. (n.d.). Social engineering. Retrieved July 30, 2017, from

http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf

Turkel, D. (2016, April 7). Victims paid more than $24 million to ransomware criminals in 2015 — and that's just the beginning. Retrieved June 25, 2017, from http://www.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4

U.S. Department of Homeland Security. (2017). Stop.Think.Connect. Retrieved June 25, 2017, from https://stopthinkconnect.org/

Wilcox, H., & Bhattacharya, M. (2015, November 21). Countering social engineering through social media. *arXiv.org*.

Wu, T. (n.d.). SRP: Industry-Standard Strong Password Security. Retrieved July 30, 2017, from http://srp.stanford.edu/

American Public University System
American Military University
American Public University

Institutional Review Board (IRB) Approval Letter

Application Number: 06-2017-084

Application Title: Combatting Cyber Social Engineering in the Digital Age

August 4, 2017

Dear Nicholas McLarty,

The APUS IRB has reviewed and approved the above application.

Date of IRB approval: **08/04/2017**

Date of IRB approval expiration: **08/03/2018**

The approval is valid for one calendar year from the date of approval. Should your research using human subjects extend beyond the time covered by this approval, you will need to submit an *extension request form* to the IRB.

Changes in the research (e.g., recruitment process, advertisements) or informed consent process must be approved by the IRB before they are implemented. Please submit a *protocol amendment form* to do so.

It is the responsibility of the investigators to report to the IRB any serious, unexpected, and related adverse events and potential unanticipated problems related to risks to subjects and others using the *unanticipated problems notification*.

Please direct any question to apus-irb@apus.edu. The forms mentioned above are available on our IRB Application page; listed under downloadable documents.

Sincerely,

Jennifer Douglas, PhD
IRB Chair