Honor Code Statement

By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/the-mason-honor-code-2/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site.

Harrison Murdock
Introduction

The Internet is one of humanity’s greatest technological achievements. Individuals, businesses, governments, educational institutions, healthcare providers, and every other institution one can imagine from every facet of human life relies upon the Internet in one way or another every day (Horrigan & Rainie, 2006). The Internet continues to pave astounding and crucial new electronic highways to enrich human interaction, information-sharing, and advancement. However, despite all the benefits it provides for unprecedented engagement, interaction and growth, the Internet also harbors many risks and dangers from cybercrimes (Leefeldt, 2017). In fact, this paper aims to discuss the threats posed by phishing and hacking and to outline helpful strategies and resources to combat the darker side of the Web so users may be better educated to avoid pitfalls and predatory practices in the future.

Current Uses

Cyber criminals use phishing and hacking to harm and rob as many people as they possibly can. They usually do their phishing from great distances and in the shadows far from the public view (Leefeldt, 2017). Phishing essentially mimicks legitimate Websites or reputable businesses in order to trick Internet users into disclosing sensitive information—particularly private information such as bank account numbers and other financial information—through common digital communication channels like email, texts, and instant-messaging (FTC, 2017). Phishers go to great lengths to project
authenticity to convince users to fall for bogus information and traps. Simply put, phishing is a form of computer fraud which has become increasingly sophisticated, deceptive, and effective in fleecing millions of dollars out of unwitting victims every year (Upton & Creese, 2014).

In fact, in 2008, the United States Justice Department defined phishing as any type of scheme that uses Internet components such as emails or websites to carry out fraudulent transactions (Daejoong, 2013). Phishing also strips people of crucial and sensitive personal information like their passwords, medical information, and social security numbers in order to access and retrieve as much specific and identifying information as possible. And once the information has been stolen, middlemen peddle the information through a vast network of underground clients and malware marketplaces known as the dark web which is nearly impossible to trace—wreaking much havoc and difficulty on the party robbed (Upton & Creese, 2014).

Although young people and seniors receive a great deal of attention for being frequently targeted, the fact is any person or organization can fall prey to this crime. For instance, a well-educated and street-smart friend of mine recently lost over $27,000 from an Internet phishing scheme. He received an email he presumed was from Amazon Prime since the email featured Amazon’s logo and other trustworthy identifying information when it informed him that Amazon Prime owed him $250.00, and wished to credit him the money. However, Amazon first needed my friend’s banking information—which he happily provided. The lure of extra money clearly blinded my friend to the risks of disclosing his financial information over the Internet. And shortly thereafter, the Amazon Prime imposters completely drained my friend’s bank account.
Unfortunately, he is still trying to recover the money today. And sadly, this is not an unusual story.

It turns out most people feel they are too smart and Internet savvy to get scammed, cyber security researchers from the University of San Antonio discovered. Their study found that many Internet users feel “overconfident” when it comes to recognizing tactics designed to swindle them out of their hard-earned money (Wang, Li, and Rao, 2017). According to the study, this overconfidence often exposes users to greater vulnerability and risk.

“In any of these situations, overconfidence is always a killer,” H. R. Rao, one of the researchers said. "Our study's focus on different types of over-confidence is unique, and allows us to understand why certain tactics appeal to different people.” The good news is that, according to Rao, “[the findings]will help us to figure out ways to teach people to guard against these kinds of methods." What’s more, according to cybercrime experts, most phishing ploys use logical appeals, causal reasoning, emotional triggers, and promises of great reward to entice the user to perform the desired behavior (Daejoong, 2013). Appeals to users’ common sense often override the users’ own judgment and internal alarm system, prompting them to divulge critical information.

Security Issues and Concerns

However, it’s not just individuals getting targeted. Small businesses, large corporations, academia, healthcare providers, and even our government are all vulnerable to attack, which could lead to tremendous losses for all concerned and could also create
substantial security risks since phishers and hackers often place spyware and other malware on computers to monitor or even sabotage victims. This definitely creates enormous security breaches that could threaten individuals, businesses, and even national security. One need only consider the recent large-scale computer attack known as “Wannacry” to understand the gravity of the growing security risks. According to CBS News, “a hacker group that calls itself Shadow Brokers stole a cyber security weapon called Eternal Blue from the U.S. National Security Agency, loaded it onto the dark web and turned it against us,” which ground many businesses and service industries to a complete stop, including hospitals and doctor offices. With the possibility of more attacks like this one on the horizon, it has never been more important to educate and protect the public, especially as Internet usage and social media outlets continue to grow in popularity.

In fact, a user vulnerability study conducted by Dr. Arun Vishwanath, which appeared in the Journal of Computer-Mediated Communication, showed that Facebook users can be particularly susceptible to phishing attacks. "Social media phishing is the attack vector of choice among cyber criminals and has been implicated in crimes ranging from home invasion to cyber bullying, illegal impersonation…and espionage," Dr. Vishwanath said. "These scams…trick people into accepting friend requests…. Hence, understanding why individuals fall victim to social media phishing scams is important from an organizational security, law enforcement, and a national security standpoint," Vishwanath added.

Dr. Vishwanath’s observations underscore the security challenges U.S. intelligence agencies face today from the growing threat of phishing and cyber warfare.
Investigative journalist Eric Schlosser recently wrote, “Without a single bullet, bomb, or missile, a foreign enemy can now launch a devastating attack on the United States…. Cyber warfare threatens all of us” (Koppel, 2015). And conservative journalist George Will added, “Try to imagine what a malevolent government—armed with the latest computer sophistication—could do to another nation’s complex and entirely digital-dependent economy and social infrastructure” (Koppel, 2015). And the reality is, many cyber security experts believe we have only seen the tip of the iceberg in terms of how phishing and cyber warefare could disrupt and dismantle our infrastructure, particularly our electric grids and transportation systems (Koppel, 2015). And given the great losses and damage that has resulted in the past and could still come to pass in the future, prevention is key.

Ethical and Social Implications

Despite the profound sense of urgency and critical need to prevent cyber crimes, there are many ethical and social implications to consider when trying to police and regulate the Internet to stop phishing and hacking since the Internet has no borders or international laws to speak of. Few hackers are ever caught or prosecuted for their crimes due to the shadowy and transient nature of organized crime on the Web since many of them operate overseas and are virtually untouchable. And if these crime ring thugs were ever identified, extraditing them to the U.S. would likely involve complicated and awkward diplomatic considerations that would test and strain foreign relations.
That’s not to say criminals should not be brought to justice. It is just simply acknowledging the intricacies and difficulties of such an endeavor. These diplomacy issues are just one of the reasons why the United States has struggled with developing a firm and fast cyber security plan and policy.

Admiral Rogers, chief cyber security chief under President Obama and former head of the National Security Agency (NSA), addressed these problems when he testified before Congress back in March 2015. “We’re at a tipping point. The threat is growing,” he stated. “We need to think about: How do we increase our capacity on the offensive side to get to that point of deterrence? [Because] in the end, a purely defensive, reactive strategy will be both late to need and incredibly resource-intense,” He emphasized that there is “a persistent presence on our networks” and “a strong direct linkage” between “individual” hackers in Iran, Russia, and China, with “the nation state directing” a cyber attack in the future (Sanger, 2015).

Arizona Senator John McCain agreed. “The failure to develop a meaningful cyber-deterrence strategy has increased the resolve of our adversaries and will continue to do so at a growing risk to our national security,” McCain warned (Sanger, 2015).

What the Future Holds

Robust phishing schemes and malignant cyber attacks are likely to not just continue, but to increase in the future—particularly if the U.S. continues to waffle over where it stands on cyber security. However, Americans are not completely helpless and at the mercy of the machinations of hackers. The government does provide resources to
help Americans better protect themselves and offers education and training on the
OnGuardOnline.gov website on how users can take steps to avoid and report phishing
schemes. Additionally, the FTC website offers vital consumer tips such as:

- Use Security Software That Updates Automatically
- Treat Your Personal Information Like Cash
- Check Out Companies to Find Out Who You’re Really Dealing With
- Give Personal Information Over Encrypted Websites Only
- Protect Your Passwords
- Back Up Your Files (FTC, 2017)

Clearly, however, more needs to be done to match wits those who wish to
infiltrate and disrupt our digital economy. Additionally, the major protection and
preservation of our infrastructure and our very way of life must come from our leadership.
So, in closing, it is vitally important for the U.S. to take steps to anticipate and prevent
cyber crimes in the future. Congress needs to move from denial and indifference to
concern and action. Even in the face of delicate international and social implications,
America needs to take a preemptive and preparatory stance on cyber crimes. In fact,
America—now more than ever—needs to dispel that disheartening belief that former
First Secretary of Homeland Security Tom Ridge declared in frustration and dwindling
hope when he said, “We are not a preemptive democracy. We are a reactive one. Rare
are the occasions on which we act in anticipation of a potential problem” (Koppel, 2015).
Instead, America needs to show strength, courage, integrity, and readiness. And finally,
we as humans must shape and define technology, rather than letting the dizzying and out-of-control nature of technology shape and define us.

References

 Retrieved on May 30, 2017, from:
http://search.proquest.com.mutex.gmu.edu/pqrl/docview/1449417841/
D2B431DEo5E44o83PQ/4?accountid=1451

 Retrieved on May 29, 2017, from
https://www.washingtonpost.com/news/arts-and-entertainment/wp/2014/03/12/36-ways-the-web-has-changed-us/?utm_term=.08cb2963a42e

 Retrieved on May 29, 2017, from
https://www.consumer.ftc.gov/articles/0003-phishing

Retrieved May 29, 2017, from


http://searchsecurity.techtarget.com/definition/phishing


www.sciencedaily.com/releases/2017/01/170109092600.htm
Wang, Jingguo; Li, Yuan; and Rao, H. Raghav. (2017) Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, Vol. 17 Iss. 11, Article 1