Navigating the Dangerous Waters of Phishing Attacks within Microsoft Programs

Joshua Morton

Old Dominion University

CYSE 280 - Windows Systems Management and Security

Professor Gladden

April 7, 2024

Introduction

In 2000, the ILOVEYOU virus infected computers throughout the world, causing $5.5 million dollars in damages. The virus was spread through a false love note email. In 2009, Coca-Cola had their personal data and operating systems hacked through a malicious PDF file found in targeted emails to executives (Hadnagy & Fincher, 2015, #8). In 2013, the biggest personal data breach in history affected Target through an email clicked on by a Target HVAC vendor with network credentials (Hadnagy & Fincher, 2015, #8). All of these targets had been victims of an often overlooked initiator of cybersecurity attacks: phishing. Although phishing is considered a form of social engineering, it is most definitely a pivotal part of initiating the hacking process. As such, it is equally pivotal to ask what phishing is, how the use of social engineering lures victims into being attacked, what we can learn from previous attacks on Microsoft systems, and the effects of phishing attacks on Microsoft systems, along with what can be done to prevent them in the future. This research paper seeks to investigate the ideology of phishing and its effects on victims, notable attacks on certain Microsoft systems and the specifics of how they occurred, and finally, frameworks and tools to create a better understanding of phishing attacks and to better prevent them.

Research Overview and Analysis of Phishing

The purpose of this essay's research is to analyze the social engineering measure of phishing and how it works to initiate a full-on hacking attack. When analyzing phishing attacks, it is important to understand that phishing cannot be simplified into a system that purely works through a linear system of emails and websites but through a combination of technical knowledge of malware and websites but rather work in a system of psychological manipulation and reliance on human vulnerabilities and oversights. It is also important to understand that although phishing attacks do not only apply to Windows operating systems, many large-scale attacks play off of the vulnerabilities of older systems as well as the abundance of its usage. With the fact that phishing directly affects Windows systems, it is time to explain what exactly phishing is and why it occurs. When phishing is used in a cyber attack, it is implemented in a multi-step process in which they first harvest information about a victim, implementing a social engineering tactic, gaining access to a victim's system through the use of coercion tactics which deceive a victim into clicking a malicious file or providing their private information. After access is gained, hackers employ malicious code that then capitalizes on unpatched exploits into Windows systems and then employ a system of data encryption or theft. (Sonowal, 2021) Phishing scams employ a multitude of methods for social engineering, including creating phishing emails, fake websites, and fake malicious software that play into the curiosity or fear of their victims to elicit a drastic or uneducated response to the engineering that leads to the initiation of the attack.

To have a better understanding of the methodology and process behind phishing it would be beneficial to look at a real world example of phishing leading to a substantial amount of damages monetarily. In 2014, Sony Pictures Entertainment announced that they would be producing and releasing a movie known as *The Interview, a comedy* movie in which two members of the CIA are sent to North Korea to assassinate North Korean leader Kim Jong Un. After the movie had been announced a group of hackers allegedly representing North Korea, known as the “Guardians of Peace” had begun their process of attacking Sony Pictures Entertainment. The Guardians of Peace began the attack with a process known as spear-phishing, a form of phishing in which attackers specifically target individuals through phishing with access to sensitive information. The targets of the phishing attacks had been Sony Pictures executives that had access to full databases with files of the movie, the GOP had sent emails with links to impersonated versions of websites in which the executives had given all of their personal and work information to. (DeSimone & Horton, 2017, #6) Once the information that was needed for the hack were stolen, for example, IP addresses, the hackers had used a SMB block exploit to gain access to computers containing the movie and create a backdoor. Once the backdoor was created the hackers then stole data pertaining to the movie and personal information from other Sony employees to also hack into their computers. After the attack was finished most of the *Interview* had been stolen or deleted, thousands of employees' data had been stolen, and had lost over 41 million dollars beginning simply with a sphear-fishing email. Two lessons learned from this attack that help to clue in on the vulnerabilities phishing can have on Windows systems are the technical oversights of running organizations on older Windows software and the lack of training in regards to company and network safety from social engineering attacks. A large oversight by the network security professionals at Sony was the very exploit that was clicked on by executives which had been an SMB exploit most influential on older windows operating systems that had not been updated or monitored securely at the Sony Pictures offices. Secondly, network security professionals at Sony had not properly trained high executives and producers with proper techniques for understanding and preventing phishing leading to their leak of data and the gaining of access for hackers.

Frameworks and Processes to Follow to Train For and Prevent Phishing Attacks.

Prevention of Phishing attacks can be separated into two parts; a technical system and an employee based organizational training system. Phishing relies on psychological thinking as a part of its social engineering processes meaning that it relies primarily on human error and feeling. Creating a training framework for Phishing must include different factors to both make it digestible for organizational employees to understand as well as be effective in actually mitigating attacks. The first part of the mitigation framework should include a complete rundown of what fishing is and how it may try to manipulate victims. According to the 2018 EY Global Information Security survey, it was found that most workers that have fallen victim to phishing scams attribute their deception to a lack of knowledge about what they even are (Mohammad et al. 2015). So starting off by providing engaging informative lectures that provide information on what phishing is can start the process of retention for phishing mitigation. The second part of the mitigation framework can be based on physical training with systems that simulate phishing attacks through methods such as cooperative learning, problem-solving training, and simulation training (Sonowal, 2021). The third part of the system would include a framework that improves decision making amongst employees.

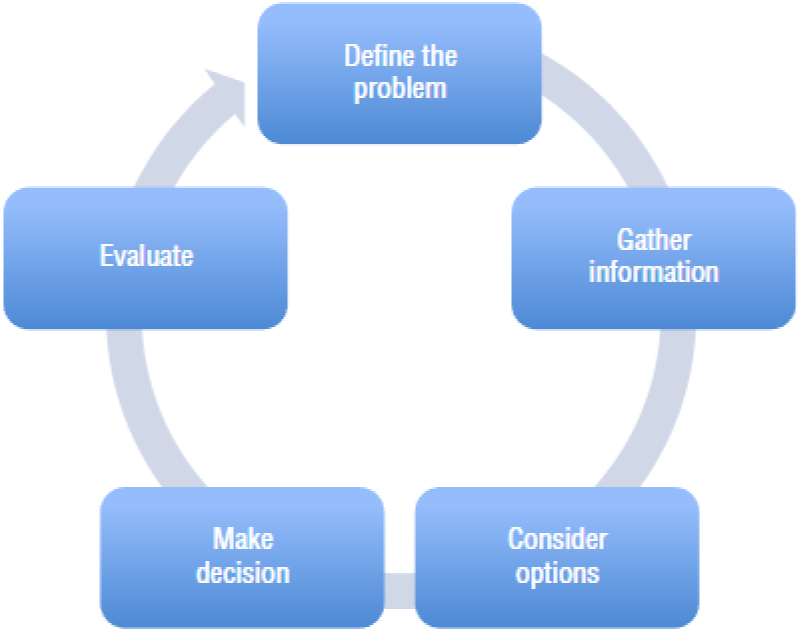

Figure 1 (Sonowal, 2021, #50)

As shown above a five step decision making process can help employees tackle the psychological challenges of dealing with phishing attacks. Understanding a problem, collecting information on the problem, considering the viable options of the problem, making a decision, and evaluating is important in terms of phishing because it creates a psychological defense to the social engineering tactics of fear and curiosity employed by phishing. For example, when a hacker sends a phishing email claiming that your files are compromised you may want to implement a decision making process by defining what might be wrong, collecting information on the sender and checking the link before clicking it, consider your other options in checking the validity of the claim, making a decision not to click it, and evaluating the possible damages if you had fallen for it.

When this training system is implemented it may also be important to remember some processes that will further the mitigation of phishing attacks. Falsified websites have been found to be extremely effective in phishing attacks so it is important to understand when given an email with a link to a website you must verify exactly every part of the site before your information is inputted. It is also important to realize and understand what is happening on your computer thoroughly as to prevent a manipulation of someone's lack of knowledge when performing processes. Finally, and most importantly, one must understand their own emotions and learn to control them in the event a phishing attack seeks to psychologically affect you into desperately clicking a malicious link (Sonowal, 2021).

Tools and Resources for the Mitigation of Phishing Attacks.

Although phishing relies on social engineering as its propelling factor in attacks and employee training is very important in the mitigation of phishing attacks it is also important to outline the technical tools and resources for preventing attacks. There are multiple techniques to identifying phishing links and attacks; for example, a whitelist and blacklist based approach entails a system in which a system administrator blacklists and whitelists certain keywords or phrases from email lists and website URLs to prevent phishing attacks from happening and prevent organizational members from making poor decisions. Examples of tools using a blacklisting and whitelisting system include Google's Safe Browsing system that has a catalog of blacklisted keywords and techniques used by hackers in phishing attacks and when found blocks the link. When false websites are created the problem arises of distinguishing between a real website and a malicious one. Systems such as the DOM similarity system make use of a tree of processes that help to determine the similarities and differences of malicious sites.

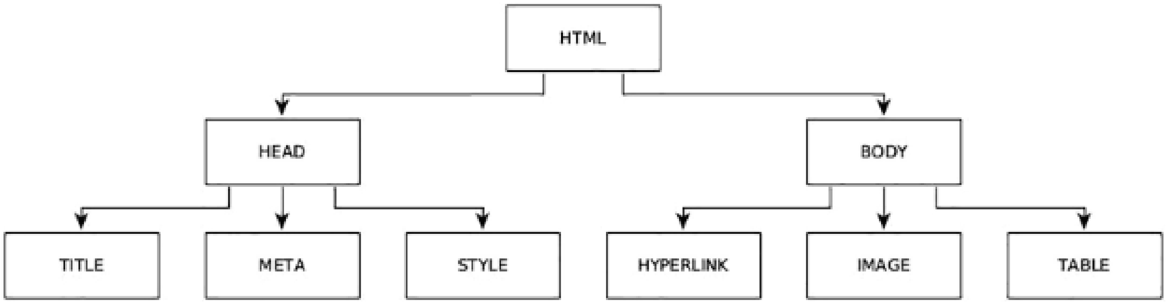

Figure 2 (Sonowal, 2021) *The Process of which a DOM system moves through two websites determining their similarities and differences.*

Conclusions

After analyzing the characteristics of phishing attacks, why they happen, and how exactly they happen with the example of the 2014 Sony Pictures, many lessons can be learned on the severity of phishing and its effect on Windows systems. Understanding the process of social engineering that phishing attacks use and its manipulation of psychological features was found to be the basis at which even the most technologically knowledgeable may fall victim too only leading to the full control of their systems due to Windows vulnerability system exploitations. The analysis and timeline of the 2014 Sony Picture helped to outline the complete process beginning with the spear-phishing social engineering of Sony executives and its eventual progression to the full data leak caused by vulnerabilities created from Microsoft and organizational missteps in regulating assets. Finally, providing tools and methods for creating a system of training and knowledge while also implementing technological systems helped to better create a sense of mitigation towards phishing's effects technologically and psychologically.

References

Akanbi, Amiri, I. S., & Fazeldehkordi, E. (2015). A machine-learning approach to phishing detection and defense (1st edition.).

DeSimone, A., & Horton, N. (2017). Sony's Nightmare Before Christmas. *National Security Report*.

Hadnagy, C., & Fincher, M. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. Wiley.

Hadnagy, & Wilson, P. (2010). *Social Engineering [e-book] The Art of Human Hacking.* John Wiley & Sons.

Middleton. (2017). *A History of Cyber Security Attacks* (1st ed., Vol. 1). Routledge. https://doi.org/10.1201/9781315155852