Cyber Phishing: Recognizing and Countering Phisher’s Attacks and Schemes

09/20/2022

ISSC451 Cybercrime

Corbin Osman

Jeremy Livingston

With technology growing each and every day, there are many innovations that provide greater benefits and capabilities to members of society. At the same time, however, these newer developments provide more tools and avenues to those who work committing crimes in the digital world. Over the last few decades there have been many new methods that criminals use in order to achieve their goals in cyber activity.

Within the vast realm of different types of cybercrime is the criminal act of phishing. This paper will focus on this type of cyber-attack and explore the reasons it is performed. In today’s world of increasingly growing technology, it is important for individuals and organizations alike to understand the intent of phishing attacks and schemes, know how to identify and respond to them, and recognize what they can do to prepare for and protect against future phishing threats.

To help us understand what a phishing attack is, it would be beneficial to know what category of crime this activity falls under. Phishing is one of many schemes that are termed social engineering attacks, which are performed with different goals in mind. One goal may be to obtain personal information from an individual or business, and another may be the intent to disrupt or damage system services through delivering dangerous software such as malware or ransomware. The reasoning behind social engineering attacks will depend on the individual or group performing them, but they generally involve the intent of tricking another into accepting or receiving harmful software or data.

One example of a social engineering attack is the phishing scheme. Similar to the definition given before, phishing is the act of obtaining information from others without consent through forms such as emails, messages, and services. Further elaborating on this, Robert Grimmick gives us a deeper understanding of this scheme in an article on phishing. He shares that phishing “targets the weaknesses of human psychology rather than technical vulnerabilities” (Grimmick, 2020). The intent of a phisher is to mask oneself and pretend to be a legitimate business or individual with the goal of obtaining information from them. Those who believe that they are communicating with the real person or business may share their information, not realizing that they have given it to someone other than who they believe received it.

One strong example of how this can be performed is through the use of a fake website that has been designed to appear as a legitimate one. If a phisher were to create their own website that looks similar to one an individual wants to access, they may attempt to sign-in with their login credentials to the fake website. In turn, the website is able to capture that individual’s credentials and whoever obtained the information would be able to access the victim’s profile within the real site. This is just one of many ways phishing attacks can be employed without those targeted recognizing what has occurred.

The act of phishing can occur both within a technological environment as well as outside it in the physical world. Digital phishing attacks are commonly attempted through emails, social media messaging services, and text messages, with the intent to have the target interact with the phisher. For similar attacks outside of the use of technology, a phisher may obtain information by having their target fill out a form with personal information. One may also masquerade as an individual they are not, such as a maintenance or IT worker, and obtain information by interacting with others who trust the phisher is who they say they are. Another method that can be considered both in and outside of digital technology is through phone calls. A phisher can make calls pretending to be a trusted individual, and if the victim is not careful, they could share confidential information that the phisher is searching for.

Now that we have a better understanding of the nature of phishing attacks, we can explore several sub-types of phishing more in-depth. Generally, phishing attacks may be aimed at a large audience with the goal of capturing information from as many people as possible who will fall for the scheme. With no specific target in mind, this method of phishing can often yield a large number of results for the attackers. In contrast, spear phishing is an attack method targeted at a specific individual or group. Instead of attempting to obtain information from anyone who may interact with a scheme, this phishing method aims to receive the information sought after from a specific party through a social engineering attack. This can be attempted by parties who gather information to create emails or messages that may look real but are in fact fake in nature. Because the target audience may believe the email or message to be legitimate, they may share their confidential information with the attackers. To help avoid falling victim to a spear phishing attack, always check the legitimacy of any emails or messages you receive, whether inside of work or in your personal life. Furthermore, be wary of any emails or messages that request you share confidential information, as these may be attacks aiming to capture sensitive information.

A similar form of phishing is whaling. The goal of whaling is the same as spear phishing, but the difference is found in the target audience. Whaling attacks are normally aimed at individuals within a company or business who have elevated privileges, such as a CEO or other management official. While it may be difficult for an attacker to trick a higher-up with a phishing attack, they may instead attempt to masquerade as the management official and ask for information from others within the company. The attacker might ask for confidential information from one of the business’ employees, and should the employee believe the request from their leadership to be legitimate, sensitive information could be given to the phisher. To protect against this social engineering scheme, all employees should confirm if these emails or messages truly originate from the person claiming to have sent them. To further ensure safety of confidential information, a business or organization would benefit from having policies in place that prohibit the transfer of confidential information over email or message.

Another common type of phishing scheme is pop-up phishing. Individuals who have used internet services before have most likely run into a pop-up scheme at some point as they are common throughout the digital world. The intent of a pop-up attack is to get a victim to click within the pop-up to allow certain services to run. Many websites require functions to be enabled by allowing them to run through a pop-up that appears. While generally harmless, attackers can insert malicious code into pop-ups. Once a target allows the pop-up feature to run, it may download the malicious code onto the victim’s device. To stay safe while interacting with pop-ups, ensure to only allow those that you are familiar with. If you question whether or not you need to allow a certain feature through a pop-up, research its validity or ask for the opinion of others who may know more about the software needing to be ran.

There are many other forms of phishing attacks that fall into other categories. One attack, known as an evil twin attack, is performed by using a fake network or internet Wi-Fi connection that looks similar to one normally used. When a victim accesses this fake connection, the attackers can capture sensitive data that is transmitted across the network. This scheme may commonly be found in public areas such as a library or airport where free public Wi-Fi is offered. Another subtle attack, called angler phishing, is commonly used inside of social media. A phisher using an angler phishing scheme may act as a customer service representative or agent and interact with a social media user who is attempting to fix issues they have with their account. The attacker asks for account information in order to help the user, while their real intent is solely to capture their credentials. Two final sub-types of phishing attacks are smishing and vishing, the former being phishing attacks used over SMS messaging and the latter involving the use of voice messages or calls to talk with someone in order to obtain information.

With all of the aforementioned forms of phishing attacks, it is important to recognize potential attacks and know how to respond to them accordingly. It is good practice to ensure that login credentials are kept secure and never shared with anyone else. Similarly, only interact with emails, messages and links that originate from within the organization or place you work to avoid accessing anything that could be malicious. Outside of the workplace, be wary of interacting with individuals who you do not know personally. Additionally, be cautious of the accounts of those who you do know when their activity seems suspicious and does not follow their normal habits as it is possible that someone else has taken over their account.

It is important to recognize that the majority of phishing attacks require the target victim to interact with a link of some sort. Depending on the type of phishing scheme and the information the attackers are seeking, the location the link leads can differ. A blog post by Security Scorecard shares insight into the purpose of using links in a phishing scheme, stating that “the links traditionally go to malicious websites that either steal credentials or install malicious code, known as malware, on a user’s device” (Security Scorecard, 2021). One phisher may attempt to obtain sensitive login credentials, while another may have the intent to load malicious files and software onto the systems of another individual or business.

With this in mind, it should be a focus of each individual and business to ensure that they understand the dangers of social engineering attacks and know how to properly handle them should they encounter one. There are several ways to protect oneself digitally while using technology and developing strong safety habits will keep users more protected from social engineering attacks and schemes.

Many email services have filters that work to keep spam or suspicious emails from entering the inbox, but there are additional steps that one can take to increase the protection of their devices and personal information. One action is to install security software that works to protect the system. Security software regularly monitors the system it is on to detect any type of malicious content, such as malware or ransomware. One can also scan the system the software is on to find any dangerous software or files in order to clean the system and rid itself of the harmful data. Security software should be updated regularly in order to keep up to date with newer digital dangers.

There are many ways users can better protect their online accounts. For accounts that require users to log in with a username and password, this information should be kept confidential and never shared with others. For separate services it is recommended to use different passwords as well. If the same password is used across multiple accounts and an attacker obtains the login credentials, they then have access to the other accounts. Passwords and other information should be updated regularly as well to ensure that accounts remain secure.

Another safety measure that can be put in place is multi-factor authorization. This is the act of requiring multiple security credentials in order to login. A blog post by the Federal Trade Commission offers a few additional security credentials that can be used by individuals to better secure their accounts. Separated into three categories are credentials that you know, credentials that you have, or something that you are. Within the first are credentials that only you know, such as a PIN code or a security question. Second are credentials that you have or receive, such as a one-time passcode you receive through an email or message. Third are credentials that are based on your identity. This can be a fingerprint, a facial scan, or a retinal scan (Federal Trade Commission, 2022). Not every account will have access to these additional security measures, but when they are supported, it is a good practice to enable multi-factor authentications.

Outside of account safety, there are good practices that users can develop to be prepared for social engineering and other digital attacks. For businesses and organizations it is important to conduct training for employees that helps them prepare for potential encounters with social engineering schemes. Most businesses have policies and protocols in place that direct employees in their technology use to ensure that sensitive information is more secure. In an infographic by Deepak Gupta with statistics on the intensity of social engineering attacks from 2019, eighty-six percent of attacks involved business email compromise attempts and sixty-six percent of malware was installed via malicious email attachments (Gupta). Knowing this should instill a recognition of the importance in maintain strong security over private email accounts. While there are no signs of these attacks stopping soon, businesses and corporations can prepare for them and mitigate damage done through training employees in safety practices.

Gupta also shares signs one can look for in order to better recognize phishing attacks. Whether talking to someone physically present or through a digital manner, look out for both overly friendly and unusual behavior. Similarly, be wary of those who ask for immediate help and emphasize specific details, as they can be attempting to obtain information as quickly as possible in order to avoid confrontation. Any requests for information from individuals that are not willing to provide their own information first may also be phishers (Gupta). In all circumstances, it can be beneficial to trust any instincts or gut feelings one may have in any situation. If someone or something seems suspicious, trust the feeling, and go through proper procedures to ensure the users and their requests are legitimate.

In your personal life, there are also many good habits one can develop to remain safe online. When using social media avoid sharing any confidential information in your profile such as your birthday, family members, or past places lived. This information is often used in order to validate someone attempting to access an account, such as a bank account, and having it socially viewable online can give attackers access to confidential personal information. Similarly, do not share any confidential information with anyone you know across social media. In the case that an account has been hacked, the phisher may be using the account acting as someone you know to obtain information. To know whether the person requesting information is a legitimate request, reach out to the person through another method, such as a phone call, to ask if the person you know really did ask for the information.

In conclusion, we can see that phishing attacks and social engineering schemes are prevalent in today’s digital society. With thousands of victims each year, it is no surprise that there are many who continue to employ and enact these schemes in order to achieve their personal goals. While we cannot expect these attacks to end, we can enable ourselves to be prepared for any encounters we may have with these schemes. Preparing beforehand and knowing how to identify and react to any attacks will better keep our personal information, and in turn the information of others, secure and safe from potential phishers.

References Cited

Federal Trade Commission. (2022, September). *How To Recognize and Avoid Phishing Scams*. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Grimmick, R. (2020, December 23). Phishing Attacks: Types, Prevention, and Examples. *Varonis*. <https://www.varonis.com/blog/phishing-attacks>

Gupta. D. (n.d.). Social Engineering Attacks: Prevention and Best Practices. *Loginradius*. https://www.loginradius.com/blog/identity/social-engineering-attacks/

SecurityScorecard. (2021, May 5). *12 Types of Phishing Attacks and How to Identify Them*. <https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them>