CYSE – 494 ENTREPRENEURSHIP in CYBERSECURITY

PROPOSAL

The innovation of modern technology has brought many threats within the cyber world, many of which are still ongoing. The implementation of different cybersecurity strategies within different corporations – big or small - for different levels of threats can be tedious, but it is necessary to minimize risk and to avoid any leaks of sensitive and valuable data. These strategies can be done and followed through by a team of specialists and cybersecurity professionals. Private citizens, however, do not have the same luxury as big corporations do when it comes to implementing such strategies. Many have fallen victim to cyber incidents such as phishing, due to the lack of knowledge and awareness of different cyberattacks.

So, what is phishing? Phishing is a form of social engineering attack. It is a scam impersonating legitimate organizations which cyber criminals use to con people into giving up personal information. There are different types of phishing attack - email phishing, spear phishing, whaling, smishing and vishing, and Angler Phishing, etc. Email phishing is the most common type of phishing attack which is done through emails. By registering fake domains and impersonating legitimate organizations, cyber criminals can send malicious emails designed to trick people into giving up sensitive information. For example, an email sent out with a sense of urgency informing the user that his/her account has been restricted and would require specific information to regain access to the said account. Included in the email is an attachment requiring you to input necessary information to regain access to the account. The user, fearing of being locked out of their account, clicks on the attachment, and responds to the email. What they failed to realize is that this email was fake and now their information is in the hands of the attacker. Attackers use a similar approach when initiating a spear-phishing attack. However, the difference is how the malicious activity is being carried out. Spear-phishing mainly targets specific individuals, groups, or organizations.

There are many problems associated with a phishing attack. For individuals and businesses, the most severe effect is data loss. By clicking on a malicious link in an email, data and system of the organization is handed over to the attackers. The attackers will then have the freedom to do as they please with the information obtained for criminal purposes such as theft, corruption, and deletion of certain data. Following a data breach, companies suffer reputation loss as well as loss of trust from the public. Other damages include monetary loss, loss of productivity, loss of customers, financial penalties, intellectual property theft, and loss of company value. Statistics show that within the United States alone, over 100,000 people have fallen victims to this type of attack each year. In 2020, the FBI's Internet Crime Complaint Center (IC3) reported phishing, among other cyberattacks, as the most prevalent threat with as many as 241,342 victims. An analysis of over fifty million emails shows that one in every ninety-nine emails is a phishing attack and twenty five percent of these emails' sneaks into one of the most widely used office app in the world – Office 365 – with an estimate of over 60 million users. Because there are so many users for platforms such as Office 365, phishing attacks have a greater chance of being successful.

Phishing attacks have been around for many years; however, it was not commonly known to everyday people. The first mention of the term "phishing" was recorded in the mid 90's and it was not until

almost ten years later when common folks started learning and hearing about it. Phishing attacks have been increasing throughout the years, especially with many organizations being digitalized and common folks turning to technology to safeguard their information. Because of this very reason, it is crucial that everyone be educated and knowledgeable about the types of online attacks that occurs daily. Modern day attackers have been impersonating government agencies with the attempt to trick online users. But with the right education and knowledge on how to spot these types of attacks, and having the appropriate tools to mitigate such attacks, users will be able to protect their data as well as save money in the long run. Because emails are not the only way attackers can retrieve information, it is also crucial to also be informed about SMShing and vishing. These types of phishing attacks are done through calls or text messages. Since the same caution and approach is different than that of an email phishing, users must be aware of the kind of threats that lingers within the digital realm. IT admins for businesses and organizations are constantly updating and implementing new tools for better security. However, this should be done for common folks as well. The issue is that common folks may not be able to afford tools necessary to manage the security on their devices. So, with technology on the rise and attacks increasing daily, all tools required to safeguard data should be made available to everyone including the common folks. Proper education should also be made available and affordable. There should be an online tool readily available on all devices that automatically deletes a spoof email or scam text message before it even gets delivered. Implementing a phishing prevention software like Clearedin could help protect yourself and your organization from being victims of a phishing attack.

Rather than having to pay a fee to have a phishing prevention software on your device, it should be made readily available on all devices whether it be personal or for business. Big corporations have the means to protect themselves, common folks do not. There are also many apps that require a small fee to download to have better protection, or a platform made specifically to inform organizations on how to mitigate certain online attacks, however these are things those common folks do not always have access to. The crossroad of having the right tools available at an affordable price is that anyone would have access to it, including the attackers. With tools available and easily accessible to just about anyone, hackers could use these to their advantage. This could be very much a problem rather than a solution. However, if the right tools are implemented and a two-factor authentication is automatically set up for every device, it could improve the security.

People who use two-factor authentication on their devices know that this is a measure of security that works. However, the user must download the app to use it. If every device sold, whether it be a PC or a cell phone, already has the two-factor authentication set up without having to download it and phishing protection software in place, phishing attacks could slowly decrease. It may not be over night, but the numbers will go down. The only way to know if it works is to implement it on newer products. It may be a long shot, but it is better than having to pay extra for software and protection that should have been included in the device from the beginning.