Jacob Edelin

Professor Campbell

INST 364-0102

May 12, 2023

Write Up

"Gone Phishing" is a simple web-based simulation of a phishing scheme. Users are presented with an email supposedly from their bank telling them that suspicious activity was detected on their account, and that they should sign into their account to remedy it. They can then either click the link or delete the email, and it is up to them to gauge the legitimacy of this email. They will be redirected to a page that gives information on why people fall for these attacks or how to avoid them using the NIST Cybersecurity framework depending on their choice. For those who know how to identify phishing attacks, it raises awareness of why they are still successful, and for those who do click the link, it provides information that should be helpful for avoiding real schemes.

In this digital age, most people are aware of phishing schemes and the signs that give them away (poor grammar, weird formatting, etc.), yet even highly educated people continue to fall for them, and there are several reasons for this. Many organizations collect highly personal information from people nowadays, but there are laws put in place that protect it from being sold or accessed by third-parties, making it difficult for hackers to steal it. However, phishers will gather data from publicly available sources, such as social media, marriage licenses, and census data, as a gateway to accessing more sensitive information. These scams prey on our emotions and instincts by using this personal data to craft believable messages from services we use and trust. We tend to view things more casually when we deem it as trustworthy, which can cause us

to lower our guard and overlook some of the obvious signs of it being a scam, leading to a successful phishing attack.

There are, of course, also people who simply do not know better when it comes to phishing schemes, and sometimes that is because some groups cannot protect themselves. As explained by power structures, much of the current security measures in the U.S. exist to keep its white male founders at the top of the power hierarchy, with marginalized groups being put at a disadvantage. Immigrants in particular have been a popular target for hackers because they are often excluded from receiving information security. Law enforcement and the federal government often do things like target undocumented immigrants and restrict the type of research they can do. Phishers use this to their advantage by sending fake messages that promise the recipient will receive a favorable legal status or Green Card if they send money. Both of these things are highly sought after by many immigrants, and hackers are preying on their desires.

For those who need help understanding how to protect themselves from a phishing attack, they could follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework is made up of five core functions, being Identify, Protect, Detect, Respond, and Recover, and although it is primarily meant for organizations, I believe it also has the potential to help at an individual level. The first function, identify, is where you take inventory of all your hardware and software, then develop an understanding of the potential threats and vulnerabilities they could face and establish cybersecurity policies and procedures that will protect your information. For phishing, this could mean taking into consideration that some emails may be sent to steal your information or infect your device with a virus, and installing a phishing detection browser extension for protection. The next stage, protect, is about developing and maintaining safeguards, which can include data encryption, regular security

software updates, and training for cybersecurity risks. Detect involves the monitoring of your devices and investigation of unusual behavior. You should always check the legitimacy of any messages that seem unusual, especially when they are asking for high personal information or monetary compensation. Respond is about the actions that will be taken in the event of a security breach. In this case of a successful phishing attack, there are many things you could do depending on the type of attack. If it involved money, you should lock your bank account and report the event to your bank's official support team, and you may also want to use the experience to develop a better strategy for the future. Finally, there is Recover, where you restore any devices or software that may have been affected. All of these steps could work with each other as a guide for people to follow to protect their data.