Sera Hill
CIDM 6341-70

Wireless Survey/Phishing

What Did I Do?

For the first part of this assignment, I scanned my area for visible network connections on my computer. The computer sends out signals to request Wi-Fi networks within range, detecting visible networks by scanning signals that are being sent from wireless routers. Routers broadcast its SSID and other information at regular intervals which allows computers scanning for available networks to pick up the response. In addition to checking which local routers were broadcasting Wi-Fi information, I walked outside of my home to see how far I could go while my phone was still able to detect my Wi-Fi network, allowing me to gauge the distance at which my network was still visible.

For the second part of the assignment, I participated in a quiz that had examples of fraudulent email messages mixed in with legitimate examples. These emails were simulations of actual messages that allowed you to hover over and inspect links, company logos, and spelling. For each example, I used my knowledge of common phishing red flags to determine whether the email example was legitimate or a phishing attempt. I went through the same process for a quiz about phishing attempts regarding websites. The quiz provided screenshots of websites that had some sort of input form on the page to collect information from the user. The screenshot of the website also included the Internet browser bar that allowed me to view what URL was being used, whether the site was secure, etc. With this quiz, I used my website knowledge to determine whether the site screenshot was legitimate or not, paying special attention to what domain the URL was using, and whether the site collecting sensitive information had an SSL certificate applied to the domain or not.

What Were the Results?

For the first part, my computer was able to detect 33 other visible Wi-Fi networks from my house. All of these were password protected, but I did notice quite a few that were using the default network name which opens the possibility that they are using the default router and login settings. This could make it easy for unintended users of that network gain

access if they have knowledge of what those default settings are. My own Wi-Fi network is detectable but is not using the default router settings and is also password protected with a unique password.

I also discovered that my wireless network is visible from about 215 feet away from my home. While it does not seem very far, it is still outside of my property. I realized that somebody from at least two or three houses away from mine are able to see and possibly attempt to access my network. I wouldn't be aware of this kind of activity until it was too late, and they were already trying to connect.

Regarding the phishing email quiz, I scored a 10 out of 10. Phishing attempt emails can be obvious, with signs like misspelled words, poor grammar, low image quality, or mismatched email addresses. However, there can also be more sophisticated attempts that exhibit more subtle signs of a scam. The less obvious phishing emails had links that did not go to where they said they would go, but you could only know that if you hovered over the link (safe way to find out), or if you actually clicked the link (unsafe way, as this opens up the possibility of downloading a virus to your computer). For example, a button should have gone to a Microsoft domain showed a completely different URL when I hovered over it. It is important to consider all pieces of an email from an unknown sender to not fall victim to scams.

For the website phishing quiz, I scored 14 out of 14. In my current role, I work with websites every day and know what to check for to make sure a site is legitimate. As with emails, there can be obvious signs that a website is a scam such as having misspelled words, incorrect logos, poor image resolution, etc. However, there are also less obvious signs. For the less obvious scams, the domain was not correct, or it didn't have an SSL certificate. Before typing in sensitive information into a website, the user must be aware of what kind of information the site is requesting, and if it is secure.

What Did I Learn?

Firstly, I learned that SSID means "Service Set Identifier" which is basically just the Wi-Fi network name. Also, I learned more about how routers work in that they are

constantly broadcasting a signal with the SSID saying that the network exists in the first place (Stegner, 2022). It helps to understand what routers are actually doing when you can search for visible networks on your computer because it makes you think more about ways you can be vulnerable to attacks.

It's easy to forget or ignore just how big one's personal attack surface is. I realized my own attack surface is quite large, especially with the fact that my own Wi-Fi network is visible to others that don't even have to physically be on my property. A visible network can invite hackers to attempt access. With that said, there are ways to lessen attack surfaces and make it harder for hackers to gain access into private networks. For the wireless connection, the SSID could be adjusted to not broadcast to casual scanners. Unless someone is determined to find the network, this decreases the chance of it being accessed by others. I also learned that it is better to not use the default router settings for the SSID or password as that makes it easier for hackers to determine how to gain access. It was interesting to learn that my network was visible even outside of my home. It seems obvious now, but I didn't think about the potential of being hacked from somebody a couple of doors down. I would not suspect anything was amiss until it was probably too late to prevent their access.

I also learned that the repetitive training at work is very useful and helps me stay wary of emails from unknown senders. This is not only beneficial for my company, but also myself personally as I am less likely to fall victim of email scams. My wariness of emails from unknown senders is already quite high as my company regularly sends out phishing email simulations to see whether the employees can detect a phishing attempt. If you fail to catch this, you are required to go through additional training to prevent an event like that happening again.

While we do not go through the same type of tests regarding websites, my professional experience working with financial institutions has brought my awareness to domain names and SSL certificates as well as paying attention to what type of information you are being asked to submit in an online form. We offer a service that allows for encrypted forms to be used on our clients' websites to collect loan applications, job

applications, etc. It's very important the form fields are encrypted as you don't want things like social security numbers floating around the internet. This has made me pay close attention to what I'm typing into form fields and to question whether it makes sense for me to even put that information in there.

As tedious as it can be sometimes, proper training on how to spot phishing attempts on the web or via email is crucial in maintaining a secure online presence. This is especially important as the vast majority of organizations are online in some way whether that be a forward-facing website or storing sensitive information in datacenters or on the cloud. Companies should routinely monitor their network security to ensure their current security methods are still working or if they need to make any changes. Organizations should also provide ongoing training and resources for its employees so everybody stays aware of the importance of cybersecurity and potential ways hackers follow to gain access to and steal information. Also, while it does not make somebody completely safe from an attack, hiding your network SSID can help reduce their personal attack surface.

Sera Hill
CIDM 6341-70

References

Sonicwall.com, 2024, www.sonicwall.com/phishing-iq-test#. Accessed 14 Sept. 2024.

Stegner, Ben. "How to Hide Your Wi-Fi Network: Everything You Need to Know." *MUO*, MakeUseOf, 15 Dec. 2019, www.makeuseof.com/tag/hide-wifi-network-prevent-detected/. Accessed 14 Sept. 2024.

"What Is Phishing? Take the OpenDNS Phishing Quiz." *OpenDNS*, www.opendns.com/phishing-quiz/.