Phishing for gold. DART449 | Anthony Lum | 40098555

DART449 | Anthony Lum | 40098555

We do a lot to protect ourselves, whether it is in the physical world or the online realm using various layers of security. We rely on passwords, security systems, biometrics, and all sorts of technology to protect us from digital attacks. But there is one factor we all seem to overlook, and it will always be our biggest downfall when it comes to our digital security.

To manipulate interactions with other people to create a favorable outcome for yourself is called “Social Engineering”. Through manipulation, we can try to trick someone into making mistakes and with human error, it is the key that makes social engineering work (Phishing.org). Rather than trying to outsmart well-built and thought out layers of security, one only need to trick one layer that could make a mistake, to get access to everything (“Social Engineering”). There are various “attacks” involved with social engineering where the goal is to trick the target through manipulation into revealing information without them knowing that they are handing it out voluntarily.

The steps involved in social engineering involve four stages: investigation, hook, play, and exit. They set up the victim, followed by manipulation and luring them into their comfort zone, the victim then reveals the targeted information, lastly leaving without a trace.

Phishing has been a term used as a type of social engineering where it was based off the nickname hackers had as “phreaks” (“Phishing Techniques”), where they are “fishing” for information. “An alarming 90% of all successful attacks to gain information have been through some form of phishing (“Phishing”)”. There are many types of phishing techniques, all with varying levels of complexity and depth. All of them require the victim to interact with the phish, while the more complex the attack, the more the victim must have provided for the phish to work.

There are two-base group of attacks with phishing. The surface level phishing is simple attacks that require the victim to have fallen into the trap because of human error and giving the information. Examples of this include “Spear Phishing”, “Vishing”, “Smishing”, and “Link Manipulation” (“Phishing Techniques”). These are surface attacks level because you can see carefully that it is a scam if you look close enough for hyperlinks that the hacker wants you to click but will redirect you to their trap hidden under the veil of a legitimate organization or flashy animation.

The fishing terminology continues into the most basic attack called “Spear Phishing”, which requires a bit of luck where the attack is randomly sent out in mass hoping that it will catch somebody through email spam. Similarly, “Vishing”, “Smishing”, and “Link Manipulation”, are voice, sms, and hyperlink based attacks which the hacker is suggesting that you interact with a link disguised to look real to have you fall into a trap to give information.

The underground level phishing attacks require more complexity like “Session Hijacking”, “Keyloggers”, “Trojans” and malware. All of these are very sophisticated that you would not be able to see it from simply looking at it. They are usually programs that the victim has downloaded thinking it was something else (“Phishing Techniques”). The hacker is then embedded deeper into your network being able to download additional software to see and record everything you do on your device. They can manage all your files, see what you type, and have full control to navigate around your computer and potentially more.

Once hackers have even the slightest amount of information or access, they can use that small piece to further advance into your network. If the hacker can phish out personal information from you, they could be able to impersonate you to get more information. One could know your name and address, and if they knew what internet provider you were with, could always call the provider pretending to be you, to then ask to reset your password to then gain further access to your network. All they would have to

do is provide some personal information to prove that they are you, and if they've phished enough information from you, your network would be compromised and the hacker could get access to your internet router, which can then be connected to your computer devices, which can lead to bank accounts and other sensitive information (Garfinkel).

Recently I personally had fallen for one of these attacks and everyone no matter how "tech-savvy" you may be, can fall victim to these traps if you are not careful enough. My interaction involved a couple of steps that made it believable by chance and good timing on the attack's part. I had injured myself and need an ambulance. Following that, they requested payment through "PayPal" and I successfully completed this transaction and did not think much more of it. Surprisingly, this portion was the legitimate. I later received an email saying there was a problem with my "PayPal" account, and I needed to reset my password. I normally ignore these emails because I never login to that account, but I believed the email because of the timing and ended up clicking the "reset password" button on the email and going through the steps to recover my account. Before completing the process, something felt wrong and I was able to spot out the signs of a phishing scheme and aborted before I had given my information. If I had followed through, my "PayPal" account would have been compromised and I wouldn't have even noticed thinking I had just "fixed" it. These types of attacks are common and can come in various forms and some are better made than others to spot and the best ways to defend against these attacks are to adopt procedures and strong technological security to minimize the impact it could cause (Garfinkel).

My goal with this website is to show how easy it is to fall for these phishing tactics, and showing you what to look out for and explaining why certain information you should be careful to protect and how. I'll be creating a website that will look and feel like a regular website and have interactive components similar to other websites, but almost everything that you can click will have a purpose to trick you into putting in your information to use later.

Works Cited

Garfinkel, Simson. “Kevin Mitnick and Anti-Social Engineering.” *CSO Online*, CSO, 7 Oct. 2002, www.csoonline.com/article/2113271/kevin-mitnick-and-anti-social-engineering.html.

Imperva. “What Is Social Engineering: Attack Techniques & Prevention Methods: Imperva.” *Learning Center*, Imperva, 29 Dec. 2019, www.imperva.com/learn/application-security/social-engineering-attack/.

KnowBe4. “Phishing.” *KnowBe4*, www.knowbe4.com/phishing.

Phishing.Org. “Phishing Techniques.” *Phishing*, www.phishing.org/phishing-techniques.