Nathaly Flores

CYSE 600

Short Analytical Paper 3

Old Dominion University

Phishing

Abstract

The importance of phishing because it can prevent us from falling into emails or phone calls that trick us into giving away our essential information. There are various parts of phishing attacks and some possible safeguards as countermeasures that every organization or person should know. Educating ourselves to prevent any future attacks is very important to know. This essay will show how social engineering has increased over the past decade, how companies should learn how to prevent these kinds of things, and the different types of phishing that exist these days.

Phishing

Phishing has become very dangerous in the internet world and is an increasing threat to technology (Aleroud, 2017). Ever since covid-19 started in 2019, cyber-attacks seem to increase over these past years; attackers are phishing to steal information from the vulnerable and victimize them until they get what they want. Attackers will not regret taking advantage of people at any given time, especially in the world of cyber-attacks, where it happens more than once. Spam is the most unwanted famous email that comes daily into our inbox. Therefore, there is a need to restrict these phishing activities to defend unsuspecting technology users from falling prey to phishers' traps such as spam. Attackers have figured out a way to offer services to phishing victims to get people to fall for its undisguised websites.

Phishing is a real risk to all Internet consumers, and it is challenging to follow or not be a victim of phishing since most emails do not seem dangerous. While phishing is typically seen in the business world as a client issue, the phishers' fake approaches are frightening in the corporate area. The different parts of phishing attacks bring on potential safeguards as countermeasures. Nowadays, everything is put on social media or any search engine like google or Firefox, and the credentials of the private client are now in danger. Phishing can be seen as the simplest and easiest method of stealing information from people. It has the go-to method of an attacker, such as tricking the individual by sending an email within the email. It leads you to a phishing site, and all your information is taken while on that site.

First attacks

Hackers use the pandemic to deceive people that they had a cure for the virus or were wrongly notifying them of their covid test results by luring them to verify the information. Another thing hackers did was say that they had the cure or the supply to sell and stop this virus, offering medications and then luring them to buy this medication by stealing their information and never giving them what they paid. One of the earliest first phishers made was the group Warez community. This group can be followed back to the 1990s through American online. A few decades ago, the early scam was made; this group developed an algorithm that generated random credit card numbers and then used them to make phony accounts. Their potential goal was to aim at a few people at a time, and then from there, they started messaging people via AOL.

As time passed, people became tech-savvy and started using messengers to phish users through their email messages. Phishers started creating similar domains from well-known firms like eBay to deceive people into believing they were on a legit site. Another well-known site, PayPal, suffered a virus by clicking a phishing email that redirected them to a phishing site and instructed them to input their PayPal login details (Hinde, 2004). Nowadays, phishers have enormously increased their form of methods with the sophistication of technology. With the increase of technology and people staying at home or working, phishers are more active than ever in stealing your information.

Cyber Attacks

Phishing was the most effective cyberattack during covid-19 when most people were at work or home. Around the world, new phishing attacks have increased more than ever; this means people have become more vulnerable and tricked, and their devices have easily been compromised through phishing. Text messages have been used to fool victims, convincing them that the text message is authentic and catchy. If your account has been compromised, you need to change your password as soon as possible, and attackers have been highly strategic and specific in the questions they use on the individual. For firms, the quality of the questions used is more accurate.

However, people now have a way to protect themselves from cyberattack victims. Since phishing is mainly sent out through emails, people need to be cautious in receiving phishing emails and the different forms of phishing attacks. Some of the attacks used today are CDC alerts and advice health issues, extortion emails, charity emails, etc. we should be cautious and look for very deceptive or abnormal emails. It can be a possible attack if open. Besides phishing emails, we should be careful when receiving suspicious calls and texts that offer gifts or bizarre email links. Phishing is now done in different ways, such as text messaging, calling, or ads. People should seek to learn more ways to protect themselves from phishing attacks. Phishing is unexpectedly growing to be more persuasive, and the reason why this is occurring is due to the high activities of technology use affected by recent causes happening, for instance, covid-19 or the war between Russia and Ukraine and the death of the Queen of England. All these events have caused technology to soar.

Different types of Exploits

The following are the types of phishing that exist today, phishing emails like spearing, whaling, vishing, and emails. Spearing Phishing is an email message scam that chooses a specific individual, company, or business. However, cybercriminals may install exploits on a targeted person's computer, often planning to steal information with malicious intentions. For example, USAID was the target of spear-phishing campaigns that sent trademarks of funded attacks. This attack was carried out by sending a massive email to contacts using the same original as USAID. The cyberattacks target over three thousand users in one hundred and fifty corporations and twenty-four countries.

A whaling attack is an approach utilized by cybercriminals to conceal themselves as executive members of an organization and instantly influential individuals to steal funds or sensitive information or acquire entrance to their computer system for criminal intentions. Executive Impersonations have skyrocketed over the past year. It has seen spoofing rages of fifty-five percent of cybersecurity experts that said companies had been spoofed or impersonated recently by sending malicious links to their sites sending gift card requests. Half of these corporations' victims have fallen victim to this.

CISA is warning the public about an ongoing voice phishing campaign targeting remote workers. The campaign stated that criminals created fake websites that created virtual private network login pages for target organizations. Vishing is social engineering by calling victims and tricking them into giving out their credentials to access private information. Vishing scammers use over-the-phone, where scammers will try to sway people to convey personal information by impersonating bank staff or other financial employees (Grobler, 2010). They also pretended to be information technology representatives in the help desk department, helping employees gain their trust and login information to their VPN. Many calls were made using voice-over-internet protocol numbers to call victims on their cell phones. Companies were counseled to restrict and strengthen their VPN connections to supervised devices, restrict VPN access times, and monitor domain modifications to the organization.

Email phishing is the most known form of phishing; this attack tries to steal sensible information via an email that seems to be from a legitimate organization (Grobler, 2010). This attack is not a pick-out attack and can be carried out by a group of hackers. One of the most recognized fast-food chains was a target of email phishing. Hackers stole information from this corporation, including from other countries as well. The breach revealed that the information was coming from an employee's email. By accidentally accepting a phishing email, hackers made their way into the system. This company was lucky enough that none of its customer's data was ever stolen. This company invested in tighter, more robust security measures to avoid further hacking.

Conclusion

Everyone should be prudent when opening phishing emails, DO NOT add your information from any of the phishing techniques mentioned. For instance, if you received a look-alike phishing email from PayPal, Facebook, or any other platform used, delete the email and do not open it. If you are in an organization, be careful about what you receive, including bribes, gift cards, or emails that pretend to look like the cooperate website. Especially if you have a social media account, be careful what job you post. That can quickly motivate hackers to attack your organization by using the information in your account and sending DDoS attacks or phishing attacks through email or personating someone with the information you gave out. The best advice for these situations is to train your employee and NOT open any email, click on any links, or download/open any attachments. Be cautious about what you open, whether personal or not.

References

Aleroud, Ahmed., & Zhou, Lina. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160-196.

Grobler, M. M. (2010). Phishing for fortune. Page: (7) 1-2.

Hinde, Stephen (2004). All you need to be a phisherman is patience and a worm. Computer Fraud & Security, (2004). (3), 4-6