Spring 5-12-2023

Phishing

Irda Voli
La Salle University, volii1@lasalle.edu

Irda Voli

4/20/2023

Capstone

Learning About Phishing.

Phishing is a cybercrime that involves a hacker identifying as a real person or institution that targets people over text message, phone calls, and emails. The hacker tries to scam the target into giving up personal information. People are targeted through text messages, phone calls, and emails. More recently in 2020 when covid became a major issue, phishing started becoming more and more popular for ways to scam. The messages became more specific, and job sites became more believable. According to article "Phishing Attacks Soar 220% During COVID-19 Peak as Cybercriminal Opportunism Intensifies", David Warburton says:

> COVID-19 continues to significantly embolden cybercriminals' phishing and fraud efforts, according to new research from F5 Labs. The fourth edition of the Phishing and Fraud Report stated that phishing incidents rose 220% during the height of the global pandemic compared to the yearly average. Based on data from F5's Security Operations Center (SOC), the number of phishing incidents in 2020 is now set to increase 15% year-on-year, though this could soon change as additional waves of the pandemic spread. The three primary objectives for COVID-related phishing emails were identified as fraudulent donations to fake charities, credential harvesting, and malware delivery. (Para. 1).

During Covid, pretty much everyone worked from home or spent a lot of time online. Hackers understood that they could use covid to their advantage when making up lies on how to convince people to hand over personal information, and how to get the user to send money without knowing it is a scam until after the damage happened. Due to people working from home, there

was no real monitoring of employees to make sure nothing was done to put the security of the company in danger, especially when it was also connected to personal Wi-Fi.

Types of Phishing.

There are different types of phishing. The five common phishing scams are email, spear, whaling, smishing and vishing, and angler. The first one which is very common is email phishing. It is just the basic email that tries to trick the user into thinking it is real and to click on something in the message that was sent. One example includes the email mimicking a domain. For example, in the sent email, there might be something misspelled. The name may be spelled wrong by one letter or an email address that is not at all real but just looks real may be used. The main key is who is sending the email out. The second sort of phishing is spearing phishing. This occurs when the hacker already has the common information about the user, such as job title, name, or an email address. They use this information when they email the person and act like someone else the user might know and try to get the user to give personal information, or possibly send money. The third type of phishing is whaling. Whaling is a more target based. The hacker imitates someone higher in power at the victim's job and tries to get them to give out information by acting like it is the boss that needs the help from the employee. The fourth common phishing is smishing and vishing. This type uses phone calls and text messages instead of email. Smishing occurs when a hacker uses text messages to send fake texts like saying "we noticed suspicious activity on your bank account", while vishing uses phone calls like in the "IRS scam". This scam has the hacker pretending to be the IRS. The caller knows the victim's name and uses it to threaten them. The victim is told that they would be in trouble with the authorities if they did not pay a certain amount of money. The fifth most common phishing is

angular phishing, this involves social media posts, instant messages, posts, and fake URLs. These types of messages are used to get information from people who are willingly providing it on social media. This type of phishing occurs when a lot of people complain against an organization that is well known. The hacker finds this information and pretends to be the organization and responds back to the user with a way to fix the complaint. In many cases, phishing has started from one step and then branched off in different ways that allows hackers steal users' information.

Cases.

Email phishing is one of the most common ways of to try and get personal information. One of the most recent cases of email phishing is when covid first hit and emails were going around about constant information supposedly from CDC. According to the FBI, they noticed a rise in fraud schemes related to the pandemic. The FBI stated:

> Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received. (Para. 2).

This was because people were verifying information from fake emails and leaving themselves open as victims. In 2016, spear phishing attacks exposed community college employees' tax information. It turns out that the employees had received an email that looked like an official

form of the IRS, that said that they already had filed a tax return with this social security number. They later discovered that all this information was sent to a cybercriminal account. According to article “Spear Phishing Attack Exposes Tax Information of 3,000 Community College Employees” company Trend said:

> In a consumer alert posted earlier this year, the IRS has warned the public of a 400% uptick of IRS scam cases reported this year—a significant growth from last year. In fact, from January to February alone, 1,389 incidents have already been reported, more than of the 2,748 total incidents reported throughout 2015. Apart from users and organizations, tax professionals were also targeted by the same techniques to steal IRS service credentials. IRS Commissioner John Koskinen said, “Watch out for fraudsters slipping these official-looking emails into inboxes, trying to confuse people at the very time they work on their taxes. We urge people not to click on these emails. (Para. 10).

These documents being sent out look official, and this is the exact reason people get tricked into giving out information. Whaling is another sort of phishing that is on the rise. One of the recent cases of whaling from 2016 racked up five billion dollars. The group hacked into many accounts executives’ accounts and would send emails saying they needed to send money to others for any reason they made up. According to the Infosecurity,

> A request for a wire transfer from the compromised account is made to a second employee within the company who is typically responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank ‘X’ for reason ‘Y’. Other versions involve W2 or personally identifiable information (PII) exfiltration from HR, attorney impersonation, or bogus ‘foreign supplier’ invoices,

> among other scenarios. In all these cases, victims receive seemingly legitimate emails from known sources, and the crooks have accurately identified the individuals and protocols necessary to perform wire or information transfers within a specific business environment. (Para. 2).

The hackers made the emails seem to come from an actual source of payment and that is how they got the executives of the company to comply. According to Infosecurity "The FBI has issued an alert warning about a dramatic increase in business email compromise (BEC) and email account compromise (EAC) scams, with a whopping 2,370% increase in identified losses from January 2015 to December 2016.". (Para. 1). Another phishing on the rise is smishing and vishing. These are two different types of phishing but trying to accomplish the same thing. One wants to get control of information with fake texts, and the other uses fake phone calls. A company called Twilio was attacked twice, once with smishing and once with vishing. Back in June the employees got calls from scammers and got tricked into giving their personal information to the hacker, this was a vishing attack. According to Security Week:

> Twilio's final report reveals that the same threat actor was likely also responsible for an attack that targeted the company in late June. The firm described it as a 'brief security incident' that involved voice phishing (vishing). The attackers used social engineering to trick an employee into handing over their credentials, which they used to access the contact information of a limited number of customers. (Para. 5).

The company claims that the hacker was identified and stopped within 12 hours. In August 2022 the hacker tried again but this time used a smishing attack that sent out hundreds of messages to current and former employees pretending to be the IT company and to urgently click the link that would send them to a fake page. According to Security Week

> The breach discovered in August was a result of a smishing attack launched in mid-July, which involved hundreds of text messages being sent to the phones of current and former Twilio employees. The messages appeared to come from IT administrators and urged recipients to click on a link that took them to a fake Okta login page. (Para. 7).

Some of the employees took the bait and entered their personal information. Finally, the most recent phishing is angular. This sort of phishing sends out links of pages that are fake but look identical to the actual organization. In the last case, Twilio company had this in the attack. The attack sent out messages to employees to a fake page to input their information, they were doing a smishing and angular phishing combined attack.

Spotting Phishing.

Some of the most common ways to spot phishing through emails is to look at the requested urgency. When the message requires urgent action, has mistaken and incorrect grammar, includes suspicious attachments, or requires login credentials, it is probably a phishing message. The article How to Spot Phishing Emails written by Cofense says:

> The first step in spotting a phishing email comes with understanding what a phishing email is. The most accurate definition of a phishing email is an email sent to a recipient with the objective of making the recipient perform a specific task. The attacker may use social engineering techniques to make their email look genuine and include a request to click on a link, open an attachment, or provide other sensitive information, such as login credentials. (Para. 3).

Spotting phishing is not as easy as people may want you to believe, the more time goes on the more advanced the hacker gets with making phishing emails look more legitimate.

Another form of phishing includes texts and phone calls. Examples include when a user gets a text message saying that their package cannot be delivered and then asking the user to click on the link to confirm the "correct" address. Some of the ways to combat this phishing is to look for errors in the message, or simply double check on the package delivered on the website where it was ordered. Another way is to double check the phone number that sent the message and check the history of any past messages with this group. Did UPS/FEDEX ever use this number in the past when it comes to contacting for a delivery?

Another way to spot phishing is seeing an offer and knowing it is too good to be true. Sometimes hackers find information on the victim they are targeting and use something to lure in the user. In 2019 a new phishing campaign was founded, which was aimed at Office365. The Cofense Phishing Defense Center discovered a new phishing which was aimed at Office365 credentials by prying on employees who are waiting for promotions or raises. According to Milo Salvia in article *New Credential Phish Targets Employees with Salary Increase Scam* says, "The threat actors use a basic spoofing technique to trick employees into thinking that their company's HR department has shared a salary increase spread sheet." (Para. 4–5). The hackers manipulated the form in the email address to make it seem like it comes from a legitimate boss. They made the information in the message body as legitimate as they could and told the victim to click on a link that discusses the yearly salary raise, the link is made to look like an excel document. In this case, the hacker takes the next step so that the document looks exactly like the Microsoft login. They already have the email address already filled in and they are just waiting for a password, this makes the scam and phishing look more legitimate and believable, so more people fall for it.

A lot of phishing scams use zoom and google calendar. Zoom, and google calendar were easy access for the hackers to send out fake invites to trick the victims. Going with zoom and

google calendar, another main thing that was affected by phishing was chatbot. Hackers are implementing their own chatbot to talk with users and try to get sensitive information from the user. According to article "The Surge in Phishing Attacks and Changing Threats in 2021" Elliot Bolland says:

> Scammers will usually start this technique through the usual methods, SMS or email phishing scams directing to a website. This website is likely a fraudulent version of a legitimate site they are claiming to be. This is when the scammer will utilize the chatbot guiding you into a conversation to extract sensitive details. Beware of offers of large prizes on chatbots, and always make sure that you access the site you intend to through a search engine, not via. an email/SMS link. (Para. 9).

This new era of phishing is making use of the new technological advancements. The hackers use the text message to send the link out and once the link is pressed, they use the chatbot to talk with the user pretending to be legitimate to retrieve sensitive information from the user. Some options for advance technology are created to make people's life easier, however something that can be used for good can always be used for bad as well. It all depends on whose hands the new advanced technology falls on.

Ways to stay protected.

Some ways to stop phishing are simply stated: do not click on unknown links, do not give out information for anything, and always double check everything that was sent. These are a few things that if checked, could slow down phishing and help it be avoided. There are some other ways to avoid phishing that employers and bosses can do. This includes conducting regular employee training on phishing, recognizing, and avoiding phishing attacks, avoiding clicking on

malicious links, deploying a spam filter which checks inbound messages and trying to recognize and prevent emails from suspicious sources from reaching employees' inbox. Another way to try and avoid/stop phishing from a company's perspective is to keep passwords secure, in this case using longer and hard to guess passwords is better, along with requiring changing the password and deploying two-step authentication. Finally, staying up to date with security patches.

Some ways that experts believe companies fall prey to phishing attacks are based on employees browsing the web freely. In article "4 Steps to Prevent Phishing Attacks (According to 33 Experts)" by Juliana De Groot. Arthur Zilberman, an IT manager says, "Companies fall prey to phishing attacks because of careless and naive internet browsing. Instituting a policy that prevents certain sites from being accessed greatly reduces a business' chance of having their security compromised." (Para. 14). In this scenario according to Zilberman employees searching freely is a way for hackers to try and target the employees. Another reason companies fall prey to phishing attacks is the apps that are installed on the employers' mobile devices. According to expert Dave Jevan's, a security CEO:

> A new threat vector that has been introduced by the BYOD trend is that apps on employees' mobile devices can access their address books and export them to sites on the Internet, exposing the contacts to attackers who use them for targeted spear phishing. One important step for businesses to take is preventing prospective attackers from accessing the corporate directory, which includes names, email addresses and other personal employee information. Installing mobile security software on user devices that scans apps and prevents users from accessing the corporate networks if they have privacy leaking apps is recommended. (Para. 28).

There are many things to consider even if an employee is not using the computer systems for the job but is still on the same network.

The one thing in common is to have an employee become more informed on phishing and being taught the consequences of falling prey to a phishing scam. Employers need to have rules and guidelines of what is allowed at work. Some more ways to avoid phishing include double checking emails that are sent out. Some users fall victim since they clicked the link of an email that was sent to them because they believe it is from someone they know. This is also the reason they give out personal information. According to expert Jared Schemanski, Security Analytics Team leader that works at Nuspire Networks,

> If the email comes directly from an acquaintance or source that you would typically trust, forward the message to that same person directly to ensure that they indeed were the correct sender. This means, do not simply just hit reply to the email with whatever information was requested in the email. Similarly, when you receive an email from a trusted source and it seems phishy (pun intended), give that person a call directly and confirm that the email was from them. You'll be able to check to see what is or what is not legitimate by dragging your cursor over the email sender as well as any links in the email. If the links are malicious, they will likely not match up with the email or link description. (Para. 36).

Sometimes something as simple as double checking with the person who sent the email can save a whole load of trouble. A hacker wants to make the lie as believable as they can, the power of phishing is how believable the hacker can make themselves be to get a user to trust them, which means sometimes the best thing is to trust no email, and always verify it.

New Developments.

Current research on dealing with phishing is simply taking statistics and seeing where the major attack really comes from. Companies can use these statistics and see where they need to get stronger security in, and where to really focus on. This would help companies make their employees more aware and help them figure out which filter should go into effect to help their employees to not receive any scammer emails. Companies are currently making sure their network is safe, and making sure to keep track of what the employers can and can't use on business systems. Another main thing new research shows is two step authentications really help with making sure that even if the hacker tries to get into the accounts, they will need the access code.

Conclusions.

Phishing started off with just emails being sent out, that tied to tricking the user into giving personal information. However, phishing has now turned into email, text message, voice recording AI, emails, and so much more. Phishing has different ways to try and be avoided, this includes making sure everyone understands the importance of a strong password, and the changing of a password. Another main thing to always remember is to make sure that everyone turns on two step authentications, this gives a little extra layer of security, and makes it harder for hackers to steal information. Phishing is something that will never be fully stopped, but one day it needs to be something that everyone is familiar with and knows how to handle for the most part.

Bibliography

Bannister, A. (2023, February 7). *Toyota sealed up a backdoor to its global supplier Management Network*. The Daily Swig | Cybersecurity news and views. Retrieved April 3, 2023, from https://portswigger.net/daily-swig/toyota-sealed-up-a-backdoor-to-its-global-supplier-management-network.

Bolland, E. (2021, February 9). *The surge in phishing attacks and changing threats in 2021*. usecure Blog. Retrieved April 3, 2023, from https://blog.usecure.io/a-complete-guide-to-Phishing-threats#:~:text=New%20Phishing%20Methods%20for%20Attackers%20in%202021&text=Smishing%20is%20essentially%20%E2%80%9Cany%20kind,users%20of%20the%20smishing%20threat.

Gillis, A. S. (2020, May 5). *What is phishing? how it works and how to prevent it*. Security. Retrieved February 1, 2023, from https://www.techtarget.com/searchsecurity/definition/phishing.

Hadnagy, C., & Fincher, M. (2015). *Phishing dark waters: The offensive and defensive sides of malicious e-mails* (1st ed.). Wiley.

Harris, E. A. (2022, January 5). *F.B.I. arrests man accused of stealing unpublished book manuscripts*. The New York Times. Retrieved February 2, 2023, from https://www.nytimes.com/2022/01/05/books/publishing-manuscripts-phishing-scam-filippo-bernardini.html.

Hebert, A., Hernandez, A., Perkins, R., & Puig, A. (2022, October 25). *How to recognize and avoid phishing scams*. Consumer Advice. Retrieved February 2, 2023, from https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

Internet Crime Complaint Center (IC3) | FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic. (n.d.). Www.ic3.Gov. https://www.ic3.gov/Media/Y2020/PSA200320

Irwin, L. (2022, October 7). *The 5 biggest phishing scams of All time*. IT Governance Blog En. Retrieved February 2, 2023, from https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time.

Irwin, L. (2023, January 31). *The 5 most common types of phishing attack*. IT Governance Blog En. Retrieved April 3, 2023, from https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack.

James, L. (2005). *Phishing exposed*. Syngress Pub.

Juliana De Groot on Friday March 3, Lord, N., & Roberts, P. (n.d.). *4 steps to prevent phishing attacks (according to 33 experts)*. Digital Guardian. Retrieved April 3, 2023, from

https://www.digitalguardian.com/blog/phishing-attack-prevention-how-identify-prevent-phishing-attacks.

Kovacs, E. (2022, October 28). Twilio Says Employees Targeted in Separate Smishing, Vishing Attacks. SecurityWeek. https://www.securityweek.com/twilio-says-employees-targeted-separate-smishing-vishing-attacks/

Lawrence, D. F. (2023, January 4). *Army warns of scams targeting new soldiers*. Military.com. Retrieved April 3, 2023, from https://www.military.com/daily-news/2023/01/04/army-warns-of-scam-targeting-new-soldiers.html.

New credentials phish targets employees with salary increase scam. Cofense. (2023, January 23). Retrieved April 3, 2023, from https://cofense.com/blog/new-credential-phish-targets-employees-salary-increase-scam/.

Novitsky, M. (n.d.). *Expert warns of new scam using deepfake AI technology*. https://www.kold.com. Retrieved April 3, 2023, from https://www.kold.com/2023/03/14/expert-warns-new-scam-using-deepfake-ai-technology/.

Phishing attacks soar 220% during COVID-19 peak as cybercriminal opportunism intensifies. F5 Feature Article. (n.d.). Retrieved April 3, 2023, from https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal.

Seals, T. (2017, May 8). FBI: Whaling and BEC Scams Rack Up $5bn in Ill-Gotten Gains. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/fbi-whaling-and-bec-5bn/

Sonowal, G. (2021). *Phishing and Communication Channels: A guide to identifying and mitigating phishing attacks* (1st ed.). Apress.

Spear Phishing Attack Exposes Tax Information of 3,000 Community College Employees - Security News. (n.d.). Www.trendmicro.com. Retrieved April 17, 2023, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/spear-phishing-attack-exposes-tax-information-of-3-000-community-college-employees

Vedova, H., & Technology, T. F. T. C. O. of. (2021, July 16). *Phishing scams*. Federal Trade Commission. Retrieved April 3, 2023, from https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams.

Www.cai.io. (2022, September 22). *How to prevent phishing in Cybersecurity*. www.cai.io. Retrieved February 2, 2023, from https://www.cai.io/resources/articles/how-cybersecurity-practices-can-prevent-phishing.

COFENSE. (n.d.). How to Spot Phishing Emails | 7 Helpful Tips for Employees. Cofense. https://cofense.com/knowledge-center/how-to-spot-phishing/\

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021, January 18). *Phishing attacks: A recent comprehensive study and a new anatomy*. Frontiers. Retrieved April 20, 2023, from https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full