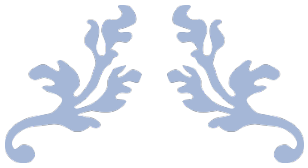


PHISHING AND HOW TO PREVENT IT

By Kimberlynn DeBolt
Henry Ford Community College
University of Detroit Mercy

Introduction

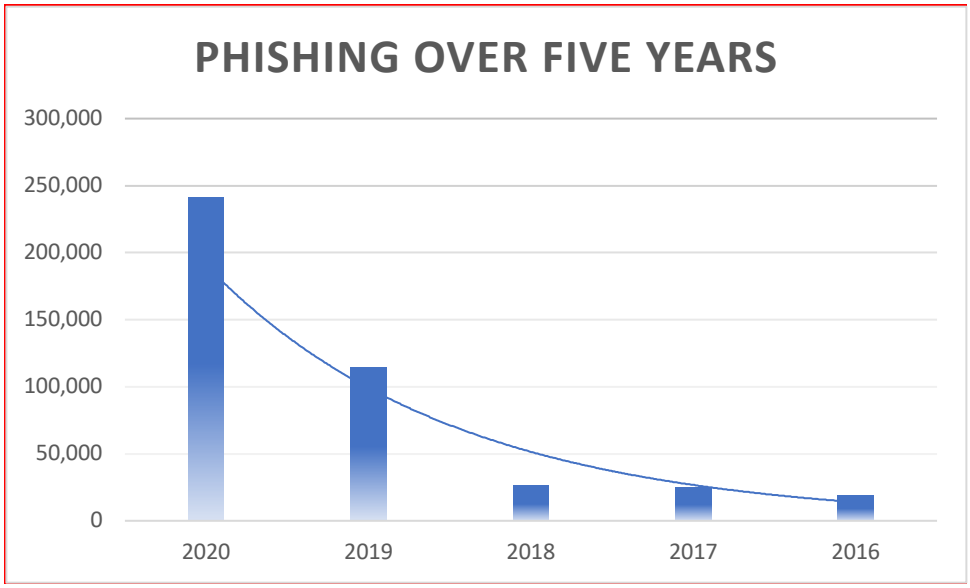
Are you at risk of a Phishing attack? Phishing can be very dangerous if you do not have the knowledge to detect it. Any information that is disclosable through email is up for grabs. This can put anyone at risk of giving information to people with malicious intent; all while appearing to be a trustworthy entity. Phishing attacks make up some of the largest portions of data threats and have been increasing in frequency at exponential rates. What is phishing? Who is most at risk and effected by phishing? How can you prevent phishing? These questions will all be explored and answered below to offer a more comprehensive understanding of the topic at hand.

What is Phishing?

Phishing, a type of cybercrime that makes use of social engineering, is extremely dangerous and should be taken very seriously. There are many different types of phishing such as: spear phishing, whaling, smishing, vishing, and more. They all revolve around using fraudulent messages that appear legitimate to deceive the receiver into providing confidential information or even downloading malware. Information that is often the goal of a phishing message can include passwords, personal information such as a social security number, credit card numbers, account numbers, other financial information, etc.

For example, an individual receives an unprompted email that prompts them to change their password; however, the link included in the email is completely unrelated to the initial website that the individual was using. The link may even route the user to a spoofed website of a copy of the original. The probability that this email is a phishing attack, attempting to gain access to the individual's password is high. *Spear phishing* utilizes the same concept; however, spear phishing emails are designed to target specific individual(s) as opposed to a less specific email

(phishing) which is typically sent in mass. *Whaling* is also a targeted phishing attack; however, the target of a whaling attack involves the "big fish" (high ranking members or executives) of an organization. *Smishing*, also known as SMS (Short Message Service) phishing, enforces the same concept as phishing while utilizing text messages instead of emails. *Vishing or* voice phishing uses automated voice massages to trick individuals into providing information.



This table was made from information gathered from the FBI- Internet Complaint Center, Internet Crime Report 2020

Who is at Risk?

Phishing can essentially affect anyone who has access to email, text messaging, a phone, or social media. Anyone who has access to these and is not equipped to spot a phishing attack is potentially a target. While whaling is specifically targeted toward high-ranking executives and spear phishing target other individuals, other forms of phishing often target a wide array of individuals and target as many people as they can to increase the chances of return.

Cybercriminals do not often discriminate so businesses, individuals, and groups can be targets. While vishing targets a variety of people, often times the elderly and those who have minimal experience with technology become victims of this scam. The cybercriminals use recordings to establish a sense of urgency to confuse and prompt the individual to disclose different types of information (with elders often times financial information). Cyber criminals can employ a multitude of attacks and use information from prior attacks to make their attacks seem even more legitimate and even pose as someone the victim knows.

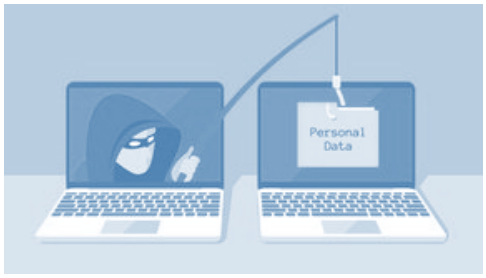
How can You Prevent Phishing?

Being able to recognize signs of phishing is the best way to be vigilant against it. If one is able to recognize a threat they will be better equipped to avoid it all together. Cybercriminals change their techniques in attempts to gain the upper hand against their victims and phishing attacks are no different. Phishing attacks come in several different shapes and sizes, so it is extremely important to be able to verify the whether the information they hold is fraudulent or not.

It is important not to immediately open any emails, attachments, or messages that are not recognizable. When an unrecognized email is received, hover the mouse over the email without clicking the email to view the sender's email address. Look for any misspelled words and suspicious placement of the domain name.

Phishing often tries to create a sense of urgency. They may proclaim that they've spotted suspicious activity or a problem with your account, include a fraudulent bill, ask for confirmation of confidential information, offer free merchandise, etc. The cybercriminals will use legitimate company logos and formats to appear more believable. It is important for the

receiver to thoroughly review the information before clicking on any links, especially when they are unsolicited and beneficial to run the links or attachments through an antivirus software. Ask yourself if you have an account with the company or if you have had any recent activity with the company to warrant a response. Contact the company by other means that are not provided by the suspected phishing attempt. For example: contact the company through a phone number. Ensure that the company is legitimate, they will most likely be able to verify information within the email if it is legitimate. When one recognizes a phishing attack, it is important to report the attempts to the federal trade commission: ftc.gov/complaint.



Email spam filters often catch many phishing attempts before they reach the receiver and redirect them to a spam folder. Smart phone technology has advanced to prevent vishing calls and immediately labels them as spam. There are many applications are available to prevent vishing and smishing calls which let the user establish a filter to catch the vishing and smishing attempts in the future and block them. Also, ensure that all software is updated on all devices and protect your devices by using a security software. Back up all of your data and ensure that that data is not connected to the main network by using an external hard drive or cloud storage. Utilizing multi-factor authentication is also a great way to add extra security to your accounts and devices.

More ways to practice stronger security to protect against phishing include: use strong passwords, encrypt sensitive data, do not save your log in information when using a browser, turn off your Wi-Fi when not in use, disable auto Bluetooth pairing when not in use, do not auto join unknown Wi-Fi networks, keep all your apps updated and do not download apps or content from suspicious developers, and any other steps you can take any security within your devices.

References:

FTC (Federal Trade Commison). (2019, May). *How to Recognize and Avoid Phishing Scams*. Retrieved from Federal Trade Commison: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Internet Crime Complaint Center. (2020). *Internet Crime Complaint Center Internet Crime Report*. Retrieved from ic3.gov: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

KnowBe4. (2021). *KnowBe4- What is Phishing?* Retrieved from knowbe4.com: https://www.knowbe4.com/phishing

Office, F. N. (2021, March 17). *FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics*. Retrieved from FBI.gov: https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics