Phishing Attack Awareness

Isaac Collins
Department of Computer Science
Hampton University
Hampton, VA

Abstract- Phishing Attacks, cybercrime in which a target(s) is contacted by someone posing as a legitimate institution to lure individuals into providing sensitive data. The problem at stake is most people who use smartphones, tablets, and computers do not know how to protect themselves from phishing attacks, making themselves susceptible to data theft. This paper will use research of phishing attack types, what makes those more vulnerable to phishing attacks, and how to detect and report them. Additionally, I will interview a Department of Homeland Security employee working in cybersecurity as they have an insightful perspective on the problem. I will combine my research and in-person interview to conduct a literary search on the best methods to prevent and avoid phishing attacks for the average technology user to practice, especially children. This will give a valuable solution to the problem, decreasing the rate at which phishing attacks are successful.

I. Introduction

Phishing is defined as the fraudulent practice of sending emails or messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers [1]. As one of the top methods used to compromise user accounts [1], phishing enables hackers to steal this personal information for personal benefit or identity theft. Here are the eleven types of phishing attacks used today. First, *email phishing* or "deceptive phishing" is one of the most well-known attack types. Here, hackers use deceptive emails impersonating a known brand to lead people to click a link [3]. Traditionally, the links go to malicious websites that either steal credentials or install malicious code, known as malware, on a user's device. Next, *spear phishing* targets specific individuals within an organization using real names, job functions, or work telephone numbers to make the recipient think the email is from someone else inside the organization [8]. *Whaling/CEO fraud* involves impersonating an organization's leader by using a similar email address, asking for a money transfer or request that the recipient review a document [3]. *Vishing* or "voice phishing" is phishing over the medium of phone calls or voice enabled devices. Cybercriminals calls a phone number and creates a heightened sense of urgency that makes a person take an action against their best interests [1]. The next evolution of vishing is *smishing,* phishing over text message or SMS that involves the recipient to act and click a link [1]. Below is a common example that I have received on several occasions.

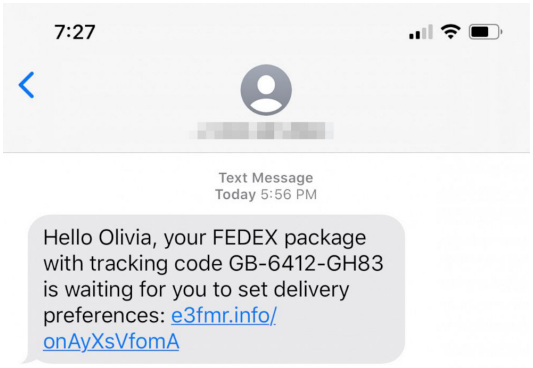


Figure 1: Smishing example on iMessage

Cybercriminals using notifications or direct messaging in social media to entice someone into taking action is defined as *Angler phishing* [7]. Next, *pharming* involves hackers hijacking a Domain Name Server (DNS) to redirect a user to their fake malicious website [8]. *Pop-up phishing* happens when cybercriminals use pop-ups to prompt users to install their trojan horse code, a malicious program that appears innocent [3]. For example, when a person visits a website, the browser prompts the person with "www.thisisabadchoice.com wants to show notifications." When the user clicks "Allow," the pop-up installs malicious code. *Clone phishing* is another targeted email phishing attack, hackers send near copy of a legitimate or previously sent emails that contain malicious links [3]. For example, many organizations use DocuSign to send and receive electronic contracts, so malicious actors might create fake emails for this service. *Man-in-the-middle* uses a fake Wi-Fi hotspot to intercept a user data during transfer [8]. If someone uses the fake hotspot, the malicious actors can engage in man-in-the-middle or eavesdropping attacks, collecting sensitive data [8]. Lastly, Watering hole phishing happens when cybercriminals infect websites that members of an organization are known to visit [7]. This is one of the most sophisticated types as no member can detect an infected but functional website [7]. Furthermore, the advancement of phishing attacks is a major drawback for a world dependent on technology. While there were once twice as many malware sites as phishing

sites, there are now nearly 75 times as many phishing sites as there are malware sites [11]. Google has registered 2,145,013 phishing sites as of January 17, 2021. This is up from 1,690,000 on January 19, 2020 (up 27% over 12 months) [2]. Today, 80,000 people are victims of malicious activity each day from phishing emails [5]. The FBI estimates cybercriminals have stolen more than $12 billion from companies (including Facebook, Google, and more) over a five-year span using phishing attacks and business email compromise [4]. The change in the phishing threat landscape is attributed to the increased use by cybercriminals of automation and AI [9]. The question is what are computer users going to do before they fall victim to another phishing attack?

Problem Statement

Phishing Attacks are increasingly becoming a real threat to the integrity and privacy of user and company data. The problem at stake is individuals don't know how to identify phishing scams from real messages or emails. This research will prove how to protect personal information from being reeled in by hackers.

II. Methodology

This study will use a combination of information gained from literature review, user surveys, and a subject-expert interview to collect data and gather results directly related to my thesis. Each methodology is explained as follows:

A. Literature Review

In review of what experts have done, we will detail how to identify/detect each of the eleven types of phishing scams. One can identify a phishing scam and its type by using its primary indicators. For example, people can identify *email phishing* by looking for shortened links that are commonly used to bypass secure email gateways [7]. One can identify *spear phishing* by disregarding any password-protect documents, which are often used to steal user credentials [12]. In a professional setting, one can detect *whaling/CEO fraud* by verifying if the senior leader's email address is legitimate. This can be done by contacting higher officials that communicate with the senior leader via email. When receiving *vishing* scams or voice call phishing, both apple and android use caller ID to detect spam risk calls, preventing the user from falling victim [8]. When identifying *smishing*, the sender usually has an abnormal area code that is outlier from your current contact list. Additionally, a text often requests a recipient to "change a delivery" using an included link [1]. On social media, direct messages from people who have no connection with you and include website links are easily seen as *angler phishing* scams [5]. When detecting *pharming*, an insecure website that start with HTTP and not HTTPS is a primary indicator [10]. *Pop-up phishing* varies in level of legitimacy between devices. On a laptop or PC, the appearance and content of the pop ups are too bizarre and abnormal to call legitimate. On mobile devices, pop ups bear legitimate and common identity elements. Nevertheless, one can review pop ups for spelling errors or abnormal color schemes in hope to detect them. *Clone phishing* is identified when the service provider begins requesting personal information (date of birth or address) that they never asks for [2]. *Man-in-the-middle* can be difficult to catch, but their presence does create ripples in regular network activity. To detect, inspect current Wi-Fi connections and check for unexpected and/or repeated connections as attackers forcefully disconnect users to intercept their login credentials upon reconnection [6]. Finally, an organization's officers can detect *watering hole phishing* by first implementing web gateways to act as a detection layer for incoming traffic. Afterwards, officers should disable user access to programs (Adobe Reader, Flash, Internet Explorer) commonly used in watering hole attacks [1]. We will review how to prevent or minimize one falling victim to phishing. One can install anti-phishing applications, such as Netcraft Anti-Phishing, MetaCert, Avast Mobile security, on their devices. These applications act as cybersecurity products designed to detect phishing content in emails and text messages, filtering messages coming from any malicious source by verifying their origin with the databases of phishing websites [3]. One can install virus protection programs, such as Norton, McAfee, and Bitdefender, on to their systems, preventing, detecting, and removing malware on a device [11]. Anti-spyware is another method to prevent phishing as this software is designed to prevent, detect, and remove unwanted spyware program installations [11]. Users must keep their software up to date to remove vulnerabilities fixed by security officials. Requiring multi factor authentication can mitigate the risk of cybercriminals stealing user credentials by having a two-step log in for networks, systems, and applications (password along with a fingerprint) [10]. Next, train yourself or your employees with phishing awareness training. As hackers evolve their methodologies, one should undergo training that goes beyond the traditional "phishing emails" approach [13]. Now for iPhone users, turning on "Block Pop-ups and Fraudulent Website Warning" under Safari in settings is a great method to prevent phishing on your device. For android users, the same applies for turning on "Enable spam protection" in settings [15]. Finally, we will discuss how to report them in personal and professional environments. For example, email platforms such as Gmail, Outlook, and Yahoo, have an option to "report phishing" within a received suspicious email. On iPhone, one can take a screenshot of a message and email it to Apple directly at imessage.spam@icloud.com [9]. On android, the same applies through the following: long press the chat containing the spam message, tap the circle with a line through it ("no" symbol) in the top right, and enable "Report Scam" [9]. Nevertheless, all cell phone users can report phishing by texting the spam message to 7726 (spells out "SPAM") [1]. Through this literature review, details about detecting, reporting, and preventing falling victim to phishing attacks can be learned and carried into one's online behavior. With this, we can contrast the above expert analysis to how educated people are on phishing via our online survey. We will use this as a foundation to formulate simplified steps and guidelines for people to follow when they encounter "phishing-like" messages.

B. Survey

We will collect data from users across campus and social media platforms (Instagram, Facebook, and GroupMe) through conducting a survey on Google forms. I chose this platform due to its user-friendly interface to create in-depth understandable surveys. Not to mention, Google form's popularity amongst the public makes it more attracting for people to fill out. I chose the social media platforms, Instagram, Facebook, and GroupMe, to

find a solid age range amongst respondent data. Younger people, or those below 38 years old, are socially active on Instagram while those of Generation X, 40 and older, are socially active on Facebook. I used GroupMe to get data from students across campus as I'm in a few group chats with hundreds of students each. This brings me to my target audience as I am aiming to get responses from people between the ages of 18-75. This will allow me to get a solid understanding of each generation's knowledge, experience, and awareness of phishing scams and attacks. In the survey, one will answer the following questions. What is your age range? Multiple-choice options are 18-24, 25-40, 41-56, 57-66, or 67-75. Which of these phishing attack types are you aware of? Checkbox options are email phishing, spear phishing, whaling/CEO fraud, vishing, smishing, angler phishing, pharming, pop-up phishing, clone phishing, man-in-the-middle, watering hole phishing, and none. Which of these phishing types have you been exposed to? Checkbox options are the same as that of the previous question as we are narrowing down which types are most active amongst general users. How many phishing scams have you received this year? Multiple-choice options are 1-3, 4-6, 7-9, 10+, or none. Check off the actions you did after receiving a phishing scam. Checkbox options are reported the scam, deleted the message, blocked the sender, clicked the link, I did nothing, or I've never received a phishing scam. Which of the following methods are you aware of to prevent or minimize phishing? Checkbox options are anti-phishing applications, virus protection programs, anti-spyware/firewalls, multi-factor authentication, phishing awareness employee training, installing website alerts in browsers, turning on turning on spam protection in settings on iPhone/android, and none. Which of the following methods are you aware of the ways to report phishing? Checkbox options are using the e-mail option to "report phishing" emails you receive, taking a screenshot of message and emailing it to Apple at imessage.spam@icloud.com, texting the spam message to 7726, long press the chat, on android, containing spam message, tap the circle with a line through it, and check off "Report Spam", and none.

C. Interview and Discussion

We will collect data about phishing attacks by interviewing Patricia Wolfhope, a Science and Technology Directorate of the Department of Homeland Security. As an intern under Wolfhope, I witnessed the extensive measures she takes in digital forensics and cybersecurity, making her an expert to be interviewed for our topic. Wolfhope will discuss her experience and knowledge of phishing scams and attacks in personal and professional environments. Wolfhope will extend by providing expert advice on how people can become less prone to phishing. For example, one of the questions asked in the results section is: given your professional career, what practices would you recommend following to avoid and prevent phishing scams? In the end, I hope to gain a relevant subject-expert influence into how I can approach the analysis of my research.

III. Results

This section will cover the cumulative results obtained from our research methodology outlined in Section II.

A. Survey

This section will cover the cumulative results obtained from our research methodology outlined in Section II subsection B, online survey. To reiterate, the purpose of the survey is to gain a solid understanding of each generation's knowledge, experience, and awareness of phishing scams and attacks. There is currently a total of 100 active participants who completed the survey. The observation I expect to see is that almost all participants have experience with phishing scams and attacks, however, only a handful know how to avoid falling victim and report phishing. Let's detail the data summary starting with the first question, what is your age range?
Considering there is a total of 100 survey responses, the percentage of each option is precisely equal to the exact number of participants.

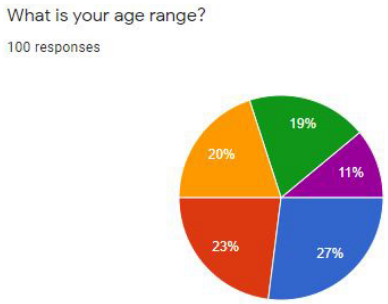


Figure 2: Question 1 from survey

As you can see, 27 participants (27%) are ages 18-24, 23 participants (23%) are ages 25-40, 20 participants (20%) are ages 41-56, 19 participants (19%) are ages 57-66, and 11 participants (11%) are ages 67-75. Currently, there is a solid number of participants from each age range, allowing the survey results to encompass all users per generation. The next question is designed to discover participant knowledge on the basics of phishing attacks. Which of these phishing attack types are you aware of? Here is a chart detailing the results:

Phishing attack type	Participants aware the type (Out of 100)
Email phishing	78
Spear phishing	23
Whaling/CEO fraud	22
Vishing	56
Smishing	79
Angler phishing	48
Pharming	23
Pop-up phishing	56
Clone phishing	21
Man-in-the-middle	17
Watering hole phishing	6

None	1

The following question is structured to depict what types of attacks are most popular amongst everyday users. Which of these phishing types (same as the previous question) has attempted to attack you? Once again, here is a chart detailing the results:

Phishing attack type	Participants who experienced the type (Out of 100)
Email phishing	64
Spear phishing	6
Whaling/CEO fraud	9
Vishing	29
Smishing	78
Angler phishing	34
Pharming	9
Pop-up phishing	26
Clone phishing	10
Man-in-the-middle	4
Watering hole phishing	2
NONE	2

The next question is written to understand how often phishing attacks present themselves to everyday users. How many phishing scams have you received in the past year? Let's look at the results in another simplified chart.

Number of phishing scams received	Participants who received this amount (Out of 100)
1-3	9
4-6	16
7-9	26
10+	47
None	2

The next question is designed to depict how participants are at identifying phishing attacks and avoiding harm. Below is a small chart displaying the results:

Action(s) done after receiving phishing scam	Participants who did action (Out of 100)
Reported the scam	20
Deleted the message	79
Blocked the sender	53
Clicked the link	24
I did nothing	14
I've never received a phishing scam	2

The following question is evaluating one's awareness in ways to prevent themselves from falling victim to phishing. Which of these methods are you aware of to prevent or minimize phishing? Here is another chart detailing the results:

Phishing prevention method	Participants aware of the method (Out of 100)
Anti-phishing applications	13
Virus protection programs	73
Anti-spyware/firewalls	34
Keeping device software up to date	71
Multi-factor authentication	62
Phishing awareness employee training	11
Installing website alerts in browsers	13
On iPhone, turning on "Block Pop-ups and Fraudulent Website Warning" under Safari in settings	22
On Android, turning on "Enable spam protection" in settings	5
None	3

Finally, the last question deals with evaluating individuals on their knowledge of reporting phishing. Which of the following methods are you aware of to report phishing? On the next column is an organized chart laying out the results.

Phishing report method	Participants aware of method (Out of 100)
Using the e-mail option to "report phishing" emails you receive	44
On iPhone, taking a screenshot of message and emailing it to Apple (imessage.spam@icloud.com)	4
On iPhone and Android, texting the spam message to 7726	8
On Android, long press the chat containing the spam message, tap the circle with the line through it, and check off "Report Spam"	5
None	51

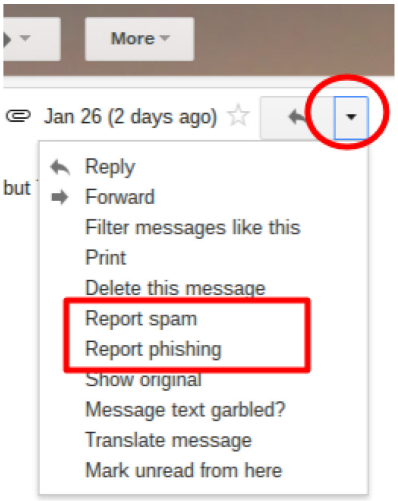


Figure 2: Example to "Report spam" and "Report phishing" on Gmail.

B. Interview and Discussion

Here, we started our interview with Patricia Wolfhope, Department of Homeland Security Science and Technology Directorate, by asking her the following question: Have you received any phishing emails or texts in the past year? If so, how many times and was your work phone number or email address involved? "Yes, I have, through both my work and personal email and cell phone. In the past year, I have received at least ten or so phishing messages or emails inside and outside of work." Once received, what do you do to report a phishing scam? "Without breaking confidentiality, specifically, at work, we have an Anti-Phishing Working Group that deals with matters like this. No matter the level of employee you are at Homeland Security, you must forward the message or email to them. This helps us avoid potential security breaches and ransomware attacks." Have any of your friends or family members been exposed or have fallen victim to phishing? "My daughter in high school received several phishing-like text messages from random numbers. I remember her asking me, did I ever order something from FedEx? I replied to her, 'I don't think so, why?' She then showed me her phone as a random number is giving her an 'update on her order' with a link attached. I blocked the number from her phone and deleted the message to avoid her falling victim." What tips you off when recognizing an email or message as a phishing scam? "To me, the fact that phishing scams are always written the same way tips me off. They start with the name of the alleged company like AT&T or Amazon, then they proceed to either give us a sentence like 'apologizes for the signal issues, here's a little gift' or 'here's an update on your order'. Finally, they wrap it up by including a link that ultimately will be used to steal someone's personal info." Given your professional career, what practices would you recommend following to avoid and prevent phishing scams? "There is no way of preventing phishing scams from being sent to you but there are ways to prevent someone from having their personal information exposed. First, if you don't know what the message or email is, do NOT click the link out of curiosity or wanting to understand what the sender is talking about. Second, minimize your digital footprint. The more active you are on technology platforms, the more likely you are to be exposed to a phishing scam. This can happen through Instagram direct messages or Facebook messenger you know; my daughter has received phishing messages on social media. Third, download anti-phishing tools on your personal and professional devices. Applications like Netcraft Anti-Phishing App, MetaCert, and Avast Security are great ways to protect your computer and/or cell phones."

C. Literature Review

In review of the 15 scholarly articles, I learned a piece of insightful phishing information that contributed to constructing my survey questions. The first article in my reference list, "Detection of phishing attacks", revealed the detailed definition of both *smishing*, phishing via text message or SMS, and *watering hole phishing*. It also provided ways to identify each phishing type using its primary indicators. The second article, "A survey of phishing attacks: Their types, vectors and technical approaches", gave the definition of *clone phishing* and how to recognize its type. The third article, "Defending against phishing attacks: taxonomy of methods, current issues and future directions", provides a review of installing anti-phishing applications, such as, Netcraft Anti-Phishing and MetaCert, in preventing or minimizing phishing. The fourth article, "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale", offers relevant background information to phishing attacks and how they have been growing most recently, something to keep in mind when evaluating survey results. The fifth article, "Preventing phishing attacks using text and image watermarking", revealed the definitions for angler phishing, phishing via direct messaging in social media, and how to detect them using their primary indicators. The sixth article, "Contributing factors to increased susceptibility to social media phishing attacks", details the definition for *man-in-the-middl*e phishing as well as how to inspect them using Wi-Fi connections and login credentials. The seventh article, "A new approach for the detection and analysis of phishing in social networks: the case of Twitter", provides the definition for *email phishing*, the most common and preventable phishing type, and how to detect them. The eighth article, "Updated Analysis of Detection Methods for Phishing Attacks", details what to do when receiving *vishing* scams, phishing via voice calls. For example, apple and android make it easier to save victims by using caller ID to detect spam risk calls. The ninth article, "Preventive techniques of phishing attacks in networks", offers two methods to report phishing. First, on iPhone, one can take a screenshot of a message and email it to Apple directly at imessage.spam@icloud.com. Second, on Android, long press the chat containing the spam message, tap the circle with a line through it ("no" symbol) in the top right, and enable "Report Scam". The tenth article, "Two-factor inauthentication–the rise in SMS phishing attacks", explains how to detect *pharming*, an insecure website used to draw victims, and *pop-up phishing,* pop-ups that prompt user to install hacker code, using their primary indicators. This article also lays out how to take advantage of multi-factor authentication to migrate the risk of phishing attacks. The eleventh article, "How Do Children Interact with Phishing Attacks?", reveals two methods in preventing phishing that everyday users (children included) can do right now. First, installing virus protection programs like Norton and McAfee. Second, installing anti-spyware, software designed to prevent, detect, and remove unwanted spyware

program installations. The twelfth article, "Cybersecurity awareness for children: A systematic literature review", identifies how can avoid *spear phishing* by disregarding any password-protected documents, often used to steal credentials. The thirteenth article, "Why is phishing still successful?", advised readers to train themselves and employees with phishing awareness training, going beyond the traditional approach. This is needed because regardless of the technical experience some employees hold, there are those who will accidentally fall victim before it is too late. For example, the fourteenth article, "Phishing Attacks: A Plan to Educate Employees and Mitigate Risks", explains how *Whaling* or *CEO fraud* is targeting newly hired employees and making companies more vulnerable to phishing. Finally, the fifteenth article, "Experimental Evaluation of Phishing Attack on High School Students", exposed a phishing prevention method for android users, to "enable spam protection" in settings. Nevertheless, all the above articles allowed me to get the most out of the participants in evaluating their knowledge and experience of phishing attacks. Combining these two methodologies with the subject-expert interview will engender a detailed analysis of results, which we will now dive into.

IV. Analysis of Results

A. User Phishing Knowledge Analysis

In section II subsection A, literature review, we discussed how to detect each of the eleven types of phishing attacks. One can easily use primary indicators to identify a phishing scam (for example, shortened URL links), nevertheless, the tactic is rendered useless if one has no idea what phishing attack types are out there. Therefore, survey participants were asked to identify the phishing attack types they are aware of. After analyzing the data summary, email phishing and smishing are well-known to the majority, with over 77 participants off. This makes sense as these are the most popular phishing types used by cybercriminals today. Additionally, this aligns with the results of my interview with Patricia Wolfhope, subject expert, who stated she is mainly exposed to email phishing and smishing in professional and personal environments. Next, vishing and pop-up phishing tie at 56 participants who are aware of the types. Given the contribution from older age groups, these types are older, yet still effective, that were more common before the 2010s. Since about 70 percent of people in the U.S. population have active social media accounts [7], the results of angler phishing were expected. Nevertheless, the remaining phishing types are unfamiliar to most. Only about 22 percent of participants knew of spear phishing, whaling/CEO fraud, pharming, and clone phishing. 17 participants know of man-in-the-middle while only 6 participants know of watering hole phishing. I expected these results as these are more advanced attack types than others previously mentioned. However, this makes them increasingly successful as the public is unaware on how to detect them. Even certain cybersecurity-career participants were unaware of watering hole phishing. These people can still do their best to implement measures to detect and disable incoming traffic that can contain watering hole attacks (web gateways, certain programs (Adobe Reader), used in watering hole attacks [1]).

B. User Phishing Experience Analysis

Next, in the literature review, we covered which phishing attack types are more common than others on everyday users. For people to eliminate themselves from becoming victims to phishing, it is important to prioritize which ones they will most likely be exposed to. Therefore, survey participants were asked to identify what phishing attack types they have been exposed to. After analyzing the data summary, smishing is the most common attack type as 78 percent of participants have been exposed. I expected this result as smishing is the most instant attack type that uses automation to send thousands of users a hacker's message [14]. Furthermore, this aligns with an interview question and response with Patricia Wolfhope. I asked Wolfhope "have any of your friends or family members been exposed or have fallen victim to phishing?" She replied that her daughter was exposed to several smishing ploys. For example, she received a text from "FedEx" offering an "update on her order" with an included hyperlink. Without Wolfhope's help, her daughter could have released her information to a cybercriminal without even knowing it. Next, 64 participants have been exposed to email phishing. I was not expecting this as email phishing is known to be the most common method used according to several sources in my literature review. Nevertheless, technology is advancing, and email is a less direct form of communication where Gmail and other email platforms are known to minimize phishing with internal tools. According to the data summary, the remaining attack types are much less known to users. 34 percent of participants are unaware of angler phishing. Clearly, younger generations, who are mostly on social media, need to educate themselves before they become victim. Vishing and pop-up phishing are only known to 26 percent of participants. I expected this result as technology is advancing past the success rate of these methods. For example, both apple and android use caller ID to detect spam risk calls, preventing the user from falling victim [8]. Once again, the more advanced types, spear phishing, whaling/CEO fraud, pharming, clone phishing, man-in-the-middle, and watering hole phishing, are only known to less than 11 percent of all participants. Especially after the previous section, these results are nothing short of expected. In fact, if these numbers were anything higher, I would be impressed as everyday users are not exposed to these like other attack types previously mentioned.

C. User Phishing Awareness Analysis

In the literature review, we highlighted methods to prevent/minimize phishing on everyday users. The methods detailed are found to be very successful at protecting people from exposure to phishing scams. Nevertheless, what good are these methods if there is awareness amongst the public to implement these tools into their devices. Therefore, I asked survey participants to identify the phishing prevention methods they are aware of. After analyzing the data summary, virus protection programs and keeping device software up to date are the most well-known methods with 72 participants checked off. This aligns with my expectations as with or without phishing, the two methods are recommended extensively by computer experts and tech companies to ensure that devices are running smoothly and protected from more common computer viruses. 62 participants recognize multi-factor authentication, something that companies like Google and Amazon are encouraging users to add onto their login credentials. Nevertheless, the remaining methods are unlikely to be known

by most participants. Only 34 percent of participants are aware of anti-spyware/firewalls. Individuals should not overlook this method as these applications and security implementations are proven to detect and remove about 50 percent of unwanted malware programs [2], like those found in phishing. 22 participants are aware of turning on "Block Pop-ups and Fraudulent Website Warning" in website browsing. I expected this result as before this research, I (a computer science major) did not know of this method. Only 13 participants are aware of installing website alerts in browsers and anti-phishing applications. Furthermore, this aligns an interview question and response with Patricia Wolfhope. I asked Wolfhope "given your professional career, what practices would you recommend following to avoid and prevent phishing scams?". She replied, "download anti-phishing tools on your personal and professional devices. Applications like Netcraft Anti-Phishing App, MetaCert, and Avast Security are great ways to protect your computer and/or cell phones." 11 participants are aware of phishing awareness training. This is more so at the fault of employers; most employees prioritize their given tasks when on the clock. If employers, implement phishing awareness training as a mandatory task for all employees, companies will be much less vulnerable to phishing attacks. Only 5 android users are aware of enabling spam protection in settings. I expected a low number here considering not too many of the participants were that of android users.

Additionally, in the literature review, practices on how to report phishing were summarized in detail. While some of these methods are more advertised than others, about half (51) of the survey participants were unaware of all practices. Not only is it important to know of ways to prevent falling victim to phishing but knowing how to report scams is crucial to stop future attacks. For example, apple and android offer simple and effective ways to report phishing. Unfortunately, only 8 percent of all participants are unaware of forwarding the spam message to 7726 (SPAM). 4 percent of iPhone-using participants are aware of sending a screenshot of the spam message to Apple directly. Big tech companies must make a stronger effort to advertise methods like this to encourage appropriate and safe action. On the other hand, it's encouraging that about 44 percent of participants are aware of using the e-mail option to report phishing emails they receive. Google, Yahoo, and other email platforms can increase these numbers dramatically if they shine a light on their integrated options. This aligns with the interview question and response with Patricia Wolfhope. I asked Wolfhope "once received, what do you do to report a phishing scam?". She answered "without breaking confidentiality, specifically, at work, we have an Anti-Phishing Working Group that deals with matters like this. No matter the level of employee you are at Homeland Security, you must forward the message or email to them. This helps us avoid potential security breaches and ransomware attacks." Therefore, no matter if it takes place in a professional or personal environment, one must report phishing to help prevent future attacks on others and yourself.

D. Phishing guidelines

To identify a phishing attack, one must search for relevant primary indicators. Obviously, certain indicators don't apply for all attack types. Therefore, first see which attack type aligns with the content of message you received. For example, when searching through a clone phishing scam, identify whether the service provider or brand is requesting personal information (date of birth or address) that they never ask for. Look out for the certain brands hackers often use to impersonate for phishing scams, like the ones below.

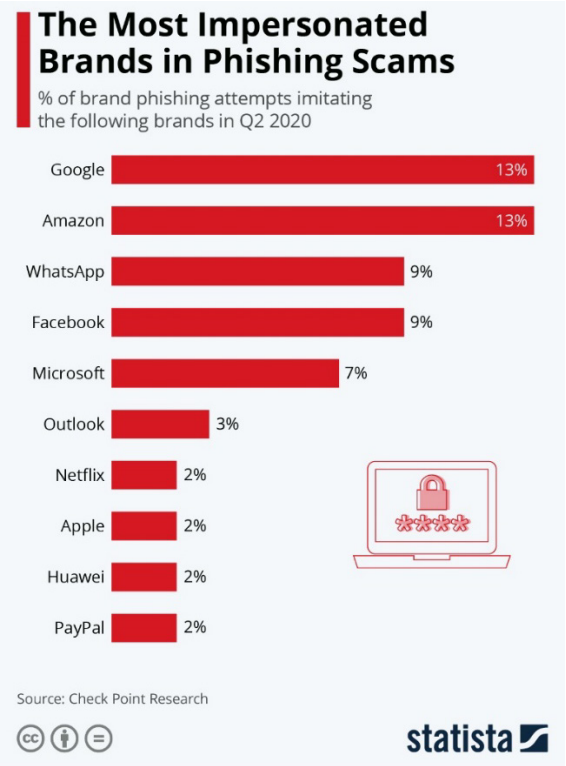


Figure 3: The most impersonated brands in phishing scams

To prevent a phishing attack, one must go through the following simplified guidelines:

1. Don't click on links impulsively, investigate them first and be suspicious
2. Install anti-phishing applications and virus protection programs on all devices
3. Doubt unexpected mails, especially if is too good to be true
4. Keep device software up to date (iOS and Windows updates)
5. Add multi-factor authentication on accounts with sensitive data
6. Install website alerts in browsers
7. Enable spam protection on mobile devices
8. Delete the message and block the sender!

To report a phishing attack, measures are simple, quick, and easy. As stated before, email platforms (Gmail, yahoo, outlook) allow users to use the “report phishing” when investigating an email, while all mobile users can forward the spam message to 7726 (SPAM), reporting the attacker.

V. Conclusion

Phishing has only seen an uprise in attacking everyday users. Clicking a link allows cybercriminals to steal your personal data in a matter of minutes. By providing simplified steps and guidelines, the above research proves how to protect personal information from being reeled in by hackers. This was accomplished through summarizing a literature review, conducting an online survey, and interviewing a subject matter expert. If I could this research over again, the only thing I would do differently is ensuring my survey questions are as detailed as possible before sending in for draft updates. I first sent out a survey and got back about 60 responses. However, after the professor reviewed my survey questions, it was clear they did not conclude anything about what the participants know about phishing in detail. After updating the questions to be more detailed, I sent the survey back out to my peers, classmates, faculty, and social media platforms. Nevertheless, it took much longer to accumulate an adequate number of responses as the survey was much more extensive and probably deterred people from taking the time to complete. Nevertheless, this research on phishing attacks has been not only insightful but a great use of my time as I enter the field of cybersecurity.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award# 1754054.

References

1. Baykara, Muhammet, and Zahit Ziya Gürel. "Detection of phishing attacks." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.

2. Chiew, Kang Leng, Kelvin Sheng Chek Yong, and Choon Lin Tan. "A survey of phishing attacks: Their types, vectors and technical approaches." Expert Systems with Applications 106 (2018): 1-20.

3. Gupta, B.B., Arachchilage, N.A.G. & Psannis, K.E. Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst 67, 247–267 (2018). https://doi.org/10.1007/s11235-017-0334-z

4. Oest, Adam, et al. "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale." 29th {USENIX} Security Symposium ({USENIX} Security 20). 2020.

5. Hajiali, Mahdi, Maryam Amirmazlaghani, and Hossain Kordestani. "Preventing phishing attacks using text and image watermarking." Concurrency and Computation: Practice and Experience 31.13 (2019): e5083.

6. Parker, Heather J., and Stephen V. Flowerday. "Contributing factors to increased susceptibility to social media phishing attacks." South African Journal of Information Management 22.1 (2020): 1-10.

7. Djaballah, Kamel Ahsene, et al. "A new approach for the detection and analysis of phishing in social networks: the case of Twitter." 2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS). IEEE, 2020.

8. Hernández Dominguez, Antonio, and Walter Baluja García. "Updated Analysis of Detection Methods for Phishing Attacks." International Conference on Futuristic Trends in Networks and Computing Technologies. Springer, Singapore, 2020.

9. Adil, Muhammad, Rahim Khan, and M. Ahmad Nawaz Ul Ghani. "Preventive techniques of phishing attacks in networks." 2020 3rd International Conference on Advancements in Computational Sciences (ICACS). IEEE, 2020.

10. Jakobsson, Markus. "Two-factor inauthentication–the rise in SMS phishing attacks." Computer Fraud & Security 2018.6 (2018): 6-8.

11. Alwanain, Mohammed I. "How Do Children Interact with Phishing Attacks?." IJCSNS 21.3 (2021): 127.

12. Quayyum, Farzana, Daniela S. Cruzes, and Letizia Jaccheri. "Cybersecurity awareness for children: A systematic literature review." International Journal of Child-Computer Interaction (2021): 100343.

13. Bhardwaj, Akashdeep, et al. "Why is phishing still successful?." Computer Fraud & Security 2020.9 (2020): 15-19.

14. McAnulty, Barry L. "Phishing Attacks: A Plan to Educate Employees and Mitigate Risks." Order No. 28495152 Utica College, 2021. Ann Arbor: ProQuest. Web. 16 Sep. 2021.

15. Marusenko, Roman, V. Sokolov, and Volodymyr Buriachok. "Experimental Evaluation of Phishing Attack on High School Students." International Conference on Computer Science, Engineering and Education Applications. Springer, Cham, 2020.

Appendix

Survey Questions

Questions Responses 100 Settings

Phishing Attack Awareness

In the form below, one will be asked a series of questions to evaluate their knowledge, experience, and awareness of phishing scams and attacks

What is your age range? *

- 18-24
- 25-40
- 41-56
- 57-66
- 67-75

Which of these phishing attack types are you aware of? *

- [ ] Email phishing - deceptive emails impersonating a known brand to lead people to click a link
- [ ] Spear phishing - targeting specific individuals within an organization
- [ ] Whaling/CEO fraud - impersonating an organization's leader by using a similar email address
- [ ] Vishing - phishing over calls (involves voice)
- [ ] Smishing - phishing over text message or SMS
- [ ] Angler phishing - notifications or direct messaging in social media
- [ ] Pharming - redirecting user to hacker's fake website
- [ ] Pop-up phishing - using pop-ups to that prompt users to install hacker code
- [ ] Clone phishing - near copy of a legitimate or previously sent emails that contain links
- [ ] Man-in-the-middle - uses a fake WiFi hotspot to intercept personal data during transfer
- [ ] Watering hole phishing - infecting websites that members of a group are known to visit
- [ ] None

Which of these phishing types has attempted to attack you? (same as above) *

- [ ] Email phishing - deceptive emails impersonating a known brand to lead people to click a link
- [ ] Spear phishing - targeting specific individuals within an organization
- [ ] Whaling/CEO fraud - impersonating an organization's leader by using a similar email address
- [ ] Vishing - phishing over calls (involves voice)
- [ ] Smishing - phishing over text message or SMS
- [ ] Angler phishing - notifications or direct messaging in social media
- [ ] Pharming - redirecting user to hacker's fake website
- [ ] Pop-up phishing - using pop-ups to that prompt users to install hacker code
- [ ] Clone phishing - near copy of a legitimate or previously sent emails that contain links
- [ ] Man-in-the-middle - uses a fake WiFi hotspot to intercept personal data during transfer
- [ ] Watering hole phishing - infecting websites that members of a group are known to visit
- [ ] None

How many phishing scams have you received this year? *

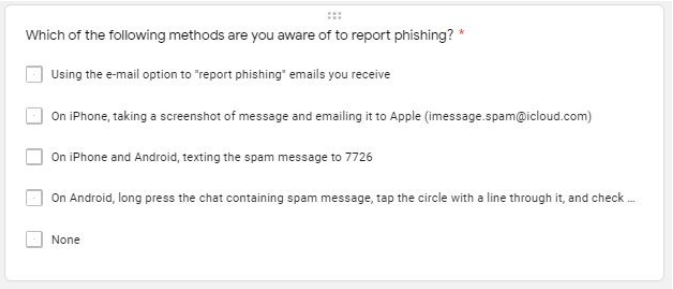
- 1-3
- 4-6
- 7-9
- 10+
- None

Check off the actions you did after receiving a phishing scam *

- [ ] Reported the scam
- [ ] Deleted the message
- [ ] Blocked the sender
- [ ] Clicked the link
- [ ] I did nothing
- [ ] I've never received a phishing scam

Which of the following methods are you aware of to prevent or minimize phishing? *

- [ ] Anti-phishing applications (Netcraft Anti-Phishing, MetaCert, Avast Mobile Security)
- [ ] Virus protection programs (Norton, McAfee, Bitdefender)
- [ ] Anti-spyware/firewalls (Spyware Detector, Anti Spy, Cell Spy Catcher)
- [ ] Keeping device software up-to-date (iOS and Windows updates)
- [ ] Multi-factor authentication
- [ ] Phishing awareness employee training
- [ ] Installing website alerts in browsers
- [ ] On iPhone, turning on "Block Pop-ups and Fraudulent Website Warning" under Safari in settings
- [ ] On Android, turning on "Enable spam protection" in settings
- [ ] None



Interview Questions

- Have you received any phishing emails or texts in the past year? If so, how many times and was your work phone number or email address involved?
- Once received, what do you do to report a phishing scam?
- Have any of your friends or family members been exposed or have fallen victim to phishing?
- What tips you off when recognizing an email or message as a phishing scam?
- Given your professional career, what practices would you recommend following to avoid and prevent phishing scams?