Phishing Attacks: Detection and Prevention

By **Shujaat Ali**

***Abstract*—Phishing is a new sort of network attack in which an attacker constructs a duplicate of an existing Web page to trick users into providing personal, financial, or password information to what they believe is the Web site of their service provider. Phishing is one of the most severe cyber-security issues, resulting in financial losses for both businesses and individuals. Detecting phishing attacks with high precision has always been a difficult task. Visual similarity-based approaches are now quite effective at detecting phishing websites. The primary purpose of this article is to evaluate the detection and prevention of phishing attacks. This article will discuss how businesses and individuals can detect phishing attacks and prevent them from happening beforehand, therefore keeping their data and personal and confidential data secure. While several methods are used to attempt a phishing attack, there are also many ways to detect and prevent them. This research paper will teach about how to detect and prevent some of the most common methods.**

Keywords—Phishing attacks, Phishing detection and prevention, Security.

I. Introduction

Phishing is a cybercrime in which a criminal sends a fake e-mail that looks to come from a well-known and reputable company or organization, requesting personal information such as bank passwords, usernames, etc. Fake e-mails frequently appear to be extremely genuine, and the website on which the Internet user is asked to enter personal information also seems to be honest. Anyone can fall victim to a phishing attack since phishing attacks are aimed to be as realistic as possible; as explained in the article Phishing & Anti-Phishing Techniques, ‘the E-mail contents have to be sufficiently realistic to cause the recipient to follow the directions in the Email’[1]. Attackers typically pose as workers of banks or other organizations to catch the victim's attention. It has become frequent in recent years as technology has advanced massively year by year; for example, banks have shut down branches since the number of people visiting a bank is decreasing and the number of people using online banking is increasing. As well as individuals, organizations are at risk of being attacked by phishing attacks; as stated in the review article, where it says, ‘Phishing is one of the major problems faced by the cyber-world and leads to financial losses for both industries and individuals.’[2].

In simple terms, phishing is when a cyber hacker attempts to gain sensitive details such as the victim's address or bank credentials. One method of doing this is posing to be a company such as a bank. Typically, attackers use the technique of phishing through websites such as banking websites because they can be designed and look very convincing, as websites are easy to replicate [3]. After this, the targets will get informed through emails or phone numbers posing as a bank, for example, saying there are details which need to be confirmed or modified [12]. This message will include a link to the replica bank website and will be used to collect the data as the user may log in thinking they need to update details. Rather than any actual information being required, the inputted data from the victim is collected and can be used or sold. This is just one method of phishing.

As mentioned, phishing attacks can be made on businesses and individuals. In a business environment, although there are many layers of protection on business networks, the attacker can still get through using methods such as using the internet when a user may click a link with a hidden virus which infiltrates the security, or even use a pop up on the web tricking a user to “update” their password by entering their current password as well as a supposed new passcode. Sometimes even a professional cyber security analyst could make a mistake, such as while downloading a program into the system network, they could potentially download a trojan into the network [13].

In the following sections, different phishing methods are explained: email phishing, social media phishing, evil twin phishing, and the personal experience of getting under attack. These methods are dangerous as they can steal sensitive information; they need to detect all these attacks. After detection, the prevention methods are also explained to prevent these malicious attacks. In the end, general prevention techniques are also described. The article's primary purpose is to explain phishing attacks and their detection and prevention methods.

II. History

Phishing started a long time back; however, until around the mid-’90s, there was little to no actual phishing software available. Before this, in 1994, there was a small community of self-identified people from America. It was mentioned in an article by the maker of the phishing software ‘AOHell’ [4], showing this is just one case from the millions of people who have done this attack, some maybe dating to the early days of the internet dating back to early-to-mid 1980s. ‘By 1983, ARPANET was being used by a significant number of defense R&D and operational organizations’ [5].

III. Different methods of phishing

There are many methods of phishing that all aim to get information on people or a specific person. Whether the target is a person or a business, there are many ways to get access to information through phishing; however, there are many ways to detect and prevent phishing. 3 main categories of phishing are presented below.

A. Phishing Email

One of the few most common ways of phishing is by asking the victim to visit a specific website. The hacker will most likely contact the potential victim by texting a phone number or sending an email that looks genuine, proposing the victim open the link and put in data, inserting their bank credentials or such information [14,15]. The website they will be directed to looks genuine, like an e-commerce or bank website, and will have a very similar URL to the official site. The potential victim in these cases can be anybody from a specific individual to a massive organization worldwide. An example of this is the bank of China, whose customers had been attacked where the actual website is www.bank-of-china.com; however, the attacker will send the victim to a website with the URL of www.bank-off-china.com and ask for information to be provided or confirmed. At a glance, these links look the same; however, if anyone look closely, the word "of" has been spelled differently in the counterfeited URL. If the target then inserts their data and information, they would have given their information to the attacker [6].

- **Detecting and Preventing the Email Threat**

There are many ways to detect phishing emails, such as checking if the email is actually from the company. It can be done in many ways; however, the first way to check if the email is genuine or not is by checking the logo shown, as an attacker would use an old or different logo. Anyone can compare this to the actual logo from the company, seeing them both side by side. In addition to this, the senders' email may not be from an honest company; for example, the official email may be "company@gmail.com", and the counterfeit email could be "C0mpany@gmail.com". There would be tiny differences such as this, which are only visible when they are looking for the authenticity of an email. On top of this, the persons can also look for any details, such as misspelt words which could suggest that the email is fraudulent.

Often, an email will come out of the blue, and most will contain a title or subtitle with the idea of the email being a high priority or a prize which awaits the details to be confirmed and shipped to needs to be replied to ASAP. Phishing emails will also contain suspicious links or sometimes will attach files to the email [16-18]. This email will lead to an unofficial site, such as a fake version of an official site. These are vital signs of an unofficial email. One of the best ways to prevent phishing emails is by ensuring the individual have security patches updated. This could prevent all users from proceeding, as many antiviruses would prevent them from giving information either by giving a warning or guiding them to a page that explains the threat the email potentially poses.

B. *Social Media Phishing*

The attacker would not always use the example of banking emails or websites. In certain circumstances, they would use a fake identity. One live example that occurs very often is that users are said to win a phone through a giveaway. Famous and well known British youtuber SuperSafs' followers have fallen victim to this many times as he is a known tech reviewer. Attackers would use fake accounts with similar names to SuperSaf. They would comment under an individual's tweet saying, "you are the winner of the iPhone 13 pro max! private message me to claim it!" or such to get details of the individual. Since they use the topic of a winner for a giveaway, the attacker would ask for details such as card details with the reason being "delivery to the address would cost". They try to attain the victims' address by asking where the device needs to be shipped, and the card details are collected after the attacker mentions the delivery cost to the specified location.

- **Detecting and preventing the social media Threat**

Typically, attackers tend to use bots to get the details of the users; therefore, it is quite straightforward to detect them. At times user can reply to the account with any random message; however, user would get the reply of "I am glad they have finally contacted me". The general conversation of this would be like a conversation with a machine because the bot will only have a fixed conversation set. With this being said, the reason for the reply given after an individual's reply to the bot is that the bots will usually have a first message response set and the next of the conversation. Since they have a bunch of messages, they send users can also try to converse with the account and see if there is an actual conversation; if not, then they know it is a bot, and it is certainly a fraudulent account. After figuring this out, the best thing to do is to report the account, as it would prevent others from possibly being phished [7].

Sometimes the victim will be directed to a website or another page of the social media site; however, they will be required to sign into their account again. If this is the case, do NOT insert any of the details, as this is a way for the attacker to access the individual's account. One of the best ways to prevent the attacker from signing into the account is by ensuring that two-factor authentication is activated. This will ensure to receive a code to confirm that the honest person is attempting to log in to the account. Also, if user feel like their account has been compromised, it is recommended to change their password to ensure security and keep the data safe [8].

C. *Evil Twin Phishing*

When the individuals are away from home and see Wi-Fi networks to which anyone could potentially connect? This could be an example of Evil twin phishing. In simple terms, the Evil twin phishing method is used to launch a man in the middle attack [9]. This means an attacker could eavesdrop on the victim or they could potentially impersonate the victim. In general, this would give the attacker details. They could check every keystroke, website, or application the victim visits as they have permission through the insecure Wi-Fi connection as they can easily modify or view unencrypted information. Sometimes the connection will even require an existing email to be used and the password. The given reason for this is to confirm an individual's identity; however, in reality, this is collecting the email address and password of the individual.

- **Detecting and Preventing Evil Twin Attacks**

"Detection is difficult for users because the access point to which a user's device binds does not identify itself in a fashion that the user can verify reliably [9]. Although this is true, there are still ways to protect from evil twin attacks; for example, one way to do this is by keeping away from any public Wi-Fi networks, which would protect individuals from any potential threat. As technology advances, antiviruses are also getting smarter; therefore, phones that can use antivirus software and laptops and devices would bring up notifications or prevent users from connecting to the network. Using the antivirus, the device could know from the start whether this connection is trustworthy or not [19-21]. If this is not available on the user's device, the next best thing to do is to disable auto-connect, as this would prevent the device from connecting whether anyone know it or not. Sometimes individual may need to use a Wi-Fi connection to do some activity. The best way to do this is by connecting to the Wi-Fi, ensuring users are not accessing any sensitive accounts or attempting to insert financial or personal details. On top of this, they can ensure connection safety by installing and running a top-quality VPN, ensuring a security level is put in place. This way, even if the data is exposed, the attacker will not use the data. Although VPNs could potentially work, there are still only several trustworthy VPNs; therefore, this could be dangerous.

Also, if the users are working in a business which has an internet connection, rest assured them will have a good secure connection as businesses would also have security measures in place to prevent attackers from accessing the internet; however, keep in mind that the connection would require details such as the work ID and password. Before connecting to a business Wi-Fi, ensure that it is the business Wi-Fi and not a third-party connection posing as the business. When out in public, the best thing to do is either use a very trusted Wi-Fi network or use the mobile data [22]. This way, users are protected from the threat of the public when there is an attacker.

D. *Personal Experience*

I have been a target of this attack when my mobile device was on sale on a massive online business (eBay), and I had been contacted about the phone regarding a purchase. The attacker's plan is straightforward; unfortunately, many people could be conned. This is because the eBay account could look genuine as it could have positive feedback from other sellers as attackers generally look for accounts created years ago that have been unused for some time. This means the account will still have details and information. The technique used in this case is messaging regarding an item of value such as a phone or laptop and asking for specific information such as "What is the reason for the sale?". After getting a reply, they would attempt to get the seller (me, in this case) to take off the item for sale and say, "I can pay for this via card, just message me through this email" and give a hacked email address. After this, they will ask for details such as card details and cardholder name etc and say they are going to send the payment; however, they are getting an error, and they will ask for more details which are personal to the individual. Since I knew how these attacks work, I did not follow any instructions given by the attacker and proceeded to report the account [23]. From research, I have learned that there are more ways; for example, they would ask for the option to collect in person, and the attacker would give a higher value for the item; for example, for a £500 item, they would offer £700 and say they wish to collect the item from the address to save time from delivery.

IV. General prevention techniques

Since phishing is a social engineering attack, an obvious solution can be educating society by informing them of the techniques used and the information the attackers try to get from the victim. This way, if there is any potential cyber hacker, people would get an inkling of what is going on and stop it before giving details that they shouldn't. A lack of knowledge on phishing attacks is why many people are targeted and successfully attacked. As shown in the International Journal of Human-Computer Studies, it is explained how, even after individuals were given the task of identifying whether a website is official or not, only 53% of the websites were detected, showing that the naked eye could potentially mistake a cyber attackers website for an official one [10].

Ultimately, the best solution in terms of email phishing in a business is ensuring all security patches in every antivirus are up to date; if they are not, it could lead to a detrimental loss of data or finances. After seeing the results of the phishing Attack on the NHS, which was caused by outdated software and only one user was vulnerable and opened to the attack, there was a massive loss after the attack. Financial loss and possible loss of lives due to the appointment stoppage was the outcome; however, lucky for the NHS, there was a kill switch found and luckily accessible. This ultimately saved more data from being exposed to the attacker [11].

V. Conclusion

After going through the main types of phishing methods as well as some prevention and detection techniques, it is concluded that in terms of an individual's day, the best way to achieve good security is by ensuring the user knows what the methods are and how to avoid falling into the trick of being phished. It is because attackers are getting wiser day by day and are finding new ways to penetrate through any security barriers they may face. One of the best and most valuable ways to avoid many threats in businesses and organizations is by ensuring the software and antiviruses are up to date. It could ultimately prevent many attacks from taking place. Having all the security patches up to date and understanding where there may be a threat is the way to go, whether users plan to protect information in a business or even their personal device with their own information.

References

[1] J. Chhikara, "International Journal of Advanced Research in Phishing & Anti-Phishing Techniques : Case Study Phishing attacks Exploit Based IM , IRC , etc," Int. J. Adv. Res. Comput. Sci. Softw. Eng., no. May 2013, pp. 458–465, 2014.

[2] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[3] A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity based approaches," Secur. Commun. Networks, vol. 2017, no. i, 2017, doi: 10.1155/2017/5421046.

[4] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," International Conference on Future Internet of Things and Cloud, Vienna, Austria, pp. 77-82, 2016.

[5] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," 16th Int. World Wide Web Conf. WWW2007, pp. 649–656, 2007, doi: 10.1145/1242572.1242660.

[6] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.

[7] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.

[8] K. Rekouche, "Early Phishing," pp. 1–9, 2011, [Online]. Available: http://arxiv.org/abs/1106.4692.

[9] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution."

International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[10] S. Rappaport, P. Podsiadlowski, and I. Horev, “The past and future history of Regulus,” Astrophys. J., vol. 698, no. 1, pp. 666–675, 2009, doi: 10.1088/0004-637X/698/1/666.

[11] C. Guo, “Detection Prevention,” Most, 2006.

[12] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, “Social Engineering Attack Strategies and Defence Approaches.” International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.

[13] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, “PhishAri: Automatic realtime phishing detection on twitter,” eCrime Res. Summit, eCrime, pp. 1–12, 2012, doi: 10.1109/eCrime.2012.6489521.

[14] A. Aleroud and L. Zhou, “Phishing environments, techniques, and countermeasures: A survey,” Comput. Secur., vol. 68, pp. 160–196, 2017, doi: 10.1016/j.cose.2017.04.006.

[15] V. Roth, W. Polak, T. Turner, and E. Rieffel, “Simple and effective defense against evil twin access points,” WiSec’08 Proc. 1st ACM Conf. Wirel. Netw. Secur., pp. 220–225, 2008, doi: 10.1145/1352533.1352569.

[16] I. Ghafir and V. Prenosil, “Malicious File Hash Detection and Drive-by Download Attacks,” International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[17] M. Alsharnouby, F. Alaca, and S. Chiasson, Why phishing still works: User strategies for combating phishing attacks, vol. 82. Elsevier, 2015.

[18] A. O’Dowd, “Major global cyber-attack hits NHS and delays treatment,” BMJ, vol. 357, p. j2357, 2017, doi: 10.1136/bmj.j2357.

[19] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, “Machine Learning for Botnet Detection: An Optimized Feature Selection Approach”. International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.

[20] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, “Security Threats to Critical Infrastructure: The Human Factor,” The Journal of Supercomputing, vol. 74(10), pp. 1-17, 2018.

[21] S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.

[22] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, “Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence,” International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[23] J. Svoboda, I. Ghafir, V. Prenosil, “Network Monitoring Approaches: An Overview,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.