ISSN: 0974-5823 Vol. 7 No. 4 April, 2022

International Journal of Mechanical Engineering

Phishing Attacks and It's Working Methodology and How Spear Phishing Is Happening in Modern IT Hubs

Sayan Karmakar,

(M. Tech Cyber Security and Digital Forensics)

Lovely Professional University

Dr Munish Bhatia

(Assistant Professor)

School of Computer Science and Engineering, Lovely Professional University

Abstract

From social media to net banking, the internet is really a pervasive technology which has made the lives of people more comfortable and easier. Security threats are being relentless with the emergence of internet technology. Phishing is one of serious threats in which attackers steal the user data with fake websites, emails or both. It is evident that both academia and industry are working tirelessly to come up with solutions to fight against phishing attacks. Hence, it is vital for organisations to look at the awareness among end users to prevent phishing threats.

Considering the above points, this paper is aimed to discuss how phishing works, types of phishing attacks, major causes of spear phishing, and measures to control such attacks. We will conclude with various challenges and issues which are vital to fight against those attacks.

Keywords *– phishing, spear phishing, hackers, security threats, cyberattacks*

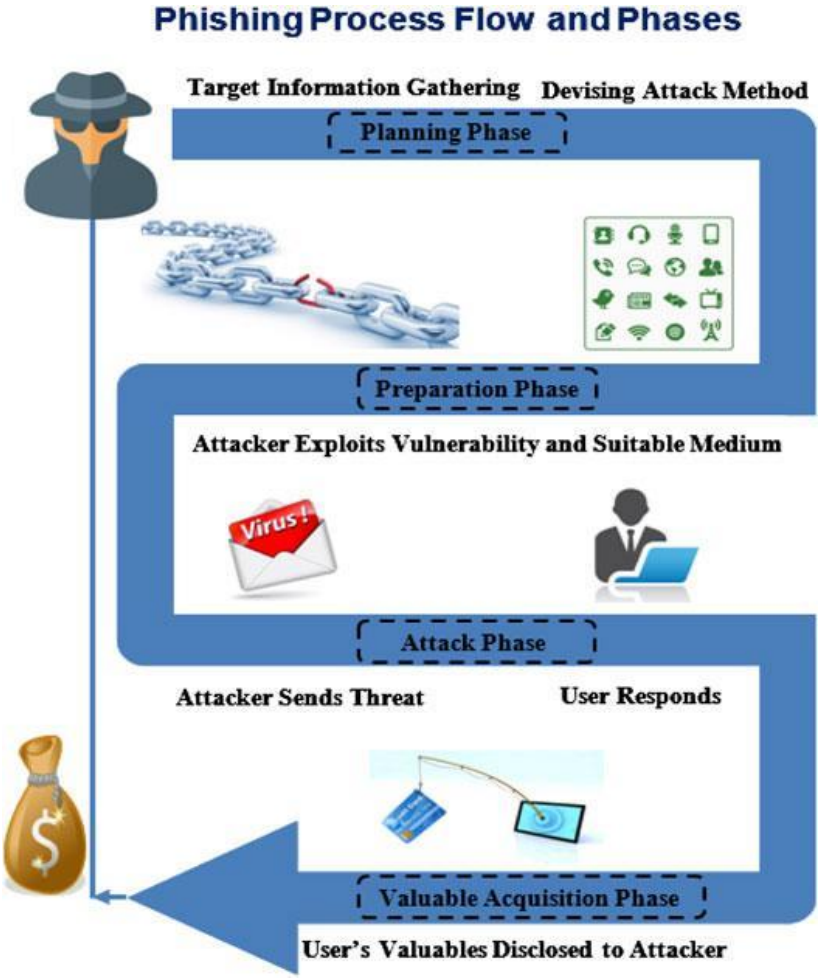
1. Introduction

Identity theft is one of the most threatening crimes on the internet (Ramanathan & Wechsler, 2012). It takes place when an attacker impersonates the identity of a person to use and steal their private data like social security number, bank details, or credit card number, etc. for their own interest for committing different crimes along with stealing money (Arachchilage & Love, 2014). Cyber criminals have their own methods to steal their data but they prefer social engineering attacks. Phishing is one of the most common social engineering attacks for identity theft. Phishing is a concept that emerged from "fishing", where a fisherman uses bait and trolls in a boat to catch the fish. This way, a "phisher" uses any mode of communication and trolls the internet to convince the user by impersonating someone else's identity as bait to steal users' data. The details they provide in the beginning look genuine at first glance.

Phishers redirect users to malicious pages by sending a malicious link through email, instant messaging, or other modes in phishing attacks (Gupta et al, 2015). They also target victims which are not specified into more selective methods by sending emails to targets through bulk email. This technique is known as "spear phishing". Users who are not much tech savvy or don't have cyber/digital ethics are major targets of cybercriminals. These attack vectors also use technical loopholes to execute their attacks. Vulnerabilities to phishing vary from person to person as per their awareness level and attributes. Phishers use human behaviour in most cases for hacking, rather than using smart technologies.

Although the weakness in the chain of information security is related more to humans than technology, lack of understanding is still prevalent on which ring is initially penetrated in this chain. According to some studies, some personal traits make individuals more receptive to several issues (Ovelgönne et al, 2017; Iuga et al, 2016; Crane, 2019). For example, people who mostly follow authorities above all are more likely to fall prey to a "Business Email Compromise (BEC)" which pretends to be from a bank or financial institution asking for quick action by making it look like an official email (Barracuda, 2020). Attackers also use humans' greediness as their tool to lure victims with attractive deals, huge discounts, goodies, free coupons, etc. (Workman, 2008).

Figure 1 – General Phishing Mechanism



Source – Alkhalil et al (2021)

Figure 1 illustrates the overall flow of the phishing process which takes place in four stages given in "Proposed Phishing Anatomy". Collecting data about the victim is usually the first stage in every phishing process. Then, choosing the appropriate attack method in the attack by the phisher is the next process as an initial step in the planning stage. Preparation is the second stage where an attacker looks for vulnerabilities to trap the victim. In the third phase, the phisher executes his attack and waits for the victim's response.

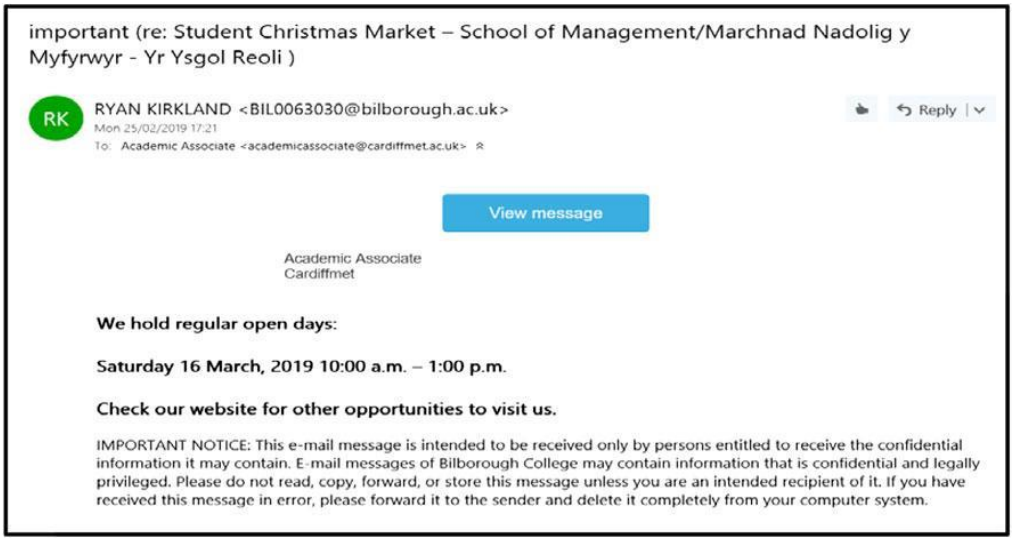
The "value acquisition" is the last step of the process of collecting the spoils. They may send a vicious email to the user showing themselves to be from a financial institution holding their accounts to elaborate the process, asking to verify account details or get their account suspended. The victim is supposed to believe that this is an official email because of the same trademarks, graphics, and colours that the bank uses. Then, the information submitted will be transferred to the phisher for various purposes like blackmailing, cash withdrawal, or other fraudulent activities.

1.1. Problem Identification

In order to identify the issues of phishing attacks, it is important to consider some real-world examples to discuss its complexity. Figure 2 illustrates a suspicious email which directly reached the mailbox of the user and bypassed the spam filters. The phisher smartly uses the sense of urgency in the matter using the term "important" in order to trigger emotional response in the user and lure them to click "View message". An embedded button was placed in the email. While hovering around that button, it didn't match the URL in the status bar.

In addition, the email address of the sender is suspicious and unknown to the receiver. When the user clicks on the attachment button, there are chances that either worm or a virus might be installed on the computer or the victim might be redirected to the malicious login page and enter the credentials.

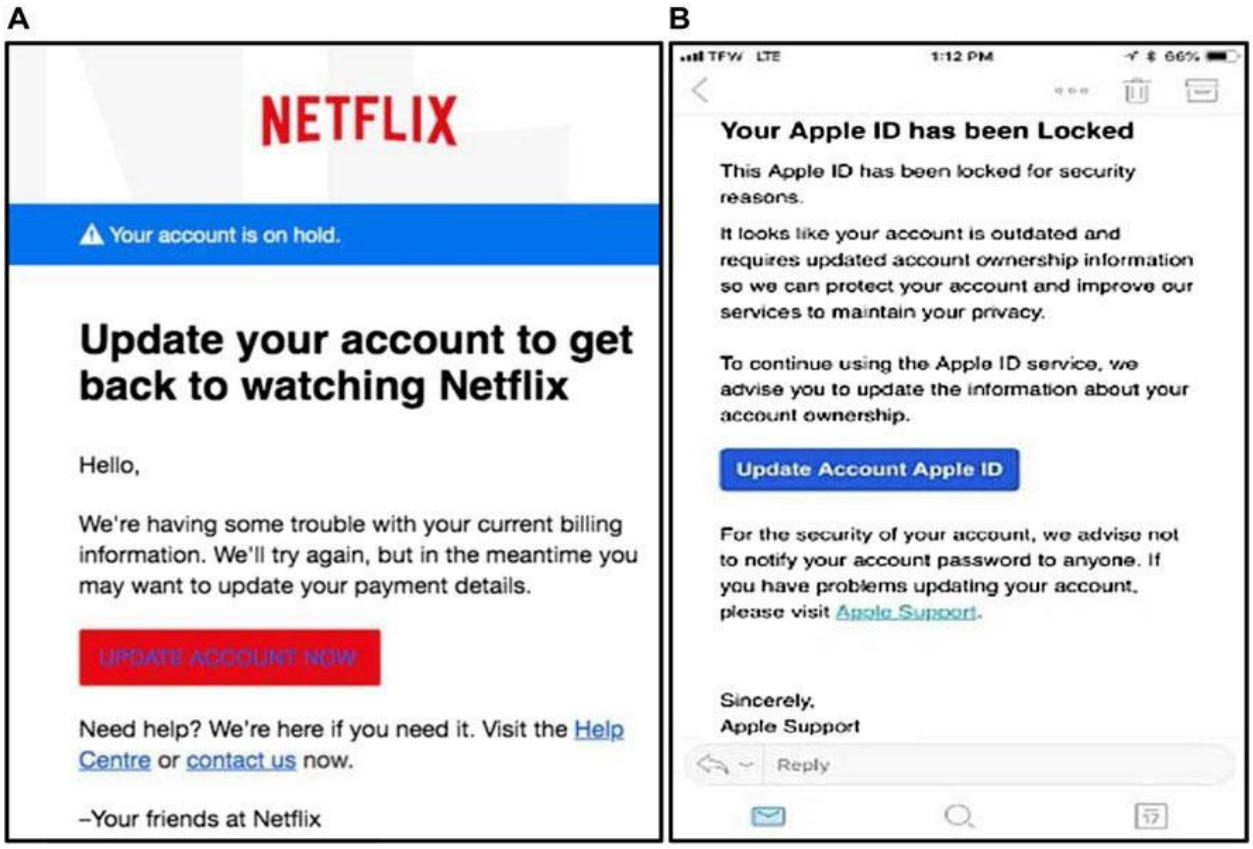
Figure 2 – A screenshot of a Phishing email



Source – **Alkhalil et al (2021)**

The phishing attack spotted at Akamai organisation by a security researcher in January 2019 is another classic example of a phishing attack. The attack masked wary URLs, beginning with "www.translate.google.com", which seems genuine to dupe users (Rhett, 2019). Another phishing scam took place when a user was asked to enter payment details to continue their Netflix account. It also redirected users to PayPal pages which looked genuine. Even though the bogus page was designed well, misspellings in the link and lack of HTTPS lock were major red flags (Keck, 2018). The "Federal Trade Commission (FTC)" received a phishing email as shown in the screenshot below (Figure 3A). It asks the user to update their payment method by clicking on the given link, showing that Netflix is having trouble with the billing details of the user (FTC, 2018).

Figure 3 – (A) Screenshot of a Netflix email scam (B) Screenshot of a fake Apple text



Source – Rhett, 2019; Keck, 2018

Figure 3B illustrates another example of a phishing attack which is even harder to detect as a fake text (Pompon et al, 2018). The text seems to be from Apple support asking for an update of the account by creating a sense of urgency to lure the user to respond. These days, phishing refers to being one of the most persistent cyber threats for all web users, despite their technical know-how and how careful they are. Such attacks may lead to extreme losses to the victims and getting more sophisticated. Stealing money is the first motivation for the attackers. But they can use sensitive information for various purposes like espionage in sensitive infrastructures. They constantly evolve over time with the emergence of technology and protective measures. This article is aimed to discuss phishing mechanisms, types of attacks, and protective measures.

1.2. Objectives

- To elaborate various phishing attacks and measures to protect sensitive data
- To discuss the overall process of phishing attacks
- To discuss challenges related to prevention of phishing attacks

1.3. Paper-organisation

In this paper, we will first discuss the working mechanism of phishing attacks as a novel evolution in cybercrime. Then, we will cover the types of phishing attacks, such as spear phishing, deceptive phishing, whaling, and pharming. Later on, we will discuss major causes of spear phishing, such as, spoofing, social media, technical issues, and human factors, and measures to mitigate such issues. Finally, we will conclude with various challenges and issues to prevent phishing attacks.

2. Phishing Mechanism – New Evolution in Cybercrime

Suppose a person checks his email and comes across a message from his bank. Though their bank has already sent a lot of emails before, this email is supposed to be suspicious. It threatens the customer to close their account if he fails to respond quickly. Such types of messages are called “phishing” or online identity theft. Along with stealing financial and personal data, phishers simply infect systems with viruses and convince people to get involved in money laundering. Phishing is mostly associated with emails that mimic or spoof credit card companies, banks, or ecommerce companies like eBay, Amazon, etc. They make these messages look genuine and lure victims to reveal their private data. Emails are just a part of this whole scenario. Here’s the overall phishing mechanism from start to end (Wilson, n.d.) –

- **Plan** – First of all, phishers choose businesses to target and strategize how to collect email addresses for their customers. They mostly use bulk emailing to collect information as spammers.
- **Setup** – After deciding the business to spoof and victims, phishers deliver messages and collect data with certain methods. They mostly use web pages and email addresses.
- **Attack** – It is the most common step. They simply send a spam message which seems to be from an authentic source.
- **Collect** – Phishers record the data entered in popup windows or web pages by the victims.
- **Initiate** – Once phishers gather information they need, they use the same for illegal purchases or any other fraudulent activity.

In order to initiate the next attack, the phisher determines the failures and success rate of the scam which is already done and starts the process again. Such types of scams make the most of security and software vulnerabilities on both server and client sides. Even the most advanced scams act as old-school con jobs (where a phisher pretends to be from a trustworthy and reliable source).

3. Categories of Phishing attacks

As per the attacker, there is a huge range of targets in social engineering attacks. They might be simple scam emails targeting anyone having a PayPal account. It is also supposed to be a targeted attack on an individual. An email is tailored as per the target and it has data that only a familiar one knows. Basically, this information is gathered when an attacker gains access to private data. Even the most careful recipients might become victims of this type of email. Around 97% of all phishing emails are used for ransomware attacks, according to PhishMe Research.

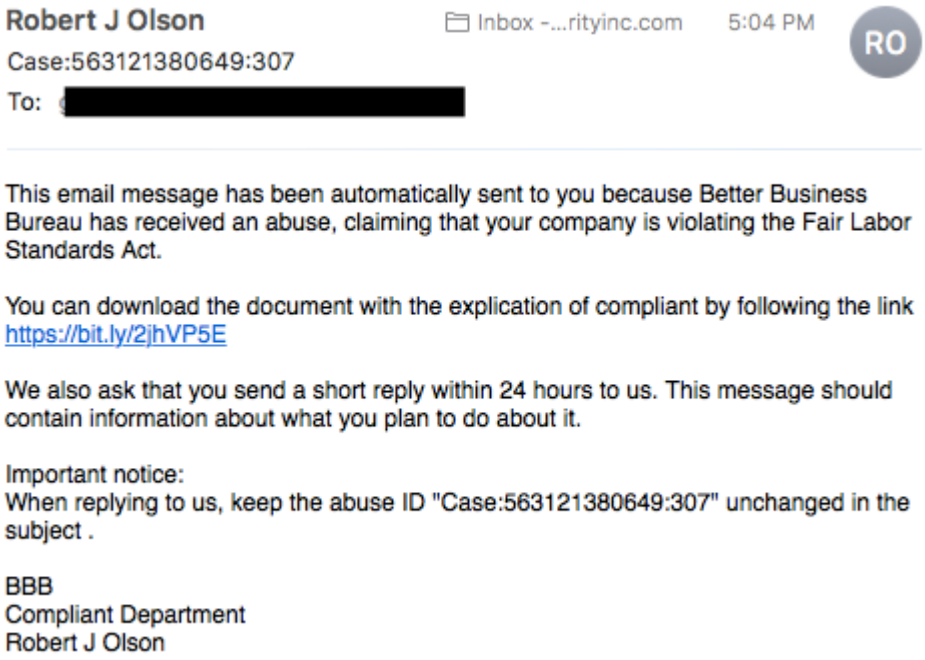
3.1. Deceptive Phishing

It is the most common phishing ploy. They impersonate an authentic company to steal personal data of the people or login details. They use threats through email along with a sense of urgency to frighten people and convince them to do what phishers want.

3.2. Spear Phishing

Fishing using a pole may bring a lot of items under the waterline, such as a piece of garbage, bottom feeder, a founder, etc. On the other side, one can target a specific fish with a spear. As the name suggests, spear phishing targets a specific kind of individual or group like a system administrator of a company. Figure 4 illustrates a screenshot of an email related to spear phishing. In this screenshot, the email requires a quick response from the recipient by clicking a download link.

Figure 4 – Screenshot of a Spear Phishing Email



Source – Trend Micro

3.3. Whaling

It is an even more targeted kind of phishing attempt that targets whales that are even bigger. Such attacks usually target a director, CEO, CFO, or anyone on a higher post in a company or an industry leader. It might mention that the company is going through a legal trouble and that the user has to click to get more info. That link redirects users to a page to provide critical information of the company like account numbers and tax ID.

3.4. Pharming

As users get more concerned over common phishing activities, some attackers drop the idea of baiting victims at all. Rather, they prefer pharming. This activity uses cache poisoning over the “Domain Name System (DNS)”, a naming scheme which is used by the internet to turn alphabetical names of the websites like www.microsoft.com to numerical IPs to locate and direct users to computer devices and services. A pharmer attacks a DNS server in a cache poisoning attack and it replaces an IP address related to the alphabetic name of the website. This way, attackers redirect visitors to a malicious portal. Even though the visitor enters the correct domain name, it still happens.

4. Major Causes of Spear Phishing

All phishing scams don’t use “spray and pray” techniques. Some depend more on personalised services because they would never succeed in other ways. This is how spear phishing works. Fraudsters tailor their spam emails with the name, position, work contact, and other details of the recipient to trick them to believe that the sender is a familiar party. The goal is still similar to deceptive phishing, i.e., to lure the victim into clicking on a spam link or attachment to steal their private data. Given the amount of data required to craft a tailor made attempt, it goes without saying that spear phishing is very common on social media platforms like LinkedIn where attackers craft a targeted mail with different data sources.

4.1. Social network connection

Malicious actors first find out who is working at a company they are targeting. They use social media accounts to investigate the overall structure of an organisation and find out whom they would want to target for their attacks.

4.2. Spoofing

In this scam, the call seems legitimate in the area code of the target. This technique is capable of lull targets into a disguised feeling of security.

4.3. Technology failure

When it comes to target company's employees, malicious actors may impersonate tech support of a target company with some technical jargon and allude to things like badging or speed issues to lure employees to hand over their data.

4.4. Human factors – Hitting the Human Weak Spot

Phishers usually deploy different techniques against specific targets. For example, malicious actors may use "mumble technique" to mutter the response to a question hoping that their answer will be suitable when it comes to target call centre agents or representatives.

5. Mitigating the Menace of Phishing Attacks

It takes a whole range of tools and techniques to prevent phishing by neutralising and identifying such kinds of attacks beforehand. Proper user education is paramount to spread awareness about phishing scams. In addition, anti-phishing tools, solutions and programs must be installed in company's systems and various security measures must be implemented to proactively prevent phishing while ensuring mitigation techniques for attacks that can breach security.

Protection from email phishing is an art more than science. It goes without saying that a huge range of advanced technologies could fail in blocking phishing attempts without proper awareness. However, creating a tailor made strategy on the basis of specific context is the most effective approach. For example, leading organisations may benefit from enterprise-level solutions for email security along with traditional email security programs which include best practices and user education along with on-going, formal training. Meanwhile, small companies may consider it more cost-effective to focus on best practices and employee awareness while saving on their software investments. One thing is sure that organisations will always be at risk of bearing serious financial and legal losses without proper mechanisms to prevent phishing attacks (PhishProtection, 2019).

Phishing scams are one of the most prevalent approaches of attack. They are very profitable methods used by cybercriminals as they target thousands of victims all year round. However, one can avoid phishing scams with proper prevention and detection due to the common nature of those attacks.

5.1. Detection Approaches

Nobody is safe from phishing attacks. These emails are usually well designed and only a trained eye can spot the fake one. There are still some ways to prevent such attacks as much as possible (Maroso, 2020).

5.1.1. **Sender's name** – One can easily spoof domain names and email addresses. Hence, it is important to look for spelling changes on suspicious emails in domain names. It is always recommended to double-check email even if they seem to be of a trusted source.

5.1.2. **Typos** – Phishers are usually not much concerned about their grammatical mistakes. Hence, spelling mistakes and typos are usually common in messages. These errors could be a red flag about the authenticity of the message.

5.1.3. **Tempting offers –** If an offer seems too good to be true, it must be! Fake rewards are used by phishing attackers to lure victims to take strict action.

5.2. Offensive Defence Approaches

5.2.1. **Avoid sharing sensitive data** – Any email asking for sensitive data about a company or individual is suspicious. For example, banks never ask for private data over SMS or email. If someone gets such an email or message, one should directly contact their bank to verify that.

5.2.2. **Sense of Urgency** – Attackers simply use urgency and scare tactics to lure victims to take quick action. Emails asking for sharing private data or making financial transactions are phishy.

5.2.3. **Hover over** – If there is no relation between the alt text and display text by hovering over the URLs, it is better not to click on it. Similarly, one should hover over attachments to verify the actual link, before downloading or clicking on it. It is recommended not to click on the link if the sender is unknown.

5.3. Correction Approaches

5.3.1. **Keep track of accounts regularly** – It is worth checking accounts to avoid any unknown changes regularly. Staying ahead of accounts and knowing what data is kept will make it easier to spot a phisher.

5.3.2. **Stay up-to-date** – Applications of devices are more vulnerable to attacks without proper update. It is recommended to check for updates and keep antivirus up-to-date.

5.3.3. **Call out when in doubt** – It is worth calling the cyber team or manager in case of security of work, data or device which has been compromised.

5.4. Human Approaches to Phishing Defence

5.4.1. **No Auto-fill service** – No doubt, password autofill is an added convenience for the users to avoid the hassle of typing passwords again and again. But phishers are good at platforms for phishing attacks. If "save password" pops up just on any website, it is worth it to skip it.

5.4.2. **2-Factor Authentication** – It is worth using the latest security measures from legitimate sources. 2-factor authentication is a commonplace these days to secure financial and sensitive data from unauthorised access.

5.4.3. **Google Drive** – If the document or attachment from an unknown sensor is supposed to be dubious or suspicious, it is better to upload the same on Google Drive. It would transform a document into HTML or image, which would help avoid installing malware on the device.

5.4.4. **Anti-phishing solutions** – The alarming rise in phishing cases is one of the major issues these days. Every corporate employee, businessman, and online user is under the radar of phishers all the time. Anti-phishing solutions are recommended to avoid falling prey to phishers.

5.5. Incentivise Reporting

It goes without saying that email is a common and widespread communication tool on the web but it is also worth noting that users are plagued by phishing emails and spam. As reported by Kaspersky Lab, around 50.37% unwanted emails have been detected in email traffic in 2020 (Kulikova, 2020). The spam abuses precious network resources and users' time. Even worse, phishing mails steal sensitive and private data of the users and compromise companies in every sector and government systems (Gangavarapu et al, 2020; Ho et al, 2019). According to the FBI, over $1.8 billion had been lost to phishing emails in 2020. Hence, email users must be secured from phishing emails.

Effective mitigation would be recommended to address issues at human and technical levels as phishing emails exploit weaknesses of humans (Khonji et al, 2013; Park et al, 2014). Machine learning is widely used to detect phishing emails but attackers may bypass it (Gangavarapu et al, 2020, Gupta et al, 2018, Sur, 2018). Users are more vulnerable and they should be the strong link to avoid phishing attacks (Das et al, 2019). Training people to improve their security hygiene is the most common strategy (Pattinson et al, 2012; Kumaraguru et al, 2007; Harrison et al, 2016; Caputo et al, 2013). They should incentivize reporting in case of any suspicious activity or email to security providers (Kwak et al, 2020). Detection can be made easier with reporting and security providers can alert other potential victims before the spread of attack. A convenient security mechanism is provided by Cofense Reporter, an email security provider, to make reporting easier. Another challenge is that most users don't report such emails despite having various benefits (Swinhoe, 2019; Verizon, 2021; Stembert et al, 2015).

6. Challenges

One of the major challenges with phishing is that attackers are constantly on the lookout for creative and emerging ways to trick users into believing that they are dealing with a legitimate email or website. Phishers have been more advanced at forging websites to look similar to the target location, even with graphics and logos in the phishing mails to look more authentic. These advanced and cutting-edge technologies are getting more dangerous for users as attacks use private data that is easy to find on public domain to produce convincing and plausible attacks. Social engineering is one of the classic examples of phishing attacks. They develop a mind-set behind their emails which trigger greed, trust, or feeling of urgency. Even more aware and cautious users might fall prey to such attacks due to legitimate feel and look of spoofed sites.

All these methods fall under spear phishing where specific victims are directly targeted with some common things. Some data about the victims is needed for spear phishing, such as bank details, workplace, and recent shopping history for a targeted attack. They

simply comb blogs, profiles, and other websites to get this data. Some attacks also use malware like trojans or worms into emails while sending which compromise the security of the system directly and create the next tool to choose victims and deploy attacks. Phishing has been more complex and is getting harder to detect for cyber security experts. With the rise in online security measures, phishing is also getting a step ahead. Attackers have developed new methods to make it harder for anyone to differentiate phishing activity.

Hence, incorporating proper anti-phishing solutions dedicated to email servers like Gmail, Outlook, etc. to protect against such attacks on a large scale. Even common and inexperienced people still need basic protection from phishing risks. Servers must have training systems embedded in their email services and users must be more aware of how phishing works and what it can do with their data. It will lead to an educated society where it would be more difficult to unleash attacks.

7. Conclusion

Phishing has become the bigger threat than ever to the users as attackers have become more upgraded over time and it is even more complex to detect. Cyber criminals are also very hard to catch. Hence, there is a need to use a filtration system that can sort out as many phishing emails as possible to keep them from reaching the user, reducing the risk of getting phished. The UI of email services should be designed so well that it could alert the users when they get suspicious email. The users can practise avoiding phishing activity with engagement from training and educational games. It is very important to stay ahead with automated defences and Machine Learning techniques to control phishing.

References

1. Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behaviour*, *29*(3), 706-714.
2. Gupta, P., Srinivasan, B., Balasubramaniyan, V., & Ahamad, M. (2015, February). Phoneypot: Data-driven Understanding of Telephony Threats. In *NDSS* (Vol. 107, p. 108).
3. Ovelgönne, M., Dumitras¸, T., Prakash, B. A., Subrahmanian, V. S., and Wang, B. (2017). Understanding the relationship between human behaviour and susceptibility to cyber attacks. *ACM Trans. Intell. Syst. Technol*. 8, 1–25. doi:10.1080/00207284.1985.11491413.
4. Iuga, C., Nurse, J. R. C., and Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Hum. Cent. Comput. Inf. Sci.* 6, 8. doi:10.1186/ s13673-016-0065-2.
5. Crane, C. (2021). The Dirty Dozen: The 12 Most Costly Phishing Attack Examples. *Hashed Out*. Retrieved 3 May 2022, from https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/#:%7E:text=At%20some%20level%2C%20everyone%20is%20susceptible%20to%20phishing,outright%20trick%20you%20into%20performing%20a%20particular%20task.
6. Business Email Compromise (BEC) | Barracuda Networks. (2020). Retrieved 3 May 2022, from https://www.barracuda.com/glossary/business-email-compromise.
7. Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Am. Soc. Inf. Sci. 59* (4), 662–674. doi:10.1002/asi.20779.
8. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*, 563060.
9. Rhett, J. (2019). Don't fall for this new Google translate phishing attack. Available at: https://www.gizmodo.co.uk/2019/02/dont-fall-for-this-new-google-translate-phishing-attack/.
10. Keck, C. (2018). FTC warns of sketchy Netflix phishing scam asking for payment details. Available at: https://gizmodo.com/ftc-warns-of-sketchy-netflix-phishing-scam-asking-for-p-1831372416.
11. FTC (2018). Netflix scam email. Available at: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing.
12. Pompon, A. R., Walkowski, D., and Boddy, S. (2018). *Phishing and Fraud Report attacks peak during the holidays. US.*
13. Wilson, T.V. HowStuffWorks, Tech, Computer, Security, & Security. How Phishing Works. Retrieved 5 May 2022, from https://computer.howstuffworks.com/phishing.htm.
14. Trend Micro. What Are the Different Types of Phishing?. Retrieved from https://www.trendmicro.com/en_in/what-is/phishing/types-of-phishing.html.
15. Bisson, D. (2021). 6 Common Phishing Attacks and How to Protect Against Them. *Tripwire*. Retrieved 5 May 2022, from https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/.
16. 17 Phishing Prevention Tips - Prevent Phishing Attacks, Scams & Email Threats | Phishprotection.com. (2019). Retrieved 5 May 2022, from https://www.phishprotection.com/content/phishing-prevention/.

17. Maroso, L. (2020). 10 Top Tips to Detect Phishing Scams. *Security HQ*. Retrieved 5 May 2022, from https://www.securityhq.com/blog/top-tips-to-detect-phishing-scams/.
18. Prevent Phishing Attacks to Secure Your Organization. *Threatcop*. (2022). Retrieved 5 May 2022, from https://threatcop.com/blog/prevent-phishing-attacks/.
19. Kulikova, T. (2020). Spam and phishing in 2020. Retrieved 5 May 2022, from https://securelist.com/spam-and-phishing-in-2020/100512/.
20. Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review*, *53*(7), 5019-5081.
21. Ho, G., Cidon, A., Gavish, L., Schweighauser, M., Paxson, V., Savage, S., ... & Wagner, D. (2019). Detecting and characterizing lateral phishing at scale. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 1273-1290).
22. Federal Bureau of Investigation, 2021. "Internet crime report. 2021," Federal Bureau of Investigation, Washington, DC, USA.
23. Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091-2121.
24. Park, G., Stuart, L. M., Taylor, J. M., & Raskin, V. (2014, October). Comparing machine and human ability to detect phishing emails. In *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 2322-2327). IEEE.
25. Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267.
26. Sur, C. (2018). Ensemble one-vs-all learning technique with emphatic & rehearsal training for phishing email classification using psychology. *Journal of Experimental & Theoretical Artificial Intelligence*, *30*(6), 733-762.
27. Das, A., Baki, S., El Aassal, A., Verma, R., & Dunbar, A. (2019). SoK: a comprehensive reexamination of phishing research from the security perspective. *IEEE Communications Surveys & Tutorials*, *22*(1), 671-708.
28. Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?. *Information Management & Computer Security*.
29. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, April). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 905-914).
30. Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*.
31. Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28-38.
32. Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails?. *Telematics and Informatics*, *48*, 101343.
33. Cofense. The Easiest Way to Report Phishing. Retrieved from https://cofense.com/product-services/reporter/.
34. Swinhoe, D. (2019). Why businesses don't report cybercrimes to law enforcement. *CSO India*. Retrieved 5 May 2022, from https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html
35. Verizon (2021). DBIR: 2021 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/
36. Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015, September). A study of preventing email (spear) phishing by enabling human intelligence. In *2015 European intelligence and security informatics conference* (pp. 113-120). IEEE.