A PERSPECTIVE REVIEW ON CYBER SECURITY PHISHING AND ITS PREVENTION

T. Shylaja, Assistant professor, Department of computer science, Sardar Raja Arts and Science College, Vadakkankulam, Tirunelveli, Tamil Nadu.India.

ABSTRACT

The constant increase in cyberthreats poses a serious threat to both personal privacy and international security. Phishing assaults continue to be one of the most harmful types of cybercrime among them. This paper offers a thorough analysis of phishing assaults, including their history, methods, effects, and defenses. Phishing assaults can now be carried out using increasingly complex techniques, such as spear phishing, whaling, clone phishing, vishing, smishing, and search engine phishing, in addition to the traditional email phishing. The study demonstrates the significant financial and non-financial repercussions of these attacks by thoroughly examining a large number of case studies. The review also provides insight into the state-of-the-art detection and prevention methods being used to lessen the dangers of phishing. Amid the growing weapons race between cybersecurity experts and cybercriminals The paper emphasizes the need for ongoing research and technological breakthroughs while highlighting emerging trends and problems. This review's goal is to give scholars, cybersecurity experts, and legislators a useful resource that will help them understand and deal with the difficulties presented by phishing attacks.

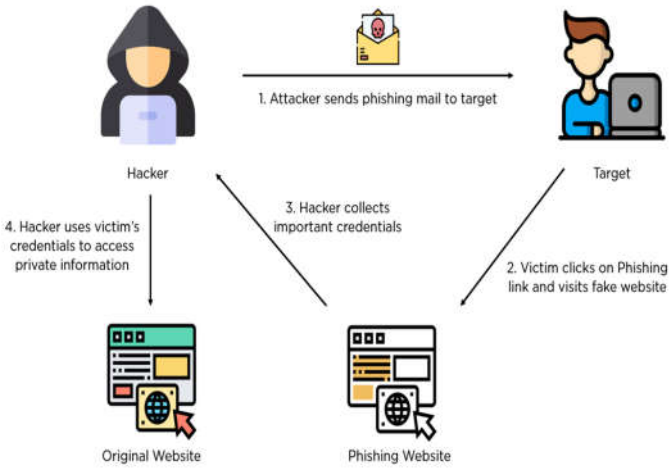
KEYWORDS: ***Phishing attacks, cybersecurity, spear phishing, whaling, clone phishing, cyber threats, detection techniques, cybersecurity trends, future challenges, impact analysis, financial consequences, privacy concerns***

1. INTRODUCTION

Phishing is the practice of trying to pass off personal information, including credit card numbers, usernames, and passwords, as a reliable source via an electronic message. The public is frequently tricked by communications posing as from well-known social media platforms, auction websites, online payment systems, or IT administrators. Links to malicious websites may be included in phishing emails.

One type of social engineering is phishing. Phishing is primarily employed in email hacking, when the hacker sends a link via email to the user of, say, bank account information or other personal information. The user then clicks on the link and fills out all the information, and the hacker receives all of the information.

Given the rapid pace of technological advancement and the increasing reliance on digital communication, it is crucial to address phishing threats with a combination of awareness, education, and technological solutions. This paper aims to explore the mechanisms of phishing attacks, their various forms, and the preventive measures that can be implemented to minimize their impact. By understanding the tactics used by attackers and adopting proactive defense strategies, it is possible to strengthen resilience against this ever-evolving cyber threat.



Phishing is explained step-by-step:
1. Attacker sends an email to victim.
2. Victim clicks on the email and goes to phishing website.
3. Attacker collects victim's credentials.
4. Attacker uses victim's credentials to access a website

Phishing begins with an email or another form of communication intended to facilitate an attack on the victim. The message is crafted to appear as if it originates from a reliable source. If it deceives the victim, the victim is giving personal information to a spam site. At times, malware is also being downloaded to the target's computer.

2.TYPES OF PHISHING ATTACK

Phishing is a form of cyberattack where attackers use deceptive techniques to trick individuals into sharing sensitive information, such as passwords, credit card numbers, or other personal data. These attacks are often carried out through emails, messages, or fraudulent websites that mimic legitimate entities.

2.1. Spear Phishing:

A wirelessbased Intrusion Detection Prevention System examines the traffic of a wireless netwok by evaluating wireless protocol activities and taking necessary measures. It identifies the unauth orized use of wireless local area networks. It is unable to detect suspicious behavior in the applic ation layer, transport layer,and protocol actions.It is positioned within a specific range that allows the organization to oversee the wireless network.

2.2. Whaling:

Whaling is one of the types of phishing, in this type of phishing the attacker aims at a wealthy and powerful status of the victim or user; the attacker takes out all the information of the victim using different medium such as social media accounts and then attacks the victim. The victims of this type of attack are also called as "Whales" or "Big Phish". Whale phishing involves the same tactics used in Spear Phishing.

2.3. Pharming:

Pharming, is a type of cyberattack that redirects users from legitimate websites to fraudulent or malicious websites without their knowledge. This redirection is achieved by manipulating the Domain Name System (DNS) or compromising the user's device, often through malware or DNS cache poisoning. Unlike phishing, pharming does not rely on the user clicking on malicious links; instead, it operates silently in the background, tricking users even when they enter the correct website address.

2.4. Smishing:

Smishing, short for SMS phishing, is a cyber scam variant that employs misleading text messages to illicitly obtain personal information. Scammers posing as trustworthy entities, like banks or popular brands, send messages to induce panic or excitement. They entice victims to divulge sensitive information or click on malicious links, using urgency or appealing deals as bait. It is a deceptive tactic leveraging social engineering, where impulsive reactions are exploited. Awareness and vigilance are crucial defenses against such attacks.

2.5. Vishing:

Vishing uses phone calls instead of emails. The attacker might leave a voice message purportedly from a bank or other service provider asking the recipient to call a number. When the victim call back, they are prompted to enter their account number or other personal information

2.6. Clone Phishing:

Pharming redirects traffic from an authentic website to a false website, in contrast to other phishing strategies that call for a lure. This method may be used to attack a DNS server software vulnerability or to modify the hosts file on the victim's machine.

2.7. Snow-shoeing

It is a term used to describe a spamming technique where attackers distribute their malicious activities across a wide range of IP addresses and domains to avoid detection by spam filters or cybersecurity systems. This strategy mimics the distribution of weight in actual snowshoeing to prevent sinking into the snow—in this case, avoiding getting flagged**.**

2.9.Deceptive Phishing:

This is a most common type of phishing, in this type the attackers impersonate a legitimate company and try to steal people's personal information or their login passwords. And then they blackmail the users to do as the hacker wants

2.10.Email Phishing

The most common kind of phishing is when cybercriminals send out mass emails pretending to be trustworthy organizations, such as banks or internet service providers, in an attempt to trick recipients into disclosing personal information or clicking on dangerous links. These emails frequently create a sense of urgency to get the recipient to act right away. Cybercriminals try to fool internet users into disclosing private and sensitive information that could be used to perpetrate fraud by using hashing, a form of online fraud. Although emails are the most popular way for phishing to occur, it can also happen through phone calls, texts, or social media. Scammers use email phishing to try to win over the recipient's trust by posing as trustworthy companies or people.

2.11.HTTPS Phishing

HTTPS (hypertext transfer protocol secure) phishing is a URL-based attack that attempts to trick users into clicking a seemingly safe link. HTTPS is the standard protocol for traffic encryption between browsers and websites and requires TSL/SSL certificates to be enabled. In the past, browsers could detect sites that did not have HTTPS enabled as the first line of protection against cybercrime**.**

2.12.Evil Twin Phishing

An evil twin phishing attack creates an unsecured Wi-Fi hotspot access point that baits unsuspecting users into connecting. Once connected, all inbound and outbound data can be intercepted, including personal data or financial information. Hackers can also prompt the users to visit a fake website portal in hopes the user will provide valuable authentication details.Evil twin phishing attacks are most common in public areas with free Wi-Fi, like coffee shops, libraries, airports, or hotels. The best way to prevent becoming an evil twin phishing target is to use a virtual private network (VPN) while using public Wi-Fi.

2.13.Business Email Compromise (BEC)

A business email compromise is similar to whaling, but instead of attempting to trick the executive, it impersonates them. Criminals will impersonate or obtain access to an executive email account with decision-making authority and send internal requests to lower-level employees.

In 2014, Omaha-based agriculture company Scoular became a victim of a BEC attack. The corporate controller, Keith McMurtry, received an email from his CEO asking for an immediate wire transfer to acquire a Chinese-based company. The email detailed a lawyer who would be in charge of the transaction, and McMurtry wired in total $17.2 million to an offshore account. However, the email was ultimately fraudulent, containing fake phone numbers and email addresses.

2.14 Watering Hole Phishing

Watering hole phishing is a tactic that targets one particular company or group of people by infecting a third-party website they frequently visit. The attackers find and exploit a vulnerability on the website, infect the site with malware, and then bait users by sending emails directing them to the site.Although this type of attack is less common than the others, once the hackers infect a single user, they can gain access to the entire network and system. Additional site visitors can also become victims, even if they have no relation to the main targeted group.

3.PREVENTION OF PHISHING ATTACK

As technology evolves, phishing attacks are expected to adapt and adopt new strategies to exploit vulnerabilities. Understanding the future trends and challenges associated with phishing is crucial for staying ahead in the ongoing battle against cyber threats. Here are some anticipated trends and challenges:

3.1. Recognize the signs of a phishing scheme

Although new phishing attack techniques are constantly being created, they all have certain characteristics that you can spot if you know what to look for. Numerous websites are available to teach you about the most recent phishing assaults and their distinguishing characteristics. Your chances of preventing a possible attack increase with the speed at which you learn about the most recent attack techniques and communicate them to your users through frequent security awareness training.

3.2 Get free anti-phishing add-ons

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there’s no reason not to have this installed on every device in your organization.

3.3. Provide training on security awareness

Because phishing assaults cannot be stopped by technical means alone, security awareness training is essential. Employees should be empowered to recognize and report questionable activities as well as learn about the dangers of phishing. Organizations can evaluate their own risk and increase staff resilience by using simulated phishing campaigns to further reinforce the training. When staff members click on phishing-simulation emails, it's critical to remind them of the dangers and how to report any questionable emails. Organizations can concentrate on enhancing training, adding more phishing defenses, and upgrading security measures by tracking the outcomes on improving their security measures, strengthening training, and implementing additional defenses for phishing protection.

3.3. Guard against spam

In this type of prevention method, the attacker comes from unrecognized senders. They ask you for confirmation of personal or financial information over the internet and make requests for giving your information.

3.4. Communicate personal information only via phone or secure web sites

In this type of phishing prevention, the user should be aware of while conducting online transactions, look for the secured sign on the browser status bar or” https.” URL where the “s” stands for “secure” rather than’ http.

3.5.Rotate passwords regularly

If you've got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

3.6. Implement anti-phishing tools

Use anti-phishing tools and technologies that can detect and block fraudulent websites and emails. Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

3.7. Don't give your information to an unsecured site

If the URL of the website doesn't start with "https", or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Sites without security certificates may not be intended for phishing scams, but it's better to be safe than sorry.

3.8. Don't be tempted by those pop-ups

Pop-ups aren't just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don't be tempted to click! Occasionally pop-ups will try and deceive you with where the "Close" button is, so always try and look for an "x" in one of the corners.

3.9.Implement anti-phishing tools

Use anti-phishing tools and technologies that can detect and block fraudulent websites and emails.

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

CONCLUSION

After discussing the primary phishing methods and a few prevention and detection strategies, it is determined that, in terms of a person's day, the best way to achieve good security is to make sure the user is aware of the methods and how to avoid falling for the phishing trick.There are numerous ways to initiate a phishing attack. In order for the client to take the required precautions against phishing assaults in the future, the study here focuses on creating detection and prevention measures. This paper examines a variety of assault types as well as how to detect and prevent them. Comparing different phishing attack protection tools will be the main focus in the future.

REFERENCES

1. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629-3654.

2. Huang, H., Zhong, S., & Tan, J. (2009, August). Browser-side counter measures for deceptive phishing attack. In 2009 Fifth International Conference on Information Assurance and Security (pp. 352-355). IEEE

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11.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.