Navigating Phishing Attacks

Berline Najacque

Old Dominion University

Windows System Management and Security

Research Paper

Malik A Gladden

April 18, 2024

Navigating Phishing Attacks

Introduction

Phishing attacks are the prevalent form of cybercrime in the digital landscape that exploits human vulnerabilities. These attacks are not just limited to one particular system structure; all messages, applications, systems, and websites are vulnerable to such attacks. For instance, Microsoft has a proactive protocol to protect its users from phishing attacks. Still, human vulnerability puts the whole network at potential risk when individuals install malware onto their systems and give up sensitive information (Alsharnouby et al., 2015). Cybercriminals use deceiving measures and methods to successfully hack the users and their systems, exposing and divulging the users' sensitive information to the attackers' source. This paper addresses the prime function of social engineering and phishing, how Microsoft systems protect vulnerable people exposed to phishing attacks, and the measures Microsoft takes to prevent them from falling victim to a phishing attack.

Overview of the Research

Phishing attacks pose a severe concern to vulnerable individuals and their information as cybercriminals exploit social engineering techniques to deceive digital users and gain unauthorized access to sensitive information. These attacks usually occur via phishing emails where attackers pretend to be legitimate entities from Microsoft Inc. The most common form of phishing attacks is phishing emails due to human error vulnerabilities. The recipient of such emails usually receives a harmful link or attachment in a typical phishing email, which downloads the malware into the system with a simple click. The malware downloaded into the system may take several forms, including identity theft, system sabotage, ransomware, or data

theft, allowing the attacker to steal banking credentials, impersonate someone, and compromise personal data.

Although many people from the digital landscape are now aware of this method of cybercrime, there is still a good percentage of vulnerable individuals working in many companies who fall prey to this method of fraud. Such defrauding attacks aim to deceive users of the digital spaces by masquerading as government agencies, banks, companies, or other legitimate entities. Through social engineering techniques, attackers manipulate users by divulging sensitive data because of the human inability to identify malicious sources. Thus, the common denominator in all phishing attacks to execute harmful actions is human vulnerability and inability to exploit human errors within the organization (Elamathi & Aruna, 2023).

While phishing attacks and their harmful actions are not just exclusive to Microsoft's system structure, the research focuses on them for simplicity as Microsoft has implemented proactive protocols to protect its network and its users from phishing attacks. The corporation still continuously works to educate its users about potential risks that come with phishing emails and enhance its security features to protect its network and users from digital threats. However, the success of these attacks still hinges on user behavior virtually as the attackers sabotage the system due to human vulnerability. Microsoft uses sophisticated cybersecurity systems such as Multi-Factor Authentication to add an extra layer of security to its network and educate users about recognizing phishing attacks through suspicious links or attachments and phishing emails. For user vigilance, Microsoft uses advanced filters to block down suspicious emails that could harm the network and encourage users to report suspicious activity promptly. However, such measures and systems cannot fully protect against human error and vulnerability (Rains, 2020).

Frameworks and Methodology

The most common form of methodology through which phishing attacks occur in the digital space is phishing email. Phishing emails are a popular way for attackers to subjugate human vulnerabilities due to organizational errors. This form of phishing explains the overall framework through which attackers send a malicious link or attachment to the attack recipient. The recipient receives a downloadable file with a safe bit of information, apparently from a legitimate entity. The critical factor of the phishing framework results in human error succeeding the manipulation game and clicking on the malicious link that exposes the attacker to the user's sensitive information. Once the prey clicks on the link or opens the attachment provided in the email, a phishing attack downloads the malware onto the system involved and launches the attack on the data present in the computer system or network. Oftentimes, the malware downloaded into the vulnerable human's system is used to steal information, sabotage the system, or ransomware.

Therefore, the email is the famous textbook example of what a phishing attack looks like and its methodology to defraud individuals or organizations with malicious intent. With the advancements in technology and awareness about the threats posed to users in the digital space, companies, and society have gained knowledge and training to keep themselves protected from such attacks, but a well-educated person may also fall victim to such attacks upon clicking the link (Sharma & Bashir, 2020). Phishing attacks launch a framework of three main types of damage involving data theft, data encryption, and monetary theft that become successfully activated and are equally harmful to the organizations as these attacks are to the individuals. In order to provide damage control that occurs due to phishing attacks, proper procedures are

followed to determine the aggression based on the variant types of phishing attacks that exploit the systems.

Data theft is one of the standard methods of successful phishing attacks that damage the whole system or steal important information from the compromised system. In this attack, the attackers adopt a methodology to steal essential data or information in the user's computer system or the network system with which the user's system is connected. Resultantly, the user lost their data because the phishing attack has stolen the sensitive information from the system. For instance, an organization keeping a record of an individual's identity, educational background, job prospects, professional opportunities, and banking credentials may lead to the organization's data being extorted to the dark web for sale.

The following form of damage that the successful methodology of phishing attacks may cause is data encryption. This phishing methodology is often called ransomware, as it encrypts crucial files on the system. The attackers then ask the recipients to pay the presented fee if they want to return the restored files, which leads to losing access to the system data and information files. This methodology causes big business disruption for individuals and organizations, depending on how long it takes to restore the damage caused to users' systems or networks.

Lastly, the methodology of damage caused by phishing attacks is monetary theft, which occurs when attackers attack the system to steal data. This occurs because data theft provides economic gain and benefits for those who triggered the attack to gain access to monetary data. This methodology allows hackers or attackers to modify any organization's invoices according to their nefarious designs if the attack succeeds. Attackers use the obtained information to create fake invoices to cash them for their malicious intents or sell their invoices or monetary

information to those who wish to cash those invoices on their behalf, exploiting the victim's rights and playing with the information illegitimately.

In Microsoft systems, there is a pre-built-in protection to prevent the success of phishing attacks. These attacks create a barrier between every user's caution and human error that relies on phishing methods. Microsoft offers these systems as an automatic protection setup that pre-enables the systems when the users log in to their Microsoft accounts. In addition, Microsoft uses various levels of scans to prevent any suspicious or malicious activity that may slip into the systems by the user. Microsoft Inc. occasionally grows its protection policy with the best security ways. For instance, Microsoft scans emails being sent to the receiver or user of the system and matches the sender's information and the emails' content for a couple of resources.

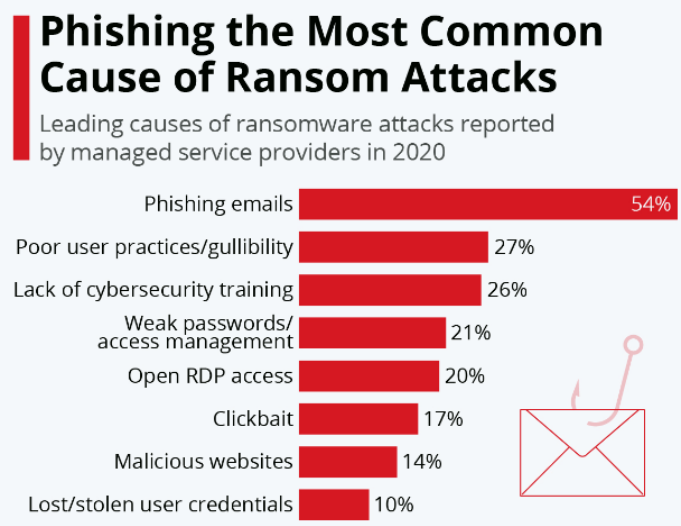
Tools/ Resources/ Results

The tools or resources commonly looked at are the information of the sender who sends the initial email to prevent phishing attacks. The sender's information and the initials are scanned so that Microsoft can detect any malicious activity, and the user can look at the content the email holds and the details of who the sender is. However, sometimes, attackers create an email with slight spelling changes to blend the malicious email with regular email. Microsoft's pre-built-in protection setup carefully scans the details and alerts the user that he has yet to send or receive an email from that address. If Microsoft detects any suspicious activity, it alerts users to review the resources to prevent phishing attacks.

The second resource that is scanned by Microsoft to prevent phishing attacks prior to the user accessing the email is the contents of the email being received by the user. If the sent email has suspicious elements or content, an alert is issued to the user, prompting a similar effect to the

scan of the sender's email initials. In addition, Microsoft might hide the email and its content altogether if any non-official link or downloadable attachment is found to help the system prevent an accidental attack on the user's email and other systems (Adil et al., 2020).

Phishing attacks are commonly present in emails through a malicious code, link, or downloadable attachment presented to the user as a safe and official resource but impersonated by an illegal entity. Cybercriminals look for human vulnerabilities and weak points to deploy a phishing attack on the vulnerable system of the user, which, when activated, causes detrimental harm to the system as well as individual personal data (Alsharnouby et al., 2015). Depending on the hacked system, the harm may result in ransomware, money theft, and identity theft.



The figure above describes how phishing emails, improper user behaviors, and a lack of cybersecurity training are the primary factors contributing to ransomware attacks. This highlights the crucial role of end-user education in ensuring IT security.

Conclusion

Though Microsoft has built-in setups and measures to keep its systems safe from potential attacks and deploys multiple scans on different areas to prevent human error, awareness and continuing growing knowledge help individuals look further to keep their systems and information safe from potential phishing attacks. Microsoft system incorporates pre-built-in protections to prevent accidental or planned phishing attacks as these protections act as barriers between the success of the successful attack and the human error. However, these systems are not immune to phishing attacks despite Microsoft focusing on and enhancing its security measures to safeguard users from falling victim. Microsoft explores anti-phishing schemes from time to time with the best of its researchers to analyze potential phishing attacks to improve its security and integrity.

References

Adil, M., Khan, R., & Ghani, M. A. N. U. (2020). Preventive techniques of phishing attacks in networks. *2020 3rd International Conference on Advancements in Computational Sciences (ICACS)*, 1–8.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82.

Elamathi, M. U., & Aruna, M. A. (2023). An effective secure mechanism for phishing attacks using machine learning approach. *Journal of Pharmaceutical Negative Results*, 27242732.

Richter, F. (2021, July 6). *Phishing the Most Common Cause of Ransom Attacks*. Statista Daily Data. https://www.statista.com/chart/25247/most-common-causes-of-ransomware-attacks/

Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd.

Sharma, T., & Bashir, M. (2020). An analysis of phishing emails and how the human vulnerabilities are exploited. *Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity, July 16–20, 2020, USA*, 49–55.