Phishing Attacks And User Awarness: A Study On Threats, Impact And Prevention Stratergies

Ishan Dhangar[1], Akansha Dubey[2]
[1]Dept of Mathematics
[2]Asst. Prof. Dept of Mathematics
[1, 2] Shri Rawatpura Sarkar University, Chhattisgarh

Abstract- *The growing pace of digital technology has changed the face of modern society because digital technology makes communication, banking, education, and performing other tasks easier and faster. However, due to the rapid development in digital technology, the threat of cyber security risks to individuals and organizations has also escalated. Among the numerous cyber security threats, phishing threats are one of the most dangerous threats on the internet. Phishing threats aim at fooling users into entering confidential information such as passwords, bank accounts, and other data in the belief that they are interacting with a trusted institution. As they target human behavior rather than technology, phishing threats are impressively effective. The purpose of this research paper is to explore the nature, types, methodologies, effects, and need for user awareness when it comes to phishing threats in cyber security. The conclusion drawn from this research work states that user awareness can play an important part in mitigating threats related to phishing security along with other security measures.*

I. INTRODUCTION

In the modern technology age, the internet has become an integral part of our daily lives. People use the internet for communication, shopping, banking, education, entertainment, and business purposes. The internet has increased the efficacy of services but also increased the vulnerability to cyber threats. Cyber security has emerged as an area of concern for people, organizations, as well as the government. The increasing incidents of cyber attacks, as well as the rising sophistication in techniques by cyber criminals, have made cyber security a prominent issue.

A common technique used for a cyber attack is phishing. Phishing is a type of cyber attack that aims at tricking a person into revealing confidential information. The technique usually involves social engineering and uses psychological effects on a person rather than depending on technology, such as a vulnerability in a computer system, for a cyber attack to happen. Phishing can involve email, social media, and even a phone call, depending on the method used by the attacker.

Despite the development of various cyber security tools, phishing still fares successfully because of a lack of awareness among users. Some persons are not skilled enough to differentiate between a phishing attack and a genuine message, and this is why the user falls prey to it. This research, based on some study, intends to investigate how phishing and user awareness can be a tool for cyber security. The case study of how, with the help of phishing and its prevention methods, a user-aware group of persons can avoid cyber security threats is what this research aspires for.

II. WHAT DOES PHISHING MEAN?

Phishing could be regarded as a type of cyber-attack that involves the use of deceptive communication. This type of attack involves the use of a deceptive communication process that seeks to deceive the user. This process usually involves the attacker acting as a trusted organization such as a bank or a reputable business. This attack usually seeks to obtain the confidential data of the user such as login details and financial data. This term phishing can also be referred to as fishing since it involves the use of a bait.

The attacker does not have a problem with the process. The reason being that the process comprises a single operation involving the designing of a mimic page that resembles a genuine page. Secondly, the attacker sends the page to his targets, which might be social, mail, or text. Thirdly, the victim clicks on the page, and this aids the attacker in hacking all the details that have been entered.

Among the risks associated with phishing attacks is the fact that it can easily be carried out. Note that even in the absence of technical expertise, harm can be inflicted. The single biggest factor in determining the success that can be attained in phishing options lies in behavior.

III. TYPES OF PHISHING ATTACK

Phishing attacks may be classified according to the method employed and the target of attack. Techniques applied by the different attacks vary.

3.1 Email Phishing

Email phishing represents the most typical form of phishing. This involves the hacker sending deceptive emails. The emails seem like they are coming from reputable organizations. They comprise urgent notifications like warnings about accounts being due for payment. The emails prompt the recipient to click on the link or download an attachment.

3.2 Spear Phishing

Spear phishing can be performed on particular individuals or organizations. The attacker gathers information about the target and designs attacks accordingly. This makes spear phishing more hazardous compared to phishing because of its targeted attacks.

3.3Smishing

Smishing can be defined as phishing attacks that target recipients through text messages. Such messages may include trick messages, verification messages, and alerts. Smishing targets mobile phone users who may have smaller screen space and fewer chances to verify.

3.4Vishing

In the case of vishing, the hackers use voice calls. They pretend to be client service representatives or government officials. The victims are convinced to give the hackers private details through the use of the phone. Vishing mainly targets people who lack knowledge about technology.

3.5 Website phishing

In the case of website phishing, the attackers develop mock websites that are similar to the actual ones. The victims are tricked into entering their login IDs and passwords, which are later harvested. The websites generally contain similar domain names.>

IV. PHISHING ATTACK METHODS

Phishing attacks involve intense psychological manipulation. Perpetrators take advantage of psychological characteristics to deceive their targets. In phishing attacks, the use of urgency is common. Messages sent to the targets state the need to take immediate action to prevent the suspension of an account or the loss of funds. Fear is also another tool in phishing attacks. In this attack, the target panics as a result.

Trust can also be taken advantage of in an attack by using familiar logos, official-sounding language, and professional-formatting. Those with curiosity can be attacked by using fake rewards, temptations, or updates about news. Impersonations, or attacks on power, can also be used, in which an attacker will claim to be a high-ranking government official or executive.

V. EFFECT OF PHISHING ATTACKS

Phishing attacks have seriously harmful effects on various levels.

5.1 Impact on Individuals

People who are prone to phishing attacks can have financial losses, identity thefts, or invasion of their privacy. Their personal particulars can be utilized for conducting phishing attacks. People can also be subjected to stress, anxiety, or loss of trust in online services.

5.2 Impact on Organizations

In addition, organizations are vulnerable to financial losses, breaches, and loss of reputation as a result of phishing attacks. Moreover, data theft can cause disruptions in the operation processes due to legal complications.

5.3 Social Effects or Impact

Societal impacts of phishing include an increase in cyber crime, thus undermining trust in cyber systems. It is difficult for governments and law enforcement agencies to locate cyber criminals. The thus intimidated cyber economy is impacted negatively.

VI. IMPORTANCE OF USER AWARENESS

User education is among the strongest methods for combating phishing attacks. Since phishing attacks the human element, education of the users plays an important role.

6.1 Role of Awareness

Awareness enables users to identify phishing messages and prevent dangerous behavior. Users with awareness will be more likely to check the source of messages and detect phishing attempts. Awareness can greatly lower the effectiveness of phishing attacks.

6.2 Awareness Program

Organisations and institutions should hold awareness programs regarding cyber threats. Training, workshops, and awareness events enable users to understand how phishing attacks occur. Live examples increase the efficiency of learning.

6.3 Safe Online Practices

It is advised that users adhere to common principles of cybersafety, such as avoiding links from strangers, checking the accuracy of the sending information, maintaining secure passwords, implementing two-factor authentication, and keeping all software up to date.

VII. TECHNICAL MEASURES FOR

Although user awareness is very important, technology is also a factor when it comes to prevention of phishing. Filtering email tools can identify and prevent phishing emails. Anti-phishing software notifies a user of a phishing website. A secure browser notifies a user of a threatening website. Multi-factor authentication provides an extra level of safety and authentication.

Technical solutions and awareness programs for users make a formidable mechanism for defending against phishing attacks. Technical solutions alone are no good without educated users.

VIII. CHALLENGES OF PHISHING PREVENTION

Despite different mechanisms put in place to prevent attacks, phishing attacks have continued to improve and become more realistic. Phishers have employed different means to trick internet users. Lack of awareness about cyberspace operations is still a challenge to internet users who are new to cyberspace. The rapid development of internet platforms exposes more targets to attacks. It is difficult to monitor and punish internet hackers.

IX. FUTURE SCOPE AND RECOMMENDATIONS

The fight against phishing must continue to advance with improved technology and education. Artificial intelligence and machine learning can improve phishing filters. Governments must develop tough cyber laws and must encourage citizens to report cyber crime incidents. Institutions of learning must integrate cyber security education in their syllabuses. Internet users must take matters into their hands and stay informed and alert for their safety on the internet.

X. CONCLUSION

Phishing attacks are considered a major threat in the field of cyber security. Phishing attacks are done by taking advantage of the trust and lack of awareness of individuals in the digital world. This paper worked on the idea of phishing attacks, and it also covered various kinds of phishing attacks, methods used in phishing attacks, and effects of phishing attacks in the digital world. Technical security steps are important but are insufficient on their own. The best protection for phishing attacks lies in awareness. By combining awareness and technology, it will become easier to make the digital world a safe place.

REFERENCES

[1] Garera, S., et al., “A Framework for Detection and Measurement of Phishing Attacks,” ACM, 2020. Kumar, R., and Mishra, A., “Cyber Security Threats and Prevention,” International Journal of Computer Science, 2021.
[2] Sharma, P., “Phishing Attacks and Social Engineering,” Cyber Security Review, 2022. National Cyber Security Centre, “Phishing Guidance and Awareness,” 2023.
[3] Stallings, W., *Network Security Essentials*, Pearson Education.