Addressing the Growing Cyber Security Threats by Understanding and Mitigating Phishing Attacks

Balam Manohar Prasad[1], N N Venkataramana[2], Sattiraju Bhargavi[3], Vundamatla Gurukumar[4], M Satyanarayana[5]

[1]*Assistant Professor, Department of CSE, Srinivasa Institute of Engineering and Technology*

[2,5] *Assistant Professor, Department of MCA BVC College of Engineering, Palacharla*

[3]*Leacturer, Department of CSE ABN PRR College of science, Kovvur*

[4] *Assistant Professor, Department of CSE BVC College of Engineering, Palacharla*

Abstract: In the current scenario, every person from the richest businessman to the normal ordinary person is facing issues regarding cyber attacks like password cracking, different types of virus attacks, phishing, etc. One of the major problems faced by the people is phishing attacks. A small link can make the biggest loss. Even though the government provides many awareness programs, many people are facing issues regarding phishing emails, messages, etc.

In this phishing attack, the attacker may send a link to the target person. In that link, the attacker may include malicious software programs to get sensitive information like bank account details, credit card details, passwords etc., which are related to the target person. Not only sending links through mail, there are also other types of phishing attacks which will be discussed in this journal.

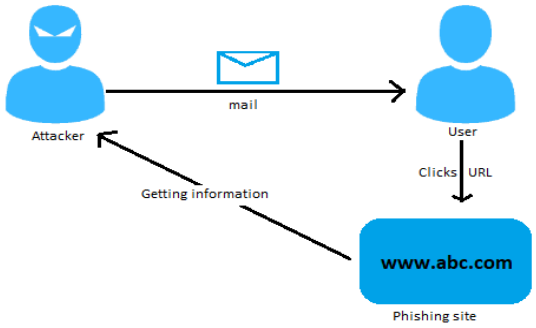
Keywords: Phishing, malicious, vulnerabilities, sensitive information, fraudulent, scenario, virus, e-commerce, credit card, injecting.

I. INTRODUCTION

In cyber attacks, so many people lose their lives by losing their information. In the process of attacking a system, the attacker may use different types of techniques like password cracking, virus injecting, phishing, etc. Phishing is a fraudulent act done by a person to gain sensitive information from the target system. This attack will be done by sending URLs to the target system to gain sensitive information like bank account details, credit card details, etc. This attack will be done by injecting malicious software programs into the target system to gain access to gathering sensitive information. This attack may also be done to identify an organization's vulnerabilities related to its software products.

II. WHAT IS PHISHING MAILS?

Phishing is the oldest but working techniques of social engineering attacks. A phishing mail is nothing but gaining sensitive information by sending an email. In that email it consists of an URL or a document which is embedded with a malicious software program. For example a friend or a known person tries to send you an email or tries to communicate with you through email and in that email, there will be a malicious virus or a malicious file to download when you click on download your system may be hacked. So you have to take care about this type of fraud while communicating with them and knowing that the email was fake or real.



III. HOW THE ATTACKER TRIES TO ATTACK?

The attacker tries to create a replica of a original website or a domain and check whether there is anything which can easily detected. After the successful creation, sometimes for the surety a tiger runs the phishing site on local host using the software like “XAMPP”.

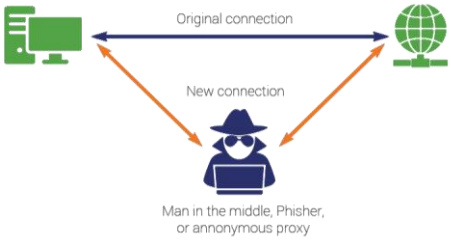
Once phishing site runs with zero errors on local host attacker register for a fake domain and fake hosting provide fake information. Attacker tries to keep domain which looks similar to the original one once

the phishing site is live, now attacker targets the user and send phishing link via email or over the charts in such a way that user gets manipulated and opens the link once the user login to the link his confidential information are recorded.

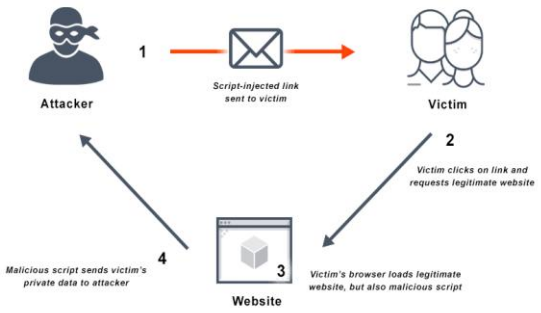
Let's try to get some knowledge related to phishing techniques, in this phishing the attacker may send an email to the target person when the target person views the email and downloads the files that are attached to the email or click the link sent in the mail then the target system may have chances to get effected by the hacker. In phishing, there are different types of techniques to attack the system some of them are as follows:

IV. TYPES OF PHISHING ATTACKS:

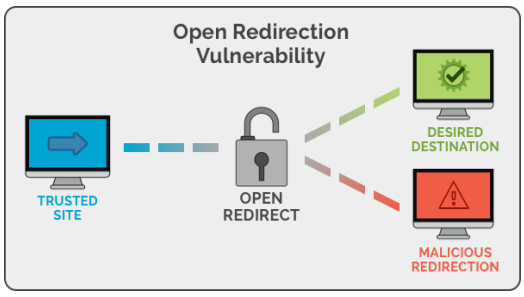
1. In Man in the middle attack a person observes the communication and activities between client and server or host to host two sniffs the activities of the target system. The attacker tries to attack the target system when the attacker gets the vulnerability to access the target system. This can be done in http and https.



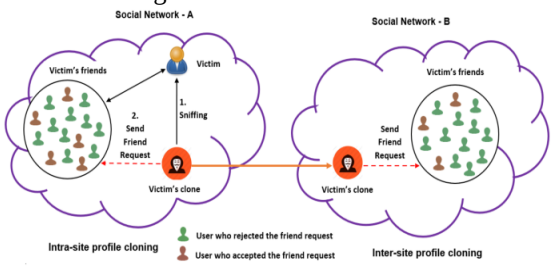
2. Cross site scripting will be done by sending a malicious link to the user who clicks it and execute the attackers code in their browser the code can bypass the browser same origin policy allowing the attacker to access cookies session tokens and other sensitive data it is also can be done rewrite the HTML (Hyper Text Markup language) content on the page and take on the user identity and perform actions on their behalf.



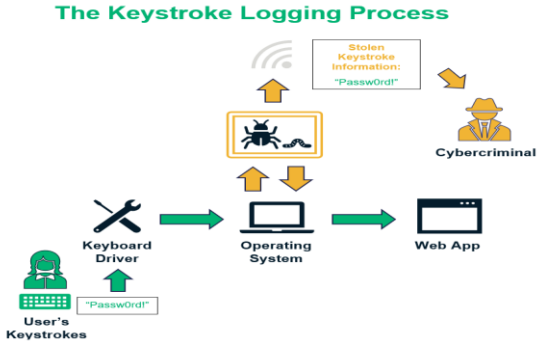
3. URL redirection vulnerability also known as open redirect is a security flaw that allows attackers to redirect users to malicious websites. Vulnerability occurs when an application uses user controllable data in an unsafe to redirect users to another resource attacker can be used this vulnerability to conduct phishing attacks on this social engineering a text.



4. A Site cloning is a phishing attack based on the attackers ability to duplicate a message that the target has previously received for example if a brand sent out a mass email a clone fisher could duplicate it alternatively someone known to be waiting for a package could be targeted using a fake tracking email



5. Keylogger or malware based attack will be done by the attacker by injecting the malicious code into the target system by using any one of the attacks like sending email or install a file which holds the malicious code into the target system etc. The keyloggers identify the activities of the target system and anonymously sends data when the target system is online state.



There are other types of phishing attacks are also there like fake search engines, client side attacks, DNS redirection attacks.

V. PREVENTION AND MITIGATION

However the number of victims is rising exponentially as a result of inadequate security technology studies have categorized phishing attacks by basic phishing methods and defenses ignoring the significance of the end to end phishing cycle. Different types of attacker's threats targets and attacker tactics the proposed anatomy will also make it easier for readers to understand how long it phishing efforts last increasing knowledge of these attacks and the techniques used as well as aiding in the creation of a comprehensive anti-phishing system. Due to the anonymity and lack of regulations on the internet phishing attacks are more likely to be successful.
In India we can complain that fraud like unauthorized access, investment fraud, OTP fraud, debit card credit card or any other type of card fraud, dating apps, fake social media handling, E-Commerce fraud, honey trap, trading fraud, etc.

When you require a complaint against cybercrime you have to submit the below documents (as per some state cyber security cells)
1. Aadhar card
2. Address proof
3. Complaint soft copy and hard copy
4. Bank statement
5. Fraud related documents

You can complain to the state cyber cell if the fraud is done above 1 lakh and if it is below 1 lakh you can complain to a nearby police station.

VI. CONCLUSION

Phishing attacks continue to the pervasive and increasingly sophisticated form of cybercrime, posing significant risks to individuals and organizations. These attackers ranking from simple emails camps to more complex technique such as keyloggers cyclone in cross seeds scripting exploit vulnerability and manipulate victims into divulging sensitive information.

Speed government initiative and cyber security awareness campaigns the success rate of phishing attacks remaining alarmingly high, highlighting the need for improved security technology better education for users and more comprehensive regulatory frameworks. Prevention starts with awareness and extends to adopting best practices such as scrutinizing emails avoiding such suspicious links and employing advanced cyber security tools.

Mitigating phishing attacks required a multi-fasted approach that includes individual vigilance, organizational security protocols, and the cooperation of law enforcement. In cases of cybercrime, prompt reporting to appropriate authorities whether a local police station or a state cyber cell can help address and CRUB fraudulent activities. The key to combating phishing life in a combination of technology fences user education and a culture of cyber security awareness that empowers people to recognized respond to and report phishing attempts. Only through continued collaboration and vigilance can be hope to demons the impact of these harmful attacks and protect valuable personal and financial information.

REFERENCES

[1] https://iacis.org/iis/2020/2_iis_2020_1-8.pdf
[2] https://ieeexplore.ieee.org/document/9055943
[3] https://www.ripublication.com/ijaer19/ijaerv14n9_15.pdf
[4] https://www.sciencedirect.com/science/article/pii/S0167404823002973
[5] https://ieeexplore.ieee.org/document/9396693
[6] https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full
[7] http://vijayawadapolice.ap.gov.in/?page_id=55596
[8] https://cybercrime.gov.in/
[9] https://hyderabadpolice.gov.in/cyber_crimes_hyderabad_police_station.html
[10] https://eservices.tnpolice.gov.in/CCTNSNICSDC/RedirectToNationalCyberCrimeReportingPortal%28NCRP%29