Study and Analysis of Phishing Attack

Thakur Pooja Prakash*[1] Gaikwad Nandini N.[2], Thakur Vrushali M.[3]

Assistant Professor, Department of Information Technology, Mahatma Phule, A.S.C. College- Panvel, Raigad[1,3]

Assistant Professor & Head, Department of Information Technology, Mahatma Phule, A.S.C. College, Panvel, Raigad[2]

Corresponding Author: pt1230120@gmail.com

Abstract: *Now a day there is lot of data security issue. Hackers are very intelligent now, they using their knowledge to hack someone system and grab their information such attack is call phishing attack. In phishing attack scammers collect personal information from user. Attacker sends fraud e-mails, text message, telephone calls to users to gather their information. Phishing is same like fishing in lake, instead of trying to capture fish, phishers are stealing personal information. The personal information could include credit card details, username and password, bank details. After gathering the information attacker could commit crimes such as financial loses and identity theft. Phishing attack is common in online communication and transaction. This paper gives fair idea about phishing attack.*

Keywords: Attack, Information, Fraud, E-mail, Communication

I. Introduction

Phishing is example of social engineering. Communication purporting to be from popular social websites, auction sites, online payment is commonly used to lure the unsuspecting public. Phishing is cybercrime, which involve luring the user into providing sensitive and confidential information. Phishing e-mail may contain link to website that are infected with malware. Phishing is mainly use in e-mail hacking. For getting personal information of user hacker send link via mail to user, and then user goes to that link and fills all details in that link and then the hacker get all personal information of the user.

Explanation of phishing step-by-step:

1. Attacker sends E-mail to the victim. The individual who are affected by the attack are called victim or target.
2. Then victim click on email and goes to the phishing website.
3. From phishing website attacker collect victim credential.
4. Attacker uses victim credential to access website.

Later we see detail mechanism of phishing attack.

Phishing attack can be performed manually but to overcome the attack and to respond effectively to the attack require a lot of time, intelligence and manpower. This may take days or even weeks to respond and analyze the attack in depth. Manual investigation has lot of dependency on the security analyst's talents and tools available for investigation. These manual investigations go wrong due to human error.

II. Types of Phishing Attack

2.1 Deceptive Phishing

In this type of phishing an attacker obtain confidential information from the victims. Attackers use the victim personal information to steal money or to launch other attacks. Example of deceptive phishing: A fake email from a bank asking you to click a link and verify your account details.

2.2 Spear Phishing

Spear phishing targets specific individuals instead of group of people. Attackers often search their victims on social media like facebook, instagram and other sites. That way, they can customize their communications and appear more authentic. Spear phishing is often the first step used to penetrate a company's defenses and carry out a targeted attack.

DOI: 10.48175/IJARSCT-3087

2.3 Whaling

A whaling attack is a specific type of phishing attack that targets high-profile employees like the chief executive officer or chief financial officer, to steal sensitive information from a company. In this attack the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker. Whaling attacks are often more difficult to detect and prevent than other phishing attacks. Security administrators can help reduce the effectiveness of whaling attacks by encouraging corporate management staff to undergo information security awareness training.

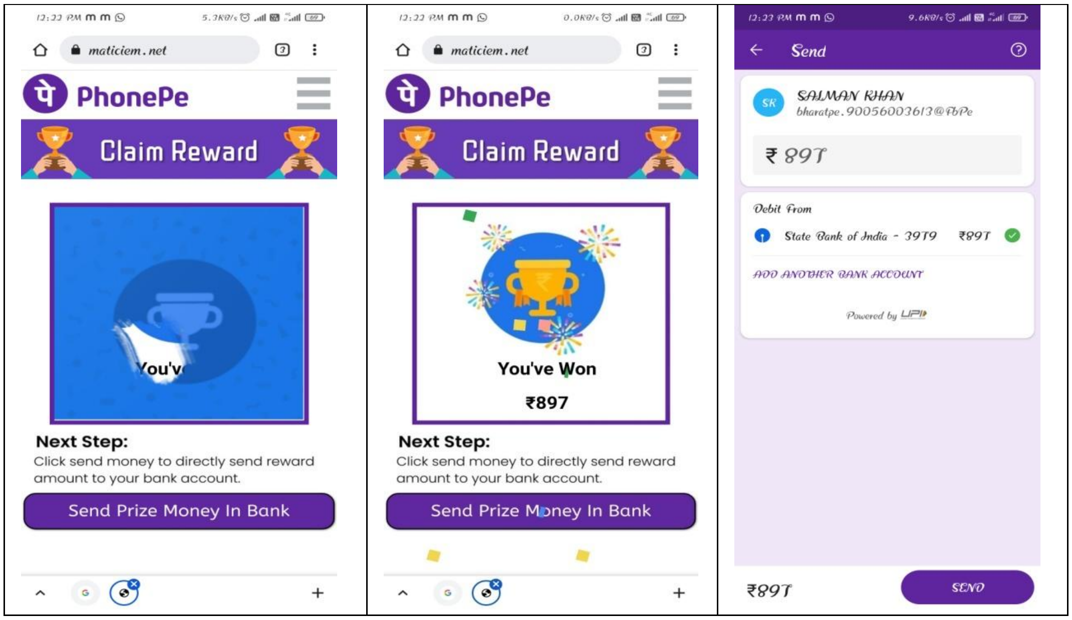
2.4 Pharming

Similar to phishing, pharming sends users to a false website that appears to be genuine. In this attack victims do not even have to click a malicious link to be taken to the fake site. Attackers can infect either the user's computer or the website's DNS server and redirect the user to a fake site even if the correct URL is typed in. Motive of all phishing attack are the same. Only the method and technique used to obtain information varies from type to type.

III. Some Examples of Phishing Attack:

3.1 Like Phishing Websites

Below diagram shows the phishing website in that attacker steal money from users. On unauthorized sites attacker pops their games like spin wheel and won prize games. Then they redirect user to any transactional application like PhonePe. And steal their money saying user won that money.



Next Step:
Click send money to directly send reward amount to your bank account.

SALMAN KHAN
bharatpe.9005600361 3@fbPe
₹ 897

State Bank of India - 3979 ₹897

₹897

Figure: Phishing website

3.2 The Fake Invoice Scam

In fake invoice scam relies on fear and urgency pressuring an end user to submit a payment for goods or services they've never even ordered or received.

3.3 Email Account Upgrade Scam

The message is supposedly from the recipient's email administration team. It claims that the user has to upgrade their mail accounts. This scam steals the email accounts by tricking recipients into providing their log-in details.

3.4 Advance-fee Scam

The scam typically involves promising the victim a significant share of a large sum of money, in return for a small up-front payment, which the fraudster claims will be used to obtain the large sum.

3.5 Google Docs Scam

In Google Docs scam access victims account data. By granting permission, users unwittingly allowed hackers to potentially access to their email account, contacts and online documents. The malware then e-mailed everyone in the victim's contacts list in order to spread itself.

3.6 Message from HR Scam

We all (hopefully) trust our HR team, especially when it comes to receiving highly important emails relating to company-wide or personal updates. The problem is, cyber criminals know just how much trust we place in our HR colleagues.

IV. Phishing Mechanism

In phishing attack attacker influence the victim to providing confidential information about her/him. To perform such an attack, the attacker mimics an authentic website. To mimic the website, attacker constructs a malicious site using a phishing website. This phishing website gathers all information of target and provides it to the attacker. The victims are unable to distinguish between genuine and phishing websites cause they fall into attacker trap.

To obtain target personal information attackers follow several steps of phishing attack. This can be explain in 6 steps:

4.1 Plan, Composed mail, Attack, Gather data, Fraud

The attacker starts process by planning the attack. In this process the attacker deciding the legal website and creates an illegal website that looks similar. Then victim cannot differentiate legal and illegal website and provide their personal information on illegal website. In this step attacker composing an email that looks like genuine for the victim to be lured into providi t followed by gathering the information on the v n tricked by the phisher. Using the target informa etc.

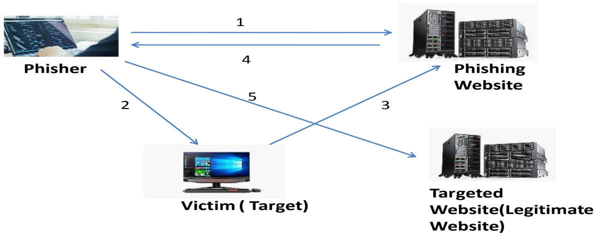


Figure: Phishing Mechanism

Above figure Phishing mechanism, shows phishing mechanism and how attackers manage to collect sensitive information of the target. In this mechanism shows several steps involve to attack target.

Step 1 shows that with the help of phishing website phisher that means attacker composes an email. This email is composed such that it looks legitimate and genuine. In step 2, attacker sends that email to victim. Step 3 shows that, the victim is not able to differentiate between legitimate email and phishing email, then victim open that email. Then that email redirect victim to the phishing website that exactly look like legitimate website. The victim enters their login credential in the webpage oblivious of the fact that it is a malicious site. In step 4 illustrate that, phishing website provides login credentials to the attacker. In the step 5 the phisher uses user data that obtain from phishing website and then logs into target website. Now attacker would be able to access all the personal information of the victim. Thus the process of phishing is complete.

DOI: 10.48175/IJARSCT-3087

IV. Preventions Of Phishing Attacks

4.1 Don't provide your information to an unsecured site

If the URL of the website doesn't start with "https", do not enter any sensitive information or download any files from that site. Sites without security certificates may not be planned for phishing scams.

4.2 Don't click on that link

Even if you know the sender, it usually not advisable to click on a link in message or email. Some attack is fairly complicated, and the destination URL looks like a carbon copy of the legitimate website. If it's possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

4.3 Get free anti-phishing add-ons

Most browser nowadays offer you to download add-ons that spot the signs of a malicious alert you about known phishing sites. This software's are usually completely free so there is no reason not to have this installed on every device in your organization.

4.4 Rotate passwords regularly

If you have online account, you should get into the habit of regularly change your password so that you prevent an attacker from gaining access. So adding that extra layer of protection through password rotation or changing can prevent ongoing attack.

4.5 Don't ignore updates

We receive numerous update messages and get frustrated, so we ignore that updates. Don't ignore this updates because updates and security patches are released for a reason, so keep up to date with modern cyber-attack methods by patching holes in security. You could be at risk of phishing attack if you don't update your browser.

4.7 Install firewalls

Installing firewalls are acting as a shield between your computer and an attacker, so firewalls are an effective way to prevent external attack. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker to steal sensitive information.

4.8 Don't give out important information unless you must

Unless you 100% trust the site you are on, you should not freely give out your card information. Make sure, you only provide information to only verified and genuine website.

V. Conclusion

Phishing is modern era to twist any number of age-old peoples to trick by giving information which are used against them till 2020, 6.95 million new phishing and scam pages were created and in a month there are 206,310.

Hence, I would like to conclude that avoid using unauthorized website where this type of phishing attack occurred and if incase it happens just closed the tab, since this type of cyber crime is occurring in daily basis you should shoulder your responsibility to protect yourself from trickery and deception Now a days there are many software tools such as spam filters and many antivirus software, that can help, but in the end, we must all be fearless and focused on all suspicious email and SMS communications.

References

[1]. https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html

[2]. https://blog.usecure.io/hubfs/Example%20of%20a%20fake%20invoice%20scam.jpg

[3]. https://blog.usecure.io/the-most-common-examples-of-a-phishing-email

DOI: 10.48175/IJARSCT-3087

[4]. https://www.pcrisk.com/removal-guides/17098-last-warning-upgrade-your-email-to-avoid-shutting-down-email-scam

[5]. https://www.bbc.com/news/business-39798022#:~:text=Victims%20of%20the%20scam%20were%20asked%20to%20let,victim%27s%20contacts%20list%20in%20order%20to%20spread%20itself.

[6]. https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/

[7]. A review on phishing attack by Akarshit Shankar, Ramesh Shetty, Badri Nath K. International journal of Applied Engineering Research ISSN 0973-4562bVolume 14,Number 9(2019) p. 2171-2175

DOI: 10.48175/IJARSCT-3087