Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

An Overview on Phishing- its types and Countermeasures

Antonette R. Muntode
Student
Dept. of Master of Computer Application
Jawaharlal Nehru Engineering College
Aurangabad, India

Sandeep S. Parwe
Assistant Professor
Dept. of Master of Computer Application
Jawaharlal Nehru Engineering College
Aurangabad, India

***Abstract*— Cyber crime is an ongoing threat these days. Every other day we come across new kinds of cyber crimes and their drastic consequences. Most of us think only "hacking" into computer systems is cyber crime. There are innumerable ways in which cyber criminals work to steal not only financial resources, but also sensitive and crucial data. This paper discusses about one of the major crimes of cyber space- Phishing.**

Keywords—Phishing, malware, pharming, cyber, crime

I. INTRODUCTION

If we happen to know about all these cyber crimes, we might want to stop using the internet entirely, which will only cause us a lot of inconvenience. Therefore, instead of completely not using the internet, it is important that we recognize the types of cyber crimes and ways in which we can keep ourselves safe from being a victim to such crimes.

A cyber crime is basically a crime that uses internet or cyber space as a medium to commit the intended deceitful acts. Cyber criminals target specific computers for the sake of monetary gains or other kinds of deceit. Pharming, phishing, skimming, eaves dropping, DOS attacks are some of the major cyber crimes that are on a rise now-a-days.

Phishing is a type of cyber crime in which the attacker masquerades as a trusted entity. The attacker tries to entice the victim by offering temptations that the victim easily falls prey to. These attackers usually steal victims' sensitive data such as credit card details or login credentials. This happens when the victim clicks on any link sent by the attacker who takes the form of a genuine entity, or when the user discloses data to the attacker over a phone call. By tempting the victim and offering fake gains, the intruder obtains user's details and uses it against the victim maliciously.

Following are generally the things that are the target of a phishing attack [4]:

- Bank Account Number
- Usernames and Passwords
- Credit card details
- Internet banking details

II. LITERATURE REVIEW

First Raymond Chiong et al have discussed certain examples of phishing along with counter measures that will protect us from the various types of phishing attacks[1].

A.Aleroud et al have investigated phishing attack and anti phishing techniques in environment such as mobiles, and social networking sites[5]

Dr.M.Nazreen et al have discussed types of phishing attacks and how these can be avoided by various anti phishing techniques[2].

Muhammet Baykara and Zahit Ziya Gurel have described the software called "Anti Phishing Simulator" which helps detect phishing emails[4].

A. Core Process of phising

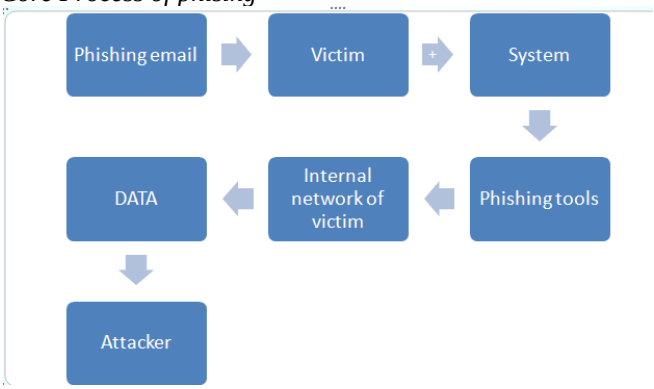

Fig.1. Process

The actual process of phishing starts when the attacker has targeted a user whose data or credentials will in some way profit the attackers. This profit can be monetary or any other gain.

The attackers then send a fraudulent email or message by a particular medium which the victim believes to be coming from genuine sources.

This email might transmit ransom ware or malware into the target system or simply redirect the victim to a page where the user's personal information, credit card details or login credentials might be demanded. Advanced Persistent Threads (APT) and other such cyber attacks all begin with phishing.

When the victim opens the malicious email or message and proceeds to perform the requested action , the phishing tools that are send by the attacker are activated and the perform the required action of stealing information attacking the financial resources of the victim .

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

III. PHISHING TECHNIQUES

A. *Email Phishing Scams*

An attacker may put in all efforts to formulate an email which may seem authentic to lure the victim into sharing the requested data. The attacker uses the original logos, signatures from spoofed firms to appear valid.

The attacker also manipulates the victim by mentioning urgency. For instance, the phishing email might talk about an expiration of something to pressurized the user to perform the necessary action at the earliest. This makes the victim vulnerable and gradually the victim falls prey.

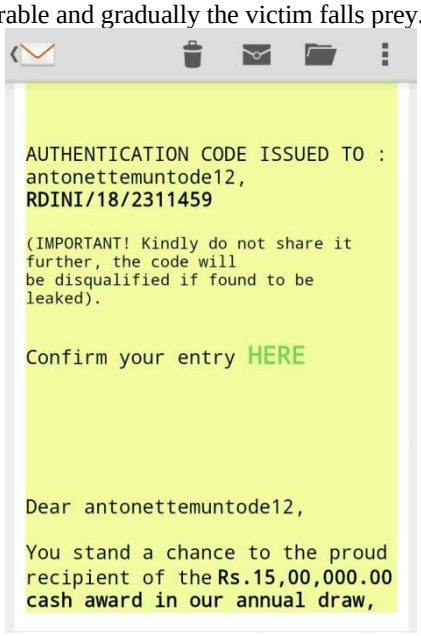

Fig.2. Email Phishing example

B. *Spear Phishing*

Spear phishing can be called as customized phishing wherein a specific organization or an individual entity might be targeted for a pre defined reason [2].

Spear phishing requires detailed knowledge of the target person or firm, including its operational structure have spear phishing targets who with something in common.

For example: - People from a particular department or an entire organization.

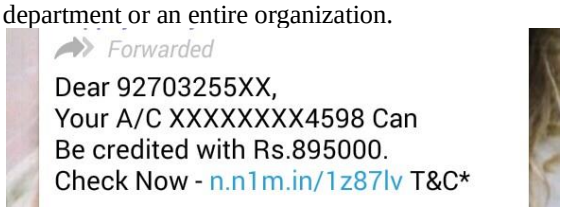

Fig.3. Spear phishing example

C. *Phone phishing*

Phone phishing includes messages that seem to be from banks or network operators. The target victim might receive an SMS which speaks about a sim expiring or about urgent updating of certain bank details or about a new service activated on your device [2].

They ask to visit a particular page which them gives way to an attack.

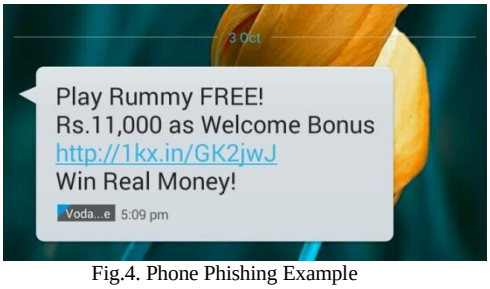

Fig.4. Phone Phishing Example

D. *Man-in-the-Middle attack*

This attack is one wherein there is third party (the attacker) who secretly interprets the data that is being transmitted between the two parties. The man-in-ithe-middle (attacker) accesses this information fraudulently, modifies it , and further transfers it to the other side the message , hence is now altered does not remain original or authentic.

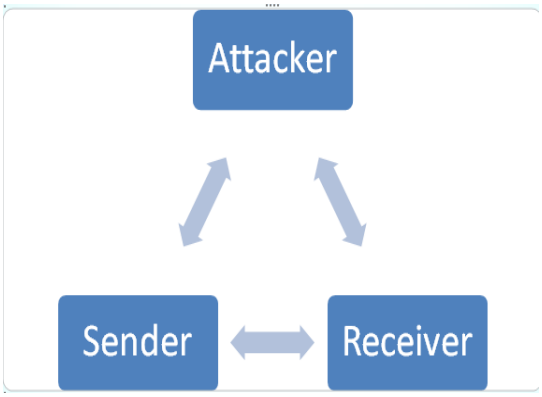

Fig. 5.Man-in-the-middle

E. *Pharming(DNS based phishing)*

In this type of attack, hindrance is done to the resolution of the domain names to an IP address. This is done so that the domain name of an authentic site is mapped onto the IP address of the fraudulent site.

Request for a genuine domain name to redirect the victim to a rogue might cause the victim a serve loss of data or money.

F. *Phishing by Search Engine Indexing*

The attractive ads and offers that pop up when you visit a particular web page through a search engine are put there with an intention that the user stumbles upon them and is mislead to a corrupt link or IP address.

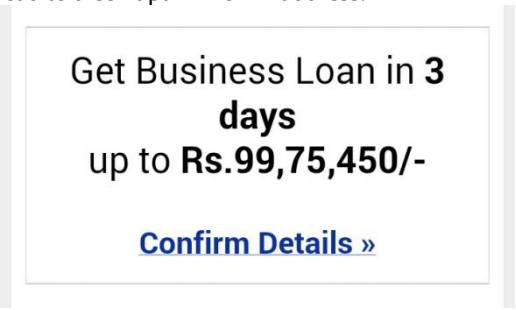

Fig.6. Example for Phishing by Search Engine Indexing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

G. Games , Social and Prizes

The gaming element on certain sites entices the users to play certain games such as the "wheel games" or the "three question" game [6].

These games promise the user exciting prizes which the victim immediately falls prey to.

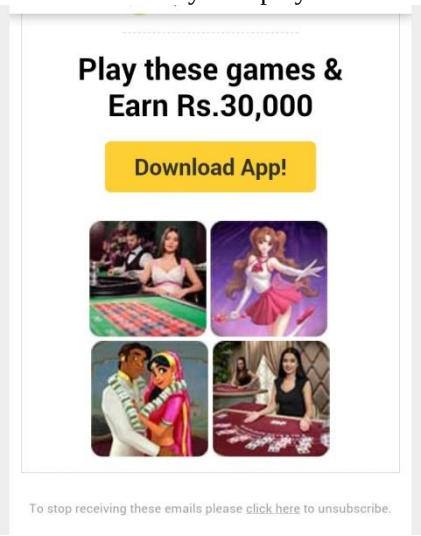

Fig.7. Phishing through games

H. Creating Fake Users to Fake it

Creating fake users and using them as a means to make the offer seem authentic hence winning the trust of the victims is another way of carrying out phishing attacks. These fake user accounts are basically JavaScript codes that are embedded as plug-ins in these phishing sites [6]. They make the victim believe that there are people who have won prizes and proceed with further steps.

Fig.8. Fake comments

I. Share and Spread

Once you have "won" these games or rewards, the site asks you to further share the link with your social contacts through various social media networks such as WhatsApp, Facebook, etc. This is done to widen the scope of distribution of the attack and increase the target network.

Fig.9. Sharing the misleading link

IV. A GENERAL PHISHING EXAMPLE

- A spoofed email is collectively sent to all members of an institution from myuniv.ac.in
- The email speaks about the urgency to change the password as the initial password is about to expire written the next few hours.
- There is a link provided at the end of the email which claims to redirect the user to a page that will update the password.
- Those who actually respond to the mail end up leaving their sensitive data to the attacker or allow a malware to be downloader or activated onto their system.

V. SOME OF THE FAMOUS SCAMS OF ALL TIMES

A. Operation Phish Phry

. In 2009, large number of bank customers reported to have face serve data loss due to providing sensitive information to fraud from which demanded their credit card numbers, login password and account number. These forms appeared to have arrived from official websites that redirected the users to false websites.

The operation phish phry managed to pilfer around $1.5 million front hundreds of thousands of targeted bank accounts [3].

B. Walter Stephan

Walter Stephan was this one man who single handedly faced th3e lose of $47 million because of a single scam. While Walter over the CEO of FACC (FACC- a company which manufactures aircraft components for Boeing and airbus) the attackers faked Walters email and demanded from the organization an enormous sum for a supposed "acquisition project" [3].

The systems at FACC were not hacked. The attackers just guessed Walter email correctly and spoofed an email address similar to that. The juniors sent the wire trusting that the email is from the CEO.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

C. The Target /FMS Scam

In 2013, the target data branch affected 41 million retail card accounts, and 110 million users .In this scam the attackers did not attack target directly. They attacked a third party HVAC vendor named Fazio Mechanical Services (FMS) which had prim ledge access to target services [3].

The attackers could easily access target servers on compromising FMS's servers.

D. The Ukraine Power Grid Attack

This scam was remarkable because a malicious firmware was specifically developed to damage physical machinery. Email phishing was used as the original source of attack here [3].

E. The Moscow World Cup Vacation Rental Scam

In this scam, enumerable emails that assured free tickets, vacation rentals, etc. were sent to world cup fans [3].

VI. ANTI PHISHING TECHNIQUES AND COUNTER MEASURES

Below are listed some counter measures that might keep us while dealing with phishing while dealing with phishing scams

- Avoid clicking on any hyperlink that do not show sign of an authentic source.
- Make use of modern and updated software that guard your devices and systems. Updated versions of anti-malware, anti-virus can provide a strong protection.
- Do not download applications or software from unreliable websites, especially when they allow download for free. These free downloads may contain malware or Trojans [1].
- Make use of "https" protocol while surfing.
- Email authentication and email filtering is highly essential.
- Avoid playing games that popup out of nowhere.
- Filter out all the content that you surf or use from over the internet.
- Blacklist all the unknown, unreliable sites, especially the ones that are blacklisted by trusted entities.
- Always be alert and try to have enough knowledge about fraudulent activities and security.
- The three basic solutions to phishing attacks are[7]:
  1. Prevent phishing
  2. Detect phishing while there is still time
  3. Train stakeholders to be aware

VII. CONCLUSION

This paper briefly discusses how the widespread use of emails and digital media paves way for cyber crimes, if used carelessly.

It also mentions some common phishing techniques. The sole process of phishing is described. This paper includes an overview of some well spoken of phishing scams. And finally, there are some countermeasures that can help you recognize a phishing attack and help you to avoid falling victim to such attacks.

Phishing is one of the most common and rapidly growing types of cyber crimes. If the digital and electronic modes of communication are not utilized with proper precautions and thoughtfulness, it may lead to severe loss of finances and data.

VIII. REFERENCES

[1] Biju Issac, Raymond Chiong, and Seibu Mary Jacob, "Analysis of Phishing Attacks and Countermeasures".
[2] Dr. M. Nazreen Banu and S. Munawara Banu, "A Comprehensive Study of Phishing Attacks," vol. 4(6). IJCSIT, 2013, pp.783–786.
[3] https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/
[4] Muhammet Baykara and Zahit Ziya Gurel, "Detection of Phishing Attacks," ISDFS, 2018
[5] Ahmed Aleroud and Lina Zhou, "Phishing Environments, Techniques, and Countermeasures: A Survey", vol. 68, 2017
[6] Or Katz (Akamai),"A New Era in Phishing"
[7] Ike Vayanksy and Sathish Kumar, "Phishing- challenges and solutions", 2018