Phishing Attack and Its Countermeasures

Arpan Chandel¹, Prashant Kumar², Dinesh Kumar Yadav³

¹ IT Dept, GCET Greater Noida, UP, India
² Delhi University, Delhi, India

DOI: 10.23956/ijarcsse/V7I6/0227

Abstract: In this paper, we have seen the various aspects of phishing attack both in theoretical and practical way. We saw the different ways being applied by the Phishers on their victims to gather their personal information. We also practically implemented a simple phishing attack and discussed how one can detect different phishing attacks and prevent it from harming you. We have also highlighted some facts and statistics about how the problem of phishing spam is growing year by year. As the technology will evolve so the power of the hackers will also increase and new and more powerful attack will come to the existence. Hence, my paper on Phishing will help others to learn to prevent and protect themselves from identity theft by doing this we altogether can create Internet a safe place.

Keywords: Phishing, Phishers, SmiShing, Deceptive, Scammers, Ransomware.

I. INTRODUCTION

With the fast growth and technological betterment, Internet has become an indivisible part of everyone’s life and especially the use of email provides a great flexibility to the users by allowing them to exchange information’s, data, media file etc. A survey conducted by Radicati Group shows that around 3.7 billion email users are there worldwide and about 205 billion emails are being generated per day and to be more precise it means 2.4 million emails per second and seeing all these facts and figures the chances of occurring of a criminal attack also increases and the entities that conduct such kind of attacks are being known as “Cybercriminals”. Cybercriminals want to acquire access to one’s personal or organization’s information and network through one’s email or mobile text messages. These methods are the simplest and most popular way cybercriminals try to conduct these attacks these are known as Spear phishing, Phishing and SmiShing. Spear phishing is an email sent to the potential victim or to a specific target individual in a company or simply an individual this is usually someone the cybercriminals knows that he will have a great access to a great amount of information that the criminal need to meet his objectives by getting the user to click on a link that will install malware (viruses, Trojan horse, spyware, ransomware etc.) on their computer. Phishing is a method by which the criminal sends vast numbers of unsolicited emails to user purporting to be from a reputable organization such as bank, an online shopping site or perhaps even the user employer. They often ask them to click on the link to update information including security details like passwords or personal information like date of birth, nick name etc. SmiShing uses mobile phones this method uses text messages for example the user will receive a text saying they’ve been chosen by their service provider to win a prize the message asks them to click on the link again whose objective is to look for person’s personal information and possibly a small payment to cover the cost of delivery of the prize, there it is another fishy email from someone who acts like one who is asking you to send money or to click link.

The cybercriminals send out billions of emails and praying that someone will open them. All they need is just one person to click a link that installs malicious software on the computer so that they can then control the user’s computer. The malware will send more emails spreading the infection to other computer around the world the malware also searches the user computer and network for passwords and more information, which is then sent back to cybercriminal. The stolen information can be used to gain access of one’s account or to steal information vital to an organization.

II. TYPE OF ATTACKS

Generally, for conducting a phishing attack requires a fake website but not all phishing attack require a fake website by conducting any of the phishing attack technique the main aim of the cybercriminal is to gain access to one’s confidential data such as user name, password, bank account number, credit card number etc. In this part we are going to discuss the several different types of phishing attack techniques used by the cyber criminals:

2.1 Deceptive Phishing.

“Deceptive” meaning is misleading and it is one of the most common way of conducting the phishing attack in this the phishers will send you an email pretending from a recognized source (banks, online shopping websites) which request you to make payment, to change yours existing password, re-enter your login username and password, verify your account information etc.

2.2 Phishing by malware software.

The phishers use malicious software to attack on a user after the installation of these infected software the phishers succeed in performing unauthorized actions, like transferring funds, accessing user’s private data etc.
2.3 Search Engine Phishing. -
In this phishers create a fake website with attractive or pleasing offers and append legally with the search engines. The user come across these websites while searching for their desired products and are being fooled into giving up their information.

2.4 Man-in-the-middle Phishing. –
In this the phisher places himself in between the user and the legal website or system. The phisher notes the entered information and later can use or sell the user information when the user is not active.

2.5 Phishing attack by Appending malign content. –
In this the phisher attaches malevolent content into a normal website.

2.6 Phishing attack by Key loggers and Screen loggers. –
In this the phisher use different type of malwares that keep record or track the keyboard input that is continuously monitor the key being pressed by the user and send this information to the phisher by the help of Internet.

III. PRACTICAL IMPLEMENTATION OF PHISHING ATTACK
In this section we are going to show how we can execute phishing attack through an example. We will be using Kali Linux to demonstrate these examples. Note the shown examples are for the education purpose only.

Phishing attack using Social Engineering Toolkit.
Social engineering toolkit or SET is a toolkit provided under the Kali Linux. Kali Linux is distribution of the Linux Operating System dedicated toward the penetration testing. Social engineering toolkit or SET is a toolkit provided under the Kali Linux. Kali Linux is distribution of the Linux Operating System dedicated toward the penetration testing. So to do this following steps are involved-

a) First open Kali Linux followed by opening Terminal. Type the command “ifconfig” to get our IP address because that’s the place where we want to send the data. The underlined inet is our IP addresses so next copy the IP address.

b) Now open SET by clicking Applications >> Social Engineering Tools >> Social Engineering Toolkit or open terminal and then type se-toolkit and hit enter. We will see a list of options and out of those we have to choose “Social Engineering Attacks” to do this press 1 and hit enter.
c) Select "Website Attack Vectors" by pressing 2 and hit enter. Under it select “Credential Harveseter Attack Method” by pressing 3 and hit enter. Since we are going to clone the Facebook website select “Site Cloner” option by typing 2 and hit enter.

d) Now paste your IP address as told in step “a” and hit enter. Now it will ask for the URL you want to clone, as we want to clone Facebook so type http://www.facebook.com. Now it would start cloning the website it could take a while. After cloning the website, it will show you the path were all the information is going to be stored. So the attack is live now and we are ready to go.
e) Now you can send this IP address to the victim through Facebook, Gmail or by any other mean but note this technique will only work when you and the victim are over the same network.

f) Now when the victim will open the link the following page will open and the victim enters his username say iamthevictim@gmail.com and password “iamthevictim” and the press login. The information will be send to the directory file of the Phisher and the victim will be the directed to the original Facebook login page. On opening the root directory file, we can see the username and the password entered by the victim.

IV. DETECTION AND PREVENTION FROM PHISHING ATTACK

In order to prevent Phishing attack, we must first spot it. According to a survey it’s being estimated that 156 million Phishing emails are being sent every day, and out of these 16 million Phishing mails get through the protection software (Anti-Phishing tools), 8 million infected mails are opened, 800,000 links are being clicked and 80,000 people fall for the scam and give away their personal information’s or details. So it becomes quietimportant that one must have knowledge to detect these scams and prevent it. So here we are going to discuss how to spot and prevent Phishing attacks.
4.1 Spotting and Preventing Phishing emails.

In this we will see different signs to recognize phishing that can reduce the chances of getting caught in a scam. So let’s have a look at some the signs.

a) First we have to look at the sender’s email address. Often criminals use different technique here: one they will insert company’s real logo before the @sign and other is the use of a web address which is much more similar or near to the original one. For example: -

Genuine Website email
https://www.vodafone.com info@vodafone.com

Scam Websites email
https://www.vodfone.com info@vodfone.com
https://www.vodapone.com info@vodapone.com
https://www.v0daf0ne.com info@v0daf0ne.com

Always be cautious of emails with generic greetings eg. ‘Dear Customer’ and ones with faulty grammar and spellings. But some time Phishers try their level best to make the email as authentic to the original one by using the names of the peoples who work in that company and other using the sense of haste, by using that your account will be deactivated, you’ll be fined if now acted, there’s a time etc. all these kind of cases could be used to create a state of panic in victims’ mind.

4.2 Spotting and Preventing Social Engineering Attacks.

It happens when someone tries to trick you into doing something that may cause harm to one. It can be like downloading malicious software, sharing of one’s personal information (username, password, bank/credit details etc.). Then it becomes quiet important to detect these Social Engineering emails because scammer generally use emails, popular websites, ads etc. that look much more genuine to the original one that people often use in their day to day life. The scammer sends you email as if it is being send from your bank, social engineering websites, credit card provider etc. but in original they are not the one who has send the mail. So it becomes quiet important for the person to not share their personal information over the email until unless person is sure that the email is being send by the authentic sender and it can be done by visiting companies’ original website and find different contact address moreover legitimate websites don’t ask for your account password and other financial detail.

How to avoid Social engineering attacks on web- Many of us sometime or the other might have seen some websites saying that they have find some issues (viruses, files) that is making your system or mobile slow and to download software in order to correct the issues but in reality a website cannot detect if your machine is being compromised or not. So when visiting a website one must surely check the page’s URL and especially look if it looks like original website like the case one we discussed in the above section that how genuine website and scam website can look before you enter your personal information on the website also check if the URL starts with HTTPS or not here ‘S’ indicates that the connection is encrypted and secure. Do watch for the browser warnings when you visit a website indicating it’s not secure so pay attention to these kind of warnings before entering personal information.

4.3 Preventing Man-in-the-Middle Attack.

These kind has caused the loss of millions of dollars worldwide. As we already know that in Man-in-the-Middle attack the hacker places himself in between two authentic communicating parties so the hacker tries to hack the communication between the two parties either by DNS spoofing, ARP poisoning or through email phishing. In an executed Man-in-the-Middle attack the communicating parties may have no idea that their communication is being watched over. So one can prevent this Man-in-the-Middle attack through three ways as discussed below-

4.3.1 VPN (Virtual Private Network)-

VPN broadens one’s private network across a public network. With the help of VPN, we can protect our sensitive data when we are browsing over a public network like public Wi-Fi and also on secure websites where we don’t want them to know our location or IP address. When we join a VPN our connection gets encrypted and secure by making us anonymous online preventing the hackers to monitor your communication. It is being creating by building a virtual point-to-point connection by the use of a dedicated connection.

4.3.2 Proxy Server with Data Encryption-

It uses reliable and secure proxy server and encrypt the transmission between the communicating parties. One can use software like OpenVPN, Tor Browser, I2P Hide My IP.

4.3.3 Secure Shell Tunneling-

A Secure Shell (SSH) is mainly used for logging into a remote machine and to execute commands but it can also support forward TCP and X11 connections. It is consisting of a tunnel which is being encrypted through SSH protocol. Use can set up SSH tunnels to transfer unencrypted traffic over a network through an encrypted channel.
4.4 Preventing Key Loggers Phishing attack.

“A key logger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke you make to a log file, usually encrypted. A key logger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. The log file created by the key logger can then be sent to a specified receiver. Some key logger programs will also record any e-mail addresses you use and Web site URL’s you visit. So how we must prevent key logger phishing attack? This can be done by the use of software tools like- Key Scrambler, Spy Shelter etc.

V. PHISHING ATTACK FACTS AND STATISTICS

While many of us tend to think of cyber criminals as mastermind hackers who perpetrate state-of-the-art attacks from behind the shadows of a hoodie, the truth is the majority are simple scam artists. They don’t bother with coming up with sophisticated ways to break through complex security systems. Why bother going to all that trouble when you can simply trick an employee into giving up information or clicking a link?

A. 85 percent of organizations have suffered phishing attacks

Wombat 2016 State of the Phish

According to Wombat Security’s 2016 State of the Phish report, not only more and more companies are falling victim to phishing attacks, the number and complexity level of the attacks they’re experiencing has gone up.

B. 30 percent of phishing emails get opened

Verizon 2016 DBIR
C. 250 percent surge in phishing detected in Q1 2016

![Unique Phishing Sites Detected October 2015 - March 2016](image)

APWG Phishing Activity Trends Report

D. 9 out of 10 phishing emails carried ransomware in March

![Percentage of phishing emails delivering ransomware](image)

PhishMe Q1 2016 Malware Review

VI. CONCLUSIONS

Phishing attack is one of the largest and fastest growing cybercrime and one must be aware of the types of attack can be conducted on him and how to protect self from these threats. Although many laws have been given by the government and educating people is the best defence against phishing attacks. Being a bit suspicious of all electronic communications and websites is recommended. Also, one must pet the habit of comparing the provided URL with an independent search for the company's website i.e. Compare the provided mail with the companies’ original URL.

REFERENCES


[13] Lakhita; Surendra Yadav; Brahmdutt Bohra; Pooja, A review on recent phishing attacks in Internet, 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Year: 2015, Pages: 1312 – 1315.
