Phishing – A Cyber Attack

Mr. Amit S Hariyani
Department of Computer Science, Bhavnagar
Maharaja Krishnakumarsinhji Bhavnagar University,
Sardar Patel Campus, Gardi Gate, Bhavnagar

Abstract— now a days "Phishing" becomes most popular in Hacking World. Here phishing doesn't means to catch a fish in net, but it seems similar to it, where victim can be anyone. In this technique hackers building some environment which is very similar to known application used by people such as Facebook, Twitter, Gmail etc., Then asking them some confidential information by providing some avarice such as 'you won some price', 'new version of so and so application is now available' or freighting by telling some lies such as 'your account security is compromised', 'we have noticed shady activity in your account in last 48 hours' etc., through emails and necessitate them to enter their confidential information, and using that they can easily hack their bank accounts.

Keywords—Gmail, Twitter, Facebook, Bank Accounts, Hacking, Phishing.

I. INTRODUCTION

The term fishing means to catch a fish, but now a days it becomes very popular in cyber world. Here the word used in cybercrime is "Phishing" instead of "Fishing" and people whose accounts have been hacked becomes victims like fish. In this technique hackers are using email as a basic tool to catch innocent people to hack their accounts and to make them foolish. They send some link with their fake email to anyone's mail account and force him/her to click on it so as they can redirect him/her to their fake website and after that they are asking to log on or to provide some confidential information to him/her, and then after victim's account can be easily hacked by hacker.

II. HOW PHISING WORKS ?

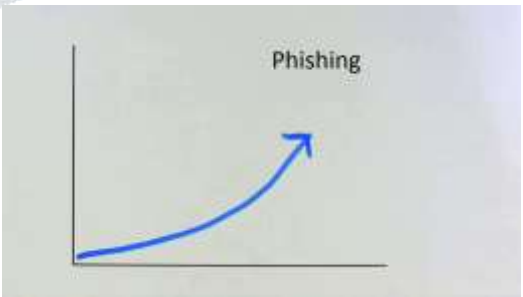
Phishing generally catches bank account numbers, credit card numbers, usernames and passwords and other personal information. There are two possible situations when people get attracted:

a. Fear (Your account is in trouble)
b. Excitement (You won some price)

Here in this technique hackers are creating environment (Such as duplicate website similar to our bank account website) and force people to redirect on it and to provide some confidential information such as username or password so that they can easily store entered data to their preferred location and use that confidential information later on to log on original website and make some transactions online or in other words they stole money online from bank account. First of all the duplicate website is created by hacker to make sure victim for log on, this website's look and feel exactly matches with the original one. After that hacker generates email which includes redirection link for his fake website, in this email he writes something that attracts people to redirect such as 'you won some price', 'new version of your application is available click here to redirect' or 'click here to verify your account' etc. People who found something real or interesting clicks on link, redirects to fake website and by mistake provide confidential information and loss their money. This is how phishing actually works.

III. EXPANSION OF PHISHING

Expansion of phishing is also a headache as it is growing fast. In this technique what happens is suppose someone has hacked my Gmail account then he will access my contact list and the hacker will send mail to persons in my contact list, people who receives mail from my account thinks that I have sent them mail and as an when they click on link they are also asked to log on Gmail account once, this time the webpage they see is duplicate one which has same look and feel as the original Gmail page has, and if by mistake they provide their login information their account also will be hacked and further their contact list used to send more fake emails. This is how the phishing expands. Recently Gmail passed out from this problem.



IV. USE OF MALWARE IN PHISHING

Sometimes phishing emails get the personal information by using malicious software or malware instead of asking you to details itself. In this situation we can prevent malware attack by considering such things:

a. **Hover a link:** when you hover a mouse cursor on link you can see a popup box or a tooltip that shows text inside the link and you can get judgment what to do whether to click on it or not.
b. **Be careful with attachments:** If you find some attachments having extensions like .pdf or .doc with extension .exe never ever click on it or download it

because actual application extension having only the original extensions no more postfix extensions.

c. **Always scan emails with attachments:** It is good practice to scan emails with reputed antivirus before downloading attachments from it as the antivirus can easily find out malicious code or malware and never allow to download and can easily protect from such attacks, but for that we need to keep antivirus definitions up to date so it can easily find new malware attacks.

V. PHISHING KIT

Phishing kit - a best weapon now a days used by hackers and it provides open space to make cybercrime for hackers. Even if someone has some technical skill of computers he can easily use this kit. This kit includes some phishing website tools which must be installed on server, after that the hacker can send email to particular victim and his work goes on. Phishing kit is freely available in some sites such as "dark web", "Phishtank" or "Openfish" etc.

A. How phisihing kit generated?

a. First of all hacker will clone the targeted website.
b. Then after its login page is changed to point to a credential – stealing script.
c. Then modified files packaged into zip file to generate phishing kit.
d. After that the phishing kit will be uploaded to the hacked website and files are unzipped.
e. And at last emails are sent with hyperlinks that points to new spoofed website.

VI. HOW TO PREVENT PHISHING ?

We can prevent phishing attacks by taking care of following such things.

A. ***Phishing emails share common signs :*** Most phishing emails can be easily export by looking for just a few singns such as --, !, STOP etc. phishing emails share common signs. If you find more than two signs it may be a sing of phishing attack.

B. ***Weren't expecting email :*** If you receive email which you weren't expecting it means something goes wrong, in that situation never open email or do not click on any link without confirming the actual message.

C. ***Mentioned urgent matter :*** If you receive email in which mentioned urgent matter such as "So and so person require urgent help or reply immidiately" then do not reply in hurry or never be excited to reply.

D. ***Emails from a business but using a free account:*** If you receive emails for some job opportunities with good salary offered and asked to deposit some amount first than always check the account used for email. For example if free account used such as Gmail, Yahoo, Hotmail, etc. than beware it may be face because most of business organizations are using their own purchased domain and it is common now, so do not reply such fake emails.

E. ***Spelling and gramatical errors :*** If you found some spelling and gramatical errors in received email than it may be a fake email.

F. ***Asking for your money or Personal Information :*** If you receive email that is asking some money for any reason or if it asks for personal information than never ever share any of your personal details to prevent phising attack.

G. ***Part of longer conversation you weren't part of :*** If email received that showing you as a part of longer conversation whereas you weren't part of than do not reply.

H. ***You won a contest you didn't enter:*** If it says that you win a contest that you didn't entered or may be it offers link to fix a problem or claim your prize that means it's a trap to get your personal details and if you click on link that doesn't go where it says that it should be a fake email.

I. ***From someone famous or important :*** If you receive emails from someone famous or important such as celebrity it clearly indicates someone is trying to cheat you.

VII. REFERENCES

[1] https://whatis.techtarget.com/definition/phishing-kit
[2] https://www.incapsula.com/web-application-security/phishing-attack-scam.html
[3] https://en.wikipedia.org/wiki/Phishing
[4] https://cofense.com/phishing-threats/