PHISHING

Pranit R. Thite[1], Ganesh Suryawanshi[2], Prof.A.M.Ingole[3]

[1]*Student, Dept. of Computer Engineering, BVCOEL Pune, Maharashtra, India*
[2] *Student, Dept. of Computer Engineering, BVCOEL Pune, Maharashtra, India*
[3] *Professor, Dept. of Computer Engineering, BVCOEL Pune, Maharashtra, India*

---***---

Abstract - *Phishing is a try to get sensitive information such as usernames, passwords, as well as credit card information often for hateful reasons, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are usually used to lure naive victims. Phishing emails can contain links to websites that are contaminated with malware. Phishing is normally carried out by email spoofing or direct messaging, and it repeatedly directs users to enter details at a fake website which are looking and there feel are almost equal to the genuine one. Phishing is an example of social engineering techniques used to trick users, and exploits the unfortunate usability of current web security technologies. Tries to deal with the increasing number of reported phishing attacks include legislation, user training, public awareness, and technical security measures. Many websites have now builded resultant tools for applications, like maps for games, but they should be clearly marked as like who created them, and users should not use the identical passwords anywhere on the internet.*

Key Words: Phishing, Link Manipulation , Web Trojans , Man-in-the-Middle , Webside Forgery.

1.INTRODUCTION

In the field of computer security, Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a fraudulent e-mail that attempts to get you to divulge personal data that can then be used for illegitimate purposes.

There are many variations on this plan. It is likely to Phish for other information in accompaniments to usernames and passwords just like as credit card numbers, bank account numbers, social security numbers and mothers' maiden names. Phishing shows direct risks with the use of stolen credentials and indirect risk to institutions which conduct business on line through corrosion of customer confidence. The harm caused by Phishing ranges from denial of access to e-mail to large financial loss.

There are several different techniques to fight Phishing, including legislation and technology created purposely to protect against Phishing. No single technology will fully stop Phishing. However a combination of good organization and practice, proper function of current technologies and improvements in safety of technology has the potential to severely reduce the prevalence of Phishing and the losses suffered through it. Anti-Phishing software and computer programs are designed to reduce the occurrence of Phishing and trespassing on private information. Anti-Phishing software is designed to track websites and observe activity; any doubtful behavior can be automatically reported and even reviewed as a report after a period of time.

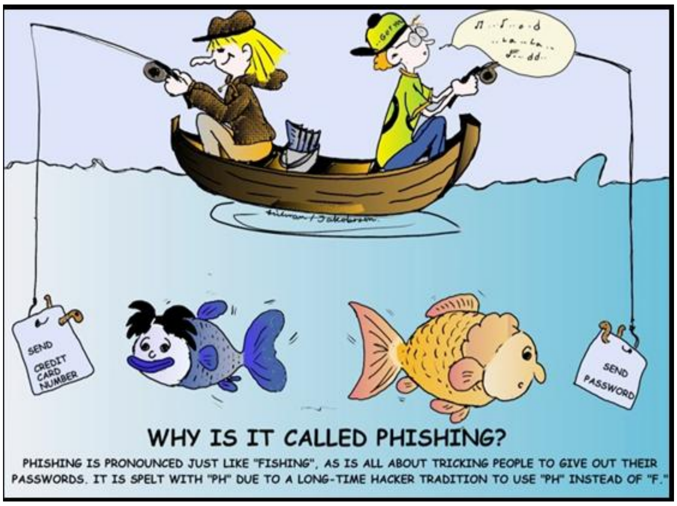
SEND CREDIT CARD NUMBER
SEND PASSWORD
WHY IS IT CALLED PHISHING?
PHISHING IS PRONOUNCED JUST LIKE "FISHING", AS IS ALL ABOUT TRICKING PEOPLE TO GIVE OUT THEIR PASSWORDS. IT IS SPELT WITH "PH" DUE TO A LONG-TIME HACKER TRADITION TO USE "PH" INSTEAD OF "F."

Fig 1. Phishing

One of the primary and important goals of phishing is to illegally carry out fraudulent financial transactions on behalf of users using a fake email that includes a URL pointing to a fake web site masked as an online bank or a government entity. A phisher may attract a victim onto giving his/her Social Security Number, full name, & address, which will then be used to apply on a credit card on the behalf of victim. Attacker uses copy of original website as a bait that is send to the user. When user grabs the attraction by filling and submitting his useful information attacker pulls the bait means saves the data for its own illegal use.

1.1 Flow of Phishing

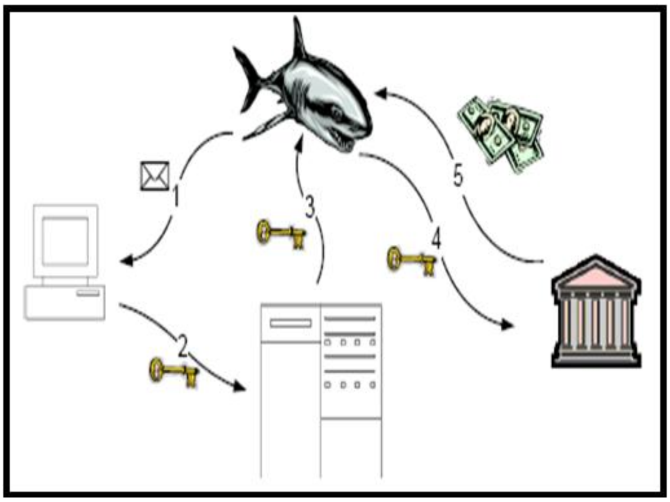

Fig 2. Flow of Phishing

1. A illusory message is sent from the Phishers to the user.

2. A user provides secret information to a Phishing server (normally after some interfaces with the server).

3. The Phisher obtains the confidential information from the server.

4. The confidential information is used to mimic the user.

5. The Phisher obtains illegal economic gain.

1.2 Process of Phishing

In general, phishing attacks are performed with the following four steps:
1) A fake web site which looks exactly like the valid Web site is set up by phisher
2) Phisher then sends a link to the fake web site in large amount of spoofed e-mails to target users by the name of genuine companies and organizations, trying to promote the likely victims to visit their web sites.
3) Victims visit the fake web site by clicking on the link and give their useful information.
4) Phishers then takes the personal information and perform their fraud such as transferring money from the victims' account.

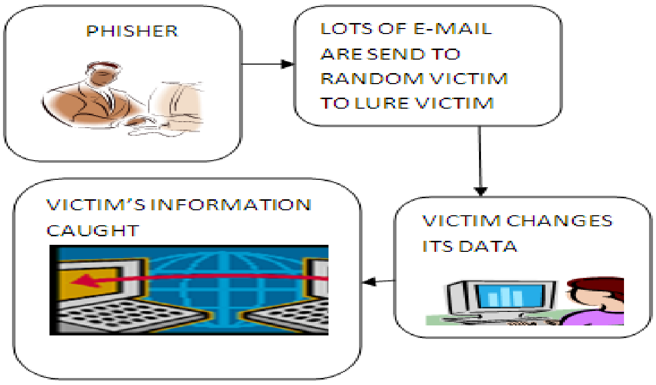
PHISHER
LOTS OF E-MAIL ARE SEND TO RANDOM VICTIM TO LURE VICTIM
VICTIM CHANGES ITS DATA
VICTIM'S INFORMATION CAUGHT

Fig 3. Process of Phishing

2. PHISHIG TECHNIQUES

Phishers use a broad variety of techniques, with one common thread.

2.1 Link Manipulation

Most types of Phishing use some form of technical deception designed to make a link in an e-mail like appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are the common tricks used by Phishers. In the following example, http://www.yourbank.example.com/, it appears as though the URL will take you to the *example* section of the *yourbank* website; actually this URL points to the "*yourbank*" (i.e. Phishing) section of the *example* website. An old method of spoofing is like links containing the '@' symbol, originally intended as a way to include a username and password. For example, http://www.google.com@members.tripod.com/ might deceive a casual observer into believing that it will open a page on www.google.com, whereas it actually directs the browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied.

2.2. Filter Evasion

Phishers have used images instead of text to make it harder for anti-Phishing filters to detect text commonly used in Phishing e-mails.

2.3. Webside Forgery

Once a victim visits the Phishing website the deception is not finished. Some Phishing scams also use JavaScript commands in order to reduce the address bar. This is done either by placing a picture of a legitimate URL on the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

2.4. Phone Phishing

Messages that are claimed to be from a bank that tell users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the Phishers) was dialed, prompts tell users to enter their account numbers and PIN. Vishing (voice Phishing) sometimes uses fake caller-ID data to give the appearance that the call has came from a trusted organization.

3. TYPES OF PHISHING

3.1 Deceptive Phishing

A phisher sends bulk email with a message. Users are inclined to click on a link. Examples: An email stating that there is a problem with recipient's account at financial institutions and requesting the recipient to click on a website link to update his details. A statement may be sent to the recipient stating that his account is at danger and offering to enroll him to an anti-fraud program. In any of the case, the website collects the user's confidential information. The phisher will subsequently mimic the victim and transfer finances from his account, buy merchandise, take a second advance on the victim's house or cause any other injure. In most of the cases, the phisher does not directly cause any economic damage, but he sells the illegally obtained information on a secondary market.

3.2 Malware-based Phishing

Malware-based phishing includes running spiteful software on the user's machine. The malware can be introduced as an email attachment or as a downloadable file exploiting security vulnerabilities. This is a particular risk for small and medium businesses (SMBs) who fails to update their their software applications.

3.3 Keyloggers and Screenloggers

Keyloggers and screenloggers are varieties of malware that track input from the keyboard and send relevant information to the hacker through the Internet. They can set in themselves into the user's browsers as small service programs.

3.4 Session Hijacking

Session Hijacking is a type of phishing attack where user's activities are monitored visibly until they log into a target account like the bank account and set up their credentials. At that point, the malicious software takes control and can undertake illegal actions, such as transferring funds, without the awareness of the user.

3.5 Web Trojans

Web Trojans pop ups when the users tries to log in to an important website or performing any transaction. These web trojans are unseen to the users. They collect user's credentials locally and broadcast them to the phisher.

3.6 Hosts File Poisoning

When a user types a URL of a website it is first translated into an IP address before it is transmitted on the Internet. The mass of user's PCs running a Microsoft Windows operating system first look up at these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. Phishers pinch information by "poisoning" the hosts file. They transmit a false address, taking the user accidentally to a fake "look alike" website.

3.7 System Reconfiguration Attacks

This is a type of phishing attack where the settings on a user's PC are customized with terrible intentions. For example: URLs in a favorites file might be customized to direct users to bogus websites that look similar For example: a financial institution's website URL may be changed from "bankofxyz.com" to "bancofxyz.com".

3.8 Data Theft

Malicious code running on a user's computer, can directly pinch private information stored on the computer. This information can be like activation keys to software, passwords, sensitive and personal email and any other data that is stored on the victim's computer. Data theft is also broadly used for phishing attacks meant at corporate espionage. In addition, confidential memos, design documents or billing information can be publicly leaked, causing embarrassment or financial damage to the organization. This information can also be leaked to competitors.

3.9 DNS-Based Phishing

Domain Name System (DNS)-based phishing or hosts file alteration is called Pharming. The requests for URLs or name service revisit a bogus address and successive communications are directed to a fake site when the hackers interfere a company's host files or domain name. As a result, users remain unconscious about the fraud website controlled by hackers.

3.10 Content-Injection Phishing

Content-injection phishing means inserting hateful content into a legitimate website. The malicious content can redirect to other websites or may install malware on a user's computer and also insert a frame of content that will redirect data to the phishing server.

3.11 Man-in-the-Middle Phishing

Man-in-the-Middle Phishing is somewhat hard to detect than many other forms of phishing. In these attacks hackers sit between the user and the website or the system. They record all the information that is being entered by the user but continue to pass the user onto the next steps so that user transactions are not affected and the user remains unaware. And Later on, they sell or use the information which may be credentials, credit card details, and bank account details.

3.12 Search Engine Phishing

Phishers develop e-commerce websites with striking offers. Later these sites are indexed legally with different search engines. When users search for any products or services, these sites are shown to the users by the search engine and are fooled into giving up their information. For example, scammers have set up false banking sites that offer lower credit costs or better interest rates than other banks. Victims are often encouraged to transfer account details. In this way, they are deceived into giving up their details.

4. CONCLUSIONS

As a future Software Engineer, it is essential that we know about phishing because in future we will be developing the several different systems and websites on our own and we must implement different security measures for protections against phishing

ACKNOWLEDGEMENT

I am thankful to Prof. A.M. INGOLE SIR from BVCOEL who took many efforts , guided me at every instant and provided all necessary information that I required to publish this paper successfully.

REFERENCES

1. http://m.in.techradar.com/news/software/Mobile-Phishing-How-to-avoid-getting-hooked/articleshow/38853630.cms
2. http://www.innovateus.net/science/what-are-different-types-phishing-attacks
3. https://en.wikipedia.org/wiki/Phishing
4. https://en.wikipedia.org/wiki/Phishing