

NETWORK SECURITY SHIELDING PHISHING ATTACKS

E.Ramkannan, Dr.L.Vigneshwaran
Research Scholar, Assistant Professor,
Department of Information Technology,
Jawaharlal Nehru University, New Delhi, India.

ABSTRACT

“PHISHING” is now the word which terrifies the mind of everyone and is also the word which is mostly on discuss in today’s network world because billions of money of millions of people and industries have been lost and the hunt still continues still more worse. This paper is going to deal with the basic ways of traps used by the phishers, their intentions, their strengths and the ways of defending, blocking or protecting us from these attacks.

INTRODUCTION

Phishing is the word which is toping the list of cyber crimes as this is the starting crime which leads to all other cyber crimes.

HISTORY

Even though the word phishing is of great use and its importance is discussed now, the first idea of phishing has aroused in 1987 November in a paper presented to International HP user group. This paper has covered all the techniques and heaviness of the adverse effects of this. But the name “*Phishing*” was first printed by the magazine “*The Hackers*” in 1993. The first recorded mention of the term “phishing” is on the alt.online-service. America- online Usenet newsgroup on January 2, 1996.

Definition

The word phishing is commonly defined as *“the act of getting others personal identity data (like passwords and id numbers) to access others private data and accounts by unauthorized use of reputed concerns or industries’ name and trade marks”*.

Persons who have fallen into the traps of phishers may lose their bank accounts money if he is a banker or lose all his private and secured data. This leads to more severe effects when the attack is on MNCs, banks and industries.

WAYS OF PHISHING

The three common ways of phishing done are,

- **E-MAIL PHISHING**
- **SOFTWARE PHISHING**
- **PHONE PHISHING**

All these three types of phishing cleverly trap the user and phish their passwords or private datas easily.

I. E-MAIL PHISHING

The e-mail phishing was the first phishing method followed by the phishers which was a great success for them. Many billions of money and still more valuable datas were looted.

Definition

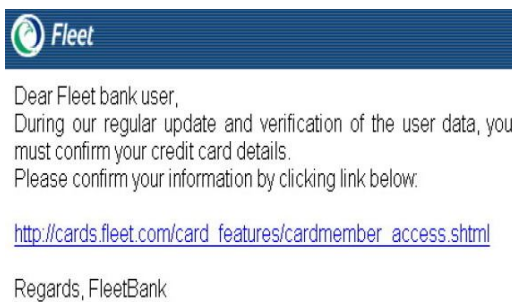
The e-mail phishing can be exactly defined as, *“ The act of sending an e-mail to a user*

falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information."

WORKING OF E-MAIL PHISHING

The techniques which trap the users into phishing through e-mail is that a mail is sent to a e-mail id stating that it is from your bank or any legitimate company asking to give your details to the link provided below which is fraudulent. If the user clicks this phishing link, his details will be snatched by the phishers and all his datas and accounts will be accessed by them.

The phishing mails looks like the mail below.



This is a phishing mail sent to hundreds of customers. The mail reads as to update the bank record with the users' details. So by seeing the banks name and symbol, if the user clicks the link given then he has fallen into the trap of the phishers. This takes the user to

some other phishing site which is not related to the bank. So all the datas of the customer will be seized and his account will be trespassed by the phishers.



CREDIT CARD PHISHING

The main danger in the e-mail phishing is that if the phisher succeeds in getting the victims credit card number, then he can loot the entire money in his account using a false credit card using his secret number acquired. Even though the law has enforced a severe punishment of \$10000 and imprisonments, the hunt still continues and many customers are loosing millions of hard earned money everyday due to mere lack of awareness about phishing activities.

TECHNIQUE USED IN E-MAIL PHISHING

LINK MANIPULATION

The main technique used in the e-mail phishing is link manipulation i.e. changing the linking keywords. **For example**, if a bank URL of a bank called "your bank" is like, <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 website) section of

the *example* website. So it easily fools you to surrender your details to them.

RATE OF INCREASE IN PHISHING MAILS SENT



WAYS TO PROTECT YOURSELVES FROM E-MAIL PHISHING

- Keep the e-mail id and passwords secured
- Do not give e-mail ids to strangers
- If any mail comes in the name of bank or company, and if you have any doubt in them contact the concern directly and enquire
- Do not click any peculiar links in your mails.

II. SOFTWARE PHISHING

Software phishing is another way of phishing which is now very prevalent in the network world.

Definition

The software phishing may be defined as, *"the way of stealing the users personal details if he mistakenly downloads the malware software designed by the phishers . These softwares will be found all over the network and when*

downloaded by any user steals all his private datas."

The adverse effect of downloading phishy software is similar to that of clicking the link of phishy mail. Both of them easily steal all the private datas of the user.

WAYS TO PROTECT YOURSELVES FROM SOFTWARE PHISHING

The ways to protect from software phishing is simple.

- Do not visit any strange or peculiar websites.
- Do not download unnecessary freeware softwares.
- Have strong spyware and malware detectors which prevent or warn you from these softwares.

III. PHONE PHISHING

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. *"Vishing"* (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

WAYS TO PROTECT YOURSELVES FROM PHONE PHISHING

- Do not give your private datas over phone

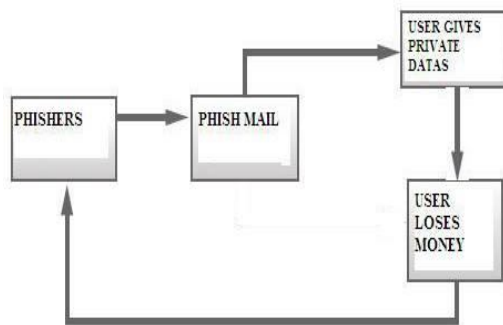
- Use caller id to trace the number and find if it is from the trusted company or bank.

- 5) The money of the victim has to be transferred to his account.

BLOCKING PHISHING

This world threatening cyber crime has to be stopped. Even though completely blocking it is difficult, we can reduce its effect by many ways.

Basically phishing takes place as,



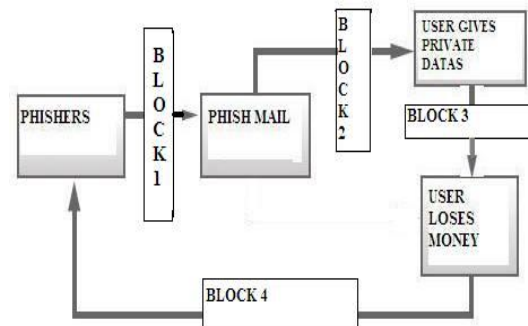
For a phisher to be successful in his hunt, 5 steps has to take place correctly,

- 1) The phishing mail has to be sent to the correct bunch of people.
- 2) The user has to click the phishing link give in the mail.
- 3) The user has to trust the boggy website and give his datas.
- 4) The user account has to be accessed by the phisher carefully.

BLOCKS

So a block can be kept to stop the phisher at any step and prevent him from moving further by which the phishing may be reduced.

The four effective places of introducing block is given in the figure below,



BLOCK 1 – RECLAIM MAIL

This is the first and most effective block which aims to prevent the phish mails from entering the users mail. This can be done by the server which can be made to reclaim unsigned mails from delivering.

BLOCK 2 – BLOCK PHISH SITES

This is the next stage in blocking. Even if a phishy mail has entered the user’s inbox, the phishing site which the mail leads can be blocked. This will save the user from becoming a victim. If all the phishing websites found are blocked, most of the users can be saved.

BLOCK 3 – AUTHENTICATE USER

Even after the user has fallen in the trap of phishing, the bank or concern can take necessary action to block the use of password or id of the victim. This can prevent some people from losing all their money.

BLOCK 4 – PROSECUTE

This is the final block for phisher to complete his hunt. Strict law enforcements have been passed to prevent bulk money transfer from victims account to a stranger's (Phisher) account. Every transaction has to be checked with care to save victims of phishing.

If these blocks function properly, it cannot stop phishing completely, but can greatly reduce the force or rate of phishing. Many victims can be saved as the phisher can slip in any one of these four blocks. This would save the customer for the company or bank. Because losing a customer is more of a loss for major companies and banks.

CASE STUDY

There are many companies and banks which faced heavy loss due to phishing. Here, we take two main companies which were the first to face the blow of phishing. They are,

I. eBay

eBay was the first company which was affected by phishing and faced a heavy loss. It got its first phishy mail in 1994.



A page like above appeared when the given link of the customers mail was clicked. Without knowing that the above page was fraudulent many filled and became a victim of phishing.

II. PayPal

PayPal is the other company which was nearly stunned by phishing. Billions of money was lost by the people of PayPal.



Dear valued PayPal® member:

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before **July 30, 2004**.

Once you have updated your account records, your PayPal® session will not be interrupted and will continue as normal.

To update your PayPal® records click on the following link:
<http://www.paypal.com/cgi-bin/webscr?cmd=login-run>

Thank You.
PayPal® UPDATE TEAM

This was the popular mail which was sent to thousands of people and hundreds of people fell in the trap and lost all their money.


The list of companies affected by phishing is in hundreds.

Many banks like “*Bank of America*”, “*CITY*”, “*AXIS*” and many many more banks have lost billions of dollars because of phishing.

STEPS TAKEN BY COMPANIES TO PREVENT PHISHING

Companies have taken various measures to differentiate between the original website and phishy fraudulent website.

IN FIREFOX

Firefox uses a red circle symbol  to denote that the website is not secure. So if a user sees a website with such a symbol, he should immediately close the website.



IN INTERNET EXPLORER 7

In Internet Explorer 7 there is a feature called “*phish filter*” which filters all the phishy websites and report them as phishing.

Many phishing websites has been found by this.



Internet explorer also has many tool bars which help to detect phishing sites. They are,

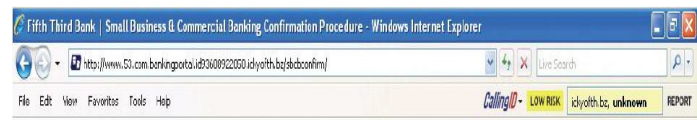


Figure 1: The CallingID Toolbar indicating a low-risk site.



Figure 2: The Cloudmark Anti-Fraud Toolbar indicating a legitimate site.



Figure 3: The EarthLink Toolbar indicating a legitimate site.

All these tool bars have a special key which identifies the phishing sites and warns the users from becoming victims.

DEFENCE

1. Do NOT follow links in suspicious emails, IM messages, or web pages.
2. Disable HTML viewing in your email client. View source (not HTML) to see if link is valid.
3. If it sounds too good to be true, it probably is.
4. Stop using Internet Explorer. Try Firefox or Mozilla instead.
5. Make sure your operating system and applications are current and patched for the latest security threats.
6. Install and update your virus protection regularly.
7. Never execute or install software from untrusted sources (including browser plug-ins and "enhancements", P2P networks, or email attachments).
8. By default be suspicious and skeptical.

CONCLUSION

The main problem with technology is that whenever it grows in positive side it equally grows in the negative side also. Even though phishing is a great threat to the network world, it will lose its power if the users have a clear awareness about what is phishing and how it works. There is no greater defense than knowledge about phishing. Thus this paper "*Shield Phishing Attacks*" has to its best explained about the phishing's working, types, effects and ways of shielding.

REFERENCES

- www.antiphishing.org
- www.nextgenss.com/papers/phishing
- www.securityfocus.com
- www.usdoj.gov
- www.indiana.edu/phishing
- www.internetnews.com
- www.phishgaurd.com
- www.theregister.uk
- www.openspf.org/whitepaper.pdf
- http://survey.mailfrontier.com/survey/phishing_uk.html