iJET EXPLORE International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 7, July, 2012

Prevention Approach of Phishing on Different Websites

Mayur Bhati, Rashid Khan
CSE, Jodhpur National University
Jodhpur

ABSTRACT

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 typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical. Such sites ask for personal information, including banking passwords or offer software downloads. This paper explains the method used for phishing prevention using secure USB Login technique to prevent phishing. This paper gives description about Hardware based locking method.

Keywords: *Phishing, Attacks, Strategies, USB Logins.*

1. INTRODUCTION

Phishing is an attempt by an individual or a group to harvest personal confidential information such as user names, passwords, credit card information, etc., from unsuspecting victims for identity theft, financial gain and other fraudulent activities. A phishing scam usually involves the phisher sending mass emails to intended victims and users replying to e-mails and in the process, divulging their personal information. Fake websites which appear very much similar to the original ones are being hosted to achieve this. Thus the users assume that they are entering information into a genuine website without realizing that they are giving away their precious information to a stranger who can misuse it for financial gains.

There is newer and more dangerous variation called "spear phishing." It's more insidious than regular phishing because the sender knows exactly who you do business with and what kind of accounts you have. The email they send is very convincing, appearing to come from a credit union, stockbroker or friend, so you're inclined to open it without hesitation. As soon as you realize you've opened one of these illegitimate emails, you need to assume that your sensitive information has been captured or is at risk.

1.1 How Phishing does Occur

The majority of phishing currently is conducted by email. In a typical phishing attempt, you will receive an authentic-looking email message that appears to come from a legitimate business; e.g., bank, online shopping site. It will ask you to divulge or verify personal data such as an account number, password, credit card number or Social Security number. Often the wording may try to scare you into providing information. For example, you might receive an email that appears to be from your bank asking that you click on a link in the message. This link might take you to a bogus Web site where you would be asked to verify your online banking information. Intimidating language might be included, e.g., "Your account will be closed or suspended if you don't follow these directions." Although legitimate online banking and e-commerce are very safe, you should always be careful about giving your personal financial information over the Internet. It is also possible for you to be phished by mail, telephone or even in person. The latest and most rapidly growing threat is through the use of Instant Messaging (IM), which can also be used for identity theft as well as spreading viruses and spyware.

1.2 How does a Phishing Attempt Look Like

A good number of phishing attempts make use of email to reach out to millions of possible victims. Such emails look very similar to the website of the company that these emails claim to be coming from.

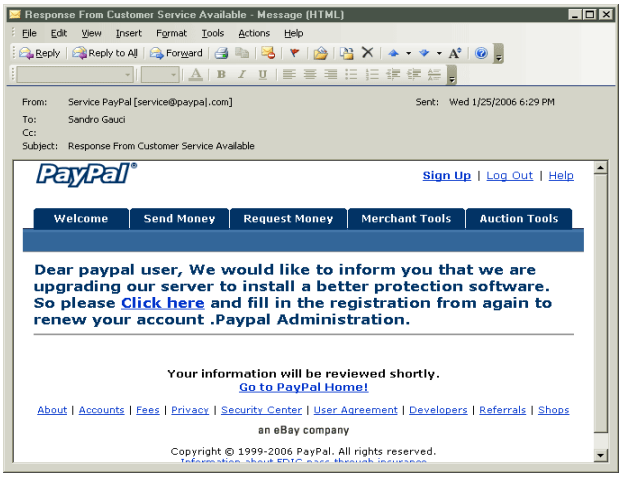

Fig 1: View of fake sites

To fool end-users, scammers make use of social attacks such as:

- Making use of logos and other trademark properties.
- The design of fraudulent email is copied from the legitimate website so that it looks exactly the same.
- The 'from' address in the email looks as though it is from a legitimate email coming from the legitimate company.
- Create a fake situation which requires user input – such as informing the victim that his/her account was compromised and asking him/her to confirm the account information.
- Sometimes attackers can also make use of technical attacks so that their emails look more authentic. One such attack is called URL spoofing, and allows hyperlinks which redirect to the attacker's site to appear as if the victim is sending the information to the correct web site.

1.3 Infected Areas

Popular targets are users of online banking services and auction sites such as eBay. If your email address has been made public anywhere on the Internet (e.g., posted on a forum, newsgroup or Web site), then you are more susceptible to phishing. Scammers can use spidering or Web-crawling programs to search the Internet and collect millions of email addresses.

2. APPROACHES

This section describes the various approaches of phishing. There are several (technical or non-technical) ways to prevent phishing attacks:

- Educate users to understand how phishing attacks work and be alert when phishing-alike e-mails are received.
- Use legal methods to punish phishing attackers.
- Use technical methods to stop phishing attackers.

2.1 Detect and Block Phishing Websites

If we detect the phishing Web sites in time, then we can then block the sites and prevent phishing attacks. It's relatively easy to (manually) determine whether a site is a phishing site or not, but it's difficult to find those phishing sites out in time. Here we list two methods for phishing site detection. 1) The Webmaster of a legal Web site periodically scans the root DNS for suspicious sites (e.g. www.1cbc.com.cn vs. www.icbc.com.cn). 2) Since the phisher must duplicate the content of the target site, he must use tools to (automatically) download the Web pages from the target site. It is therefore possible to detect this kind of download at the Web server and trace back to the phisher. Both approaches have shortcomings. For DNS scanning, it increases the overhead of the DNS systems and may cause problem for normal DNS queries, and furthermore, many phishing attacks simply do not require a DNS name. For phishing download detection, clever phishers may easily write tools which can mimic the behavior of human beings to defeat the detection.

2.2 Enhance the Security of the Website

The business Web sites such as the Web sites of banks can take new methods to guarantee the security of users' personal information. One method to enhance the security is to use hardware devices. For example, the Barclays bank provides a hand-held card reader to the users. Before shopping on the net, users need to insert their credit card into the card reader, and input their (personal identification number) PIN code, then the card reader will produce a onetime security password, users can perform transactions only after the right password is has entered. Another method is to use the biometrics characteristic (e.g. voice, fingerprint, iris, etc.) for user authentication. For example, PayPal had tried to replace the single password verification by voice recognition to enhance the security of the Web site. With these methods, the phisher cannot accomplish their tasks even after they have gotten part of the victims' information. However, all these techniques need additional hardware to realize the authentication between the users and the Web sites hence will increase the cost and bring certain inconvenience. Therefore, it still needs time for these techniques to be widely adopted.

2.3 Use of Spam Filters

Phisher generally use e-mails as 'bait' to allure potential victims. SMTP (Simple Mail Transfer Protocol) is the protocol to deliver e-mails on the Internet. It is a very simple protocol which lacks necessary authentication mechanisms. Information related to sender, such as the name and email address of the sender, route of the message, etc., can be counterfeited in SMTP. Thus, the attackers can send out large amounts of spoofed e-mails which are seemed from legitimate organizations.

The phisher hide their identities when sending the spoofed e-mails, therefore, if anti-spam systems can determine whether an e-mail is sent by the announced sender (Am I Whom I Say I Am?), the phishing attacks will be decreased dramatically. From this point, the techniques that preventing senders from counterfeiting their Send ID

(e.g. SIDF of Microsoft) can defeat phishing attacks efficiently. SIDF is a combination of Microsoft's Caller ID for E-mail and the SPF (Sender Policy Framework) developed by Meng Weng Wong. Both Caller ID and SPF check e-mail sender's domain name to verify if the e-mail is sent from a server that is authorized to send e-mails of that domain and from that to determine whether that e-mail use spoofed e-mail address. If it's faked, the Internet service provider can then determine that e-mail is a spam e-mail. The spoofed e-mails used by phisher are one type of spam e-mails. From this point of view, the spam filters can also be used to filter those phishing e-mails. For example, blacklist, whitelist, keyword filters, Bayesian filters with self learning abilities, and E-Mail Stamp, etc., can be used at the e-mail server or client systems. Most of these anti-spam techniques perform filtering at the receiving side by scanning the contents and the address of the received e-mails. They all have pros and cons as discussed below. Blacklist and whitelist cannot work if the names of the spammers are not known in advance. Keyword filter and Bayesian filters can detect spam based on content, hence can detect unknown spasm. But they can also result in false positives and false negatives. Furthermore, spam filters are designed for general spam e-mails and may not very suitable for filtering phishing e-mails since they generally do not consider the specific characteristics of phishing attacks.

2.4 Anti-Phishing Softwares

Despite all the above efforts, it is still possible for the users to visit the spoofed Web sites. As a last defense, users can install anti-phishing tools in their computers. The antiphishing tools in use today can be divided into two categories: blacklist/whitelist based and rule-based.

- Category I: When a user visits a Web site, the antiphishing tool searches the address of that site in a blacklist stored in the database. If the visited site is on the list, the anti-phishing tool then warns the users. Tools in this category include ScamBlocker from the EarthLink Company, PhishGuard, and Netcraft, etc. Though the developers of these tools have announced that they can update the blacklist in time, they cannot prevent the attacks from the newly emerged (unknown) phishing sites.

- Category II: this category of tools uses certain rules in their software, and checks the security of a Web site according to these rules. Examples of this type of tools include Spoof Guard developed by Stanford, Trust Watch of the GeoTrust, etc. Spoof Guard checks the domain name, URL (includes the port number) of a Web site, it also checks whether the browser is directed to the current URL via the links in the contents of e-mails. If it finds that the domain name of the visited Web site is similar to a well-known domain name, or if they are not using the standard port, SpoofGuard will warn the users.

3. PHISHING TECHNIQUES

This section shows various attempts and techniques by which a user can access the details of others

3.1 Phishing Attempts

Phisher are targeting the customers of banks and online payment services. E-mails, supposedly from the Internal Revenue Service, have been used to glean sensitive data from U.S. taxpayers. While the first such examples were sent indiscriminately in the expectation that some would be received by customers of a given bank or service, recent research has shown that phisher may in principle be able to determine which banks potential victims use, and target bogus e-mails accordingly. Targeted versions of phishing have been termed spear phishing. Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

3.2 Link Manipulation

Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phisher. Following URL, 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. Another common trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers' site. The following example link, http://en.wikipedia.org/wiki/Genuine, appears to take you to an article entitled "Genuine"; clicking on it will in fact take you to the article entitled "Deception". In the lower left hand corner of most browsers you can preview and verify where the link is going to take you.

An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password (contrary to the standard). 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. Such URLs were disabled in Internet Explorer, while Mozilla Firefox and Opera present a warning message and give the option of continuing to the site or cancelling.

A further problem with URLs has been found in the handling of Internationalized domain names (IDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing or homograph attack, phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain. Even digital certificates do not solve this problem because it is quite possible for a phisher to purchase a valid certificate and subsequently change content to spoof a genuine website.

3.3 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.

3.4 Other Techniques

Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information.

3.5 I.D. Hacking

It shows the various steps of I.D. hacking of a user. The fake user can execute the following steps:

Step1: Sent phishing mail

Step2: User access the link

Step3: Link will open the phishing site

Step4: User will access and send his user name and password

Step5: This will send user's password and I.D. to the phisher.

Step 6 and 7: Phisher will use his account information and misuse.

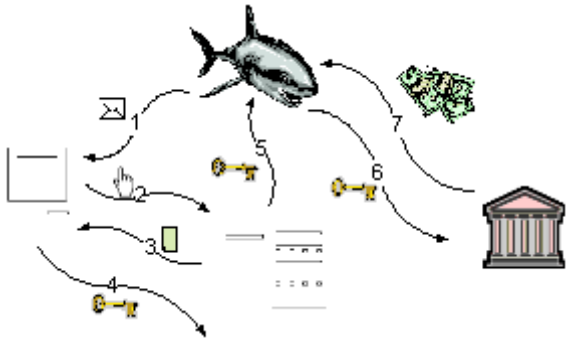

Figure 2: Graphical view of I.D. hacking

4. ANTI PHISHING

Phishing will stop if the majority of users are educated and know how to handle computers.There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing.

4.1 Social Responses

One strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback. One newer phishing tactic, which uses phishing e-mails targeted at a specific company, known as spear phishing, has been harnessed to train individuals at various locations, including United States Military Academy at West Point, NY. In a June 2004 experiment with spear phishing, 80% of 500 West Point cadets who were sent a fake e-mail were tricked into revealing personal information.

4.2 Technical Responses

Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

4.2.1 Helping to Identify Legitimate Websites

Most websites targeted for phishing are secure websites, meaning that SSL with strong cryptography is used for server authentication, where the website's URL is used as identifier. In theory it should be possible for the SSL authentication to be used to confirm the site to the user, and this was SSL v2's design requirement and the meta of secure browsing. But in practice, this is easy to trick. The superficial flaw is that the browser's security user interface (UI) is insufficient to deal with today's strong threats. There are three parts to secure authentication

using TLS and certificates: indicating that the connection is in authenticated mode, indicating which site the user is connected to, and indicating which authority says it is this site. All three are necessary for authentication, and need to be confirmed by/to the user.

4.2.2 Secure Connection

The standard display for secure browsing was the padlock, which is easily missed by the user. Mozilla fielded a yellow URL bar in 2005 as a better indication of the secure connection. Unfortunately, this innovation was then reversed due to the EV certificates, which replaced certain high-value certificates with a green display, and other certificates with a white display.

4.2.3 C lick-thru Syndrome

However, warnings to poorly configured sites continued, and were not down-graded. If a certificate had an error in it (mismatched domain name, expiry), then the browser would commonly launch a popup to warn the user. As the reason was generally misconfiguration, the users learned to bypass the warnings, and now, users are accustomed to treat all warnings with the same disdain, resulting in Click-thru syndrome. For example, Firefox 3 has a 4-click process for adding an exception, but it has been shown to be ignored by an experienced user in a real case of MITM. Even today, as the vast majority of warnings will be for misconfigurations not real MITMs, it is hard to see how click-thru syndrome will ever be avoided.

4.3 Legal Responses

On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected phisher. The defendant, a Californian teenager, allegedly created a webpage designed to look like the America Online website, and used it to steal credit card information. Other countries have followed this lead by tracing and arresting phishes. A phishing kingpin, Valdir Paulo de Almeida, was arrested in Brazil for leading one of the largest phishing crime rings, which in two years stole between US$18 million and US$37 million. UK authorities jailed two men in June 2005 for their role in a phishing scam, in a case connected to the U.S. Secret Service Operation Firewall, which targeted notorious "carder" websites. In 2006 eight people were arrested by Japanese police on suspicion of phishing fraud by creating bogus Yahoo Japan Web sites, netting themselves 100 million yen ($870,000 USD). The arrests continued in 2006 with the FBI Operation Card keeper detaining a gang of sixteen in the U.S. and Europe.

5. SECURE USB LOGIN

- In order to access account, user has to provide following required information:

1. Personal Identification Number (User ID)
2. Password
3. USB Lock (USB Device Provided by the Bank)

- Each user has its own unique USB Device for each account.

There are Following Steps in this Process:-

Step 1:
Connect to web page of online banking and input personal identification number ID, password and Plug-in that USB device which is provided by the respective Bank for Login.

Step 2:
After that Plugging, User inputs User_Id and Password. Then the computer will verify the client's information accompanied with USB device in Offline Mode.USB Device contains information related to user in Encrypted way. In verification process we use Encryption and Decryption algorithm for enhancing security. After that Successful verification of Offline process this information communicates with host computer of the bank for verification and authentication. In case of failure User will not be able to access the account.

Step 3:
In this process all information goes to host computer in encrypted way and at the host end, it verifies from the database and allow accessing the account and user can further proceed for Online Transactions.

Note: In this process USB Device is connected with the Client Computer, in the absence of this USB Device, User can't access the Account.

6. CONCLUSION

Phishing is an issue of increasing importance since everyone can be targeted and since the techniques used by phishers are more and more sophisticated. Moreover, the damage done can be enormous and the phishers are hard to catch. Therefore, without being an expert of information techniques, it is possible to implement some simple measures in the everyday life to strengthen protection when we are online. Learning to be suspect and getting the reflex of checking the truth of the information you might receive is important. Changing passwords often and being able to recognize signs of spoofed e-mails or website is also necessary. In order to improve the security on E-commerce transaction, application of information techniques and restriction from law would block the illegitimate transaction from happening. Users need to change him own habit to attend to personal information so as to make the online transaction more secure.

We believe that Secure USB Login is not only useful for preventing phishing attacks, but also can shield users from malicious or unsolicited links in Web pages and Instant messages. Our future work includes further extending the Secure USB Login approach.

REFERENCES

[1] I. Androutsopoulos, J. Koutsias, K.V. Chandrinos, and C.D. Spyropoulos. An Experimental Comparison of Naive Bayesian and Keyword- Based Anti-Spam Filtering with Encrypted Personal E-mail Message.In Proc. SIGIR 2000, 2000.

[2] Georgina Stanley. Internet Security - Gone phishing. http://www.cyota.com/news.asp?id=114.

[3] Berners-Lee, Tim. "Uniform Resource Locators (URL)". *IETF Network Working Group*. http://www.w3.org/Addressing/rfc1738.txt. Retrieved January 28, 2006.

[4] Ian Fette, Norman Sadeh, and Anthony Tomasic. Learning to detect phishing emails. In *ACMInternational conference onWorldWideWeb (WWW)*, 2007.

[5] Tyler Moore and Richard Clayton. An Empirical Analysis of the Current State of Phishing Attack and Defence. In*Workshop on the Economics of Information Security*, 2007.

[6] "Phishing". *Word Spy*. http://www.wordspy.com/words/phishing.asp. Retrieved September 28, 2006.

[7] A. Herzberg and A. Gbara, "Protecting Naive Web Users," Draft of July 18, 2004.

[8] "APWG - Phishing activity trends: Report for December 2007," http: //www.antiphishing.org /reports/apwg report dec 2007.pdf, 2007.