ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (111-118), Month: January - March 2015, Available at: www.researchpublish.com

Phishing Mitigation: The Effect of Using Attack-Based Understanding Techniques

[1]A.E. DUROSIMI, [2]D.W.S. ALAUSA

[1]Information & Communication Technology Unit, The Federal Medical Centre, Abeokuta. Ogun State, Nigeria
[2]Department of Computer Engineering, the Federal Polytechnic Ilaro, Ogun State. Nigeria

Abstract: **Most internet users have encountered series of electronic deception (Phishing) in form of e-mails originating from malicious source and made to persuade the recipient to hand over personal information such as credit card details. These criminals often pose as ones bank or financial institution employer or any other entity you normally trust with your information. These phishing crimes can be solved using HTTPS, which is a more secure protocol than HTTP as it encrypts your browser and all information sent or received. Also, the use of firewall prevents many browser hijackers and effective against virus attacks. Thus users can secure their confidential information from phishing attacks by checking that the padlock appeared on the top or bottom of the webpage before entering login details, which shows that users are communicating with the real website.**

Keywords: **Phishing, fraud, detection, E-mail.**

1. INTRODUCTION

Phishing is a form of electronic deception where an individual is persuaded to perform actions or divulge information by an attacker impersonating a trustworthy entity. Most Internet users have encountered phishing in the form of emails purporting to come from a bank or other business, but in fact originating from a malicious source and designed to persuade the recipient to hand over personal information such as credit card details[1]. Phishing scams normally occur via emails, websites, text messages and phone calls that can delude recipients' to think that Christmas came early. Cybercriminals will often pose as your bank or financial institution, your employer, or any other entity that you normally trust with your information. Only when the email phishing process and characteristics are fully understood can effective measures be designed against phishing attacks. Successful phishing attacks are based on a form of copying, or reengineering, a website's design and layout in order to pass themselves off as a genuine (targeted) website. A malicious website is crafted which looks and feels like the original site, convincing unsuspecting users that they are giving personal information to a trusted organization**.** Users are frequently drawn to the sites by forged emails designed to look like legitimate correspondence and may even copy the body from real email, but when the user clicks a link to visit the website, they will be directed to the malicious site instead. The more convincing a phishing attack appears - or rather, the more genuine a malicious website looks - the more success the attack will have in extracting personal information. Some phishing attacks go so far as to create faux websites for which there is no legitimate counterpart; e.g. a page prompting users for personal information the organization wouldn't have otherwise asked for. According to Anti-Phishing Working Group (APWG), phishing activities have been increasing and most phishing websites are hosted in the US. In 2012, averages of over 25,000 unique phishing email reports were reported to the APWG. Plus, the number of unique phishing sites detected exceeded 45,000 per month [2]. Financial services and payment services are common targets for phishing fraud but also stated in the report is a 12% hike in reports of phishing in online games.

1.1 Steps In Phishing Attack:

All phishing attacks fit into the same general information flow.

The steps are:

1. User receives deceptive email messages that appear to be sent from a legitimate source, such as a business partner, that

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (111-118), Month: January - March 2015, Available at: www.researchpublish.com

contain an explicit request to verify account information with a web service, without which the account will be suspended.

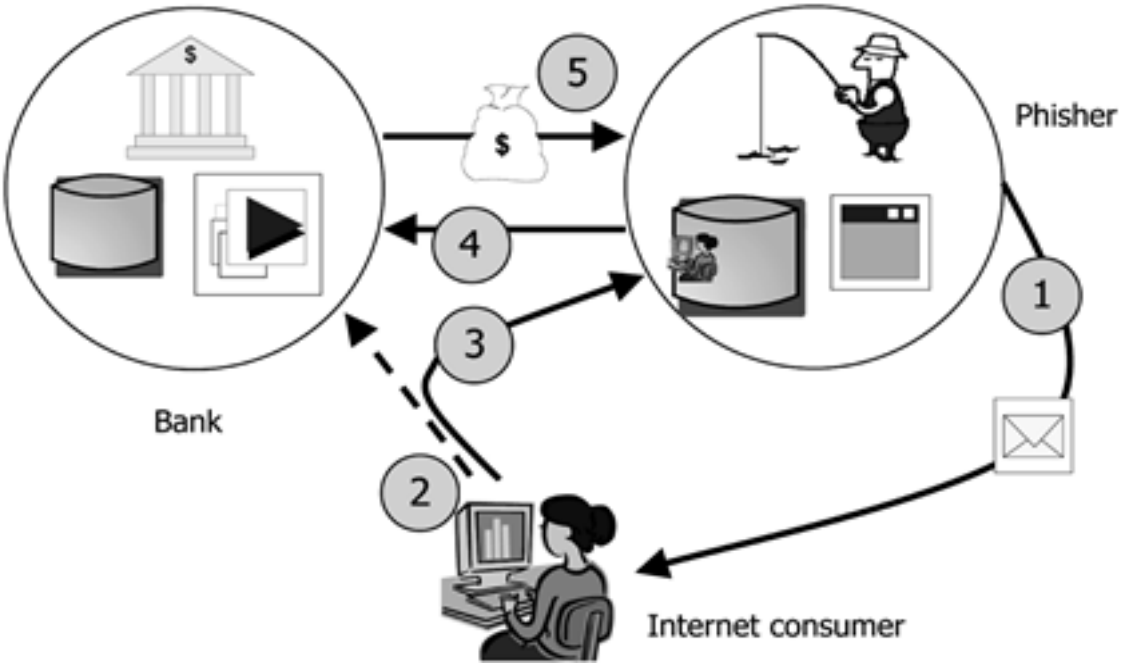


Fig. 1: Typical Phishing Scenario

2. Users are encouraged to visit fake websites that can be similar in appearance to legitimate sites. When a user visits the compromised website, malicious software can be downloaded automatically to his computer. Typically, the malware installed records the credentials used by the users to access to target services (e.g., banking), sending them to the command and control servers managed by the attackers.
3. User receives messages from false charities that request direct donations in cash.
4. Users of a social network platform receive messages, apparently from the platform, that contain a link leading them to a compromised website. The compromised website could download a malicious application onto the victim's machine to steal sensible information or it could offer a web form that appears to belong to a legitimate site that request authentication data. This form of phishing is also known as social phishing.
5. Users receive phone calls that claim to originate from legitimate organizations or private businesses and that ask him to dial a phone number because of problems with his bank accounts or other services. When the user calls a phone number that is managed by the attacker, it prompts said user to enter his account numbers and authentication code. Vishing (voice phishing) in many cases uses fake caller ID data to trick the user about the real origin of the call.

2. PHISHING TECHNIQUES

There are a number of different phishing techniques used to obtain personal information from users. As technology becomes more advanced, the phishing techniques being used are also more advanced. To prevent Internet phishing, users should have knowledge of various types of phishing techniques and they should also be aware of anti-phishing techniques to protect themselves from getting phished. Let's look at some of these phishing techniques.

2.1 E-Mail Phishing:

Phishers may send the same email to millions of users, requesting them to fill in personal details. These details will be used by the phishers for their illegal activities. Phishing with email and spam is a very common phishing scam. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, and verify accounts. Sometimes, they may be asked to fill out a form to access a new service through a link which is provided in the email

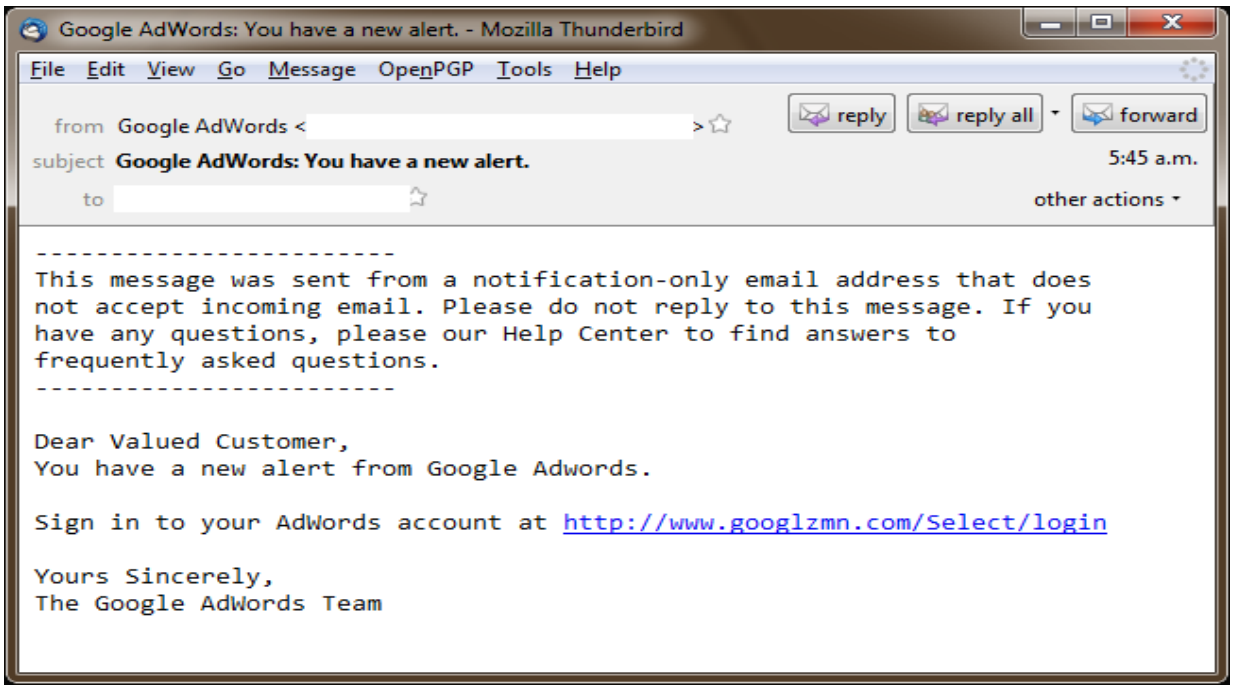
ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (111-118), Month: January - March 2015, Available at: www.researchpublish.com

a. For those of you who have a Google Ad Words account, be wary of a new Google Ad Words spam campaign we have seen in-the-wild earlier this week. The spam email may use the following subject lines:

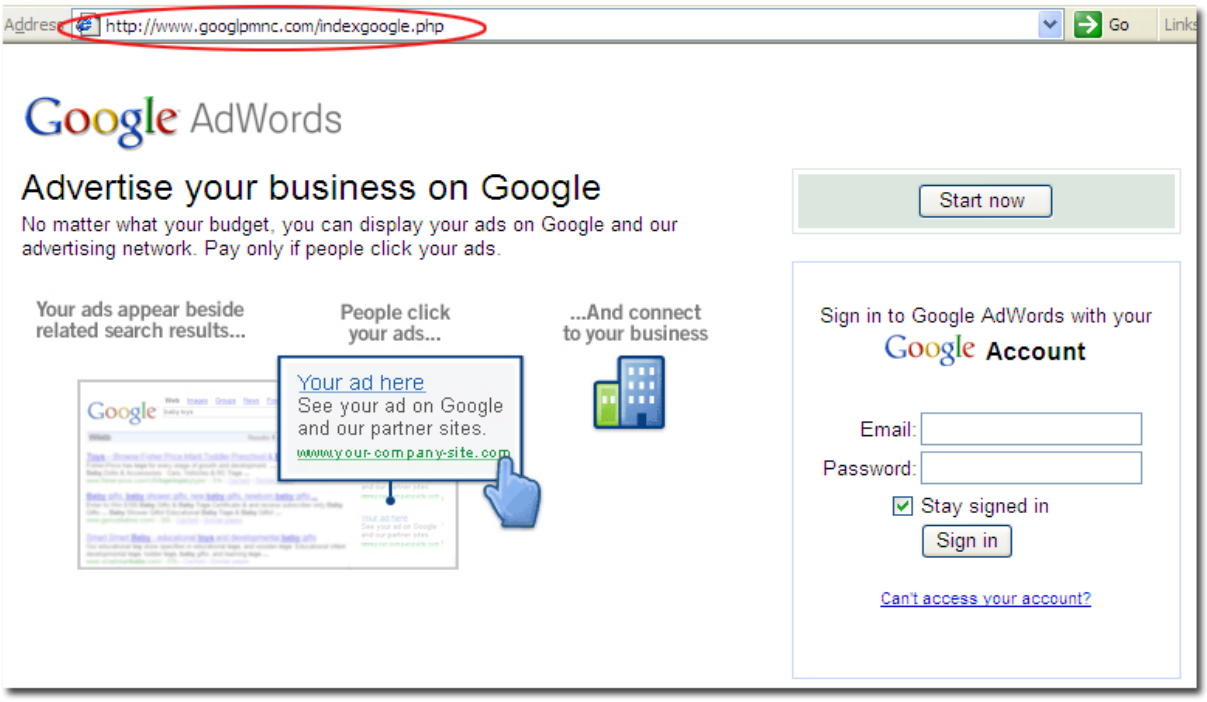
Google Ad Words: You have a new alert.

Google Team: You have a new alert

Here is an example of the spam email posing as a notification email from Google AdWords.

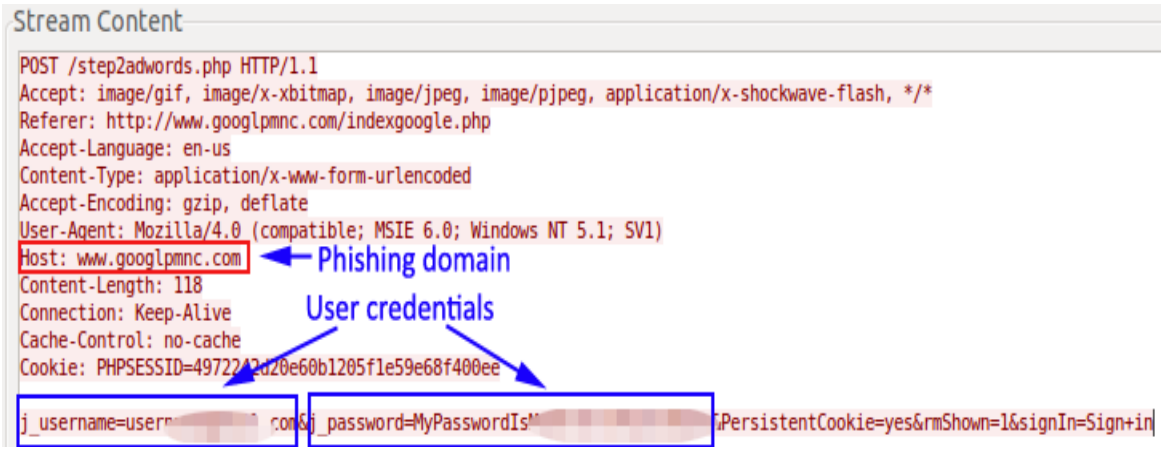


If you notice in the sample email, the URL link that appears to be linking to your Adwords account looks dodgy. But if that obvious sign didn't prevent you from clicking the link, you would have been redirected to a Google AdWords phishing webpage.



After entering a username and password, the webpage sends these credentials to the cyber-criminal's web server.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (111-118), Month: January - March 2015, Available at: www.researchpublish.com



The HTTP POST request when the user enters their Google account credentials. It sends the username and password to the phisher's webpage.

Of course, once you enter your Google account credentials in the phishing page this will NOT just compromise your Google AdWords account but all your Google services like GMail or Google+ will be affected as well. When you receive these sorts of notification emails, always double check the URL before you click on them – if it looks suspicious, it probably is [4].

b. Recognizing Scam Messages & Other Useful Information

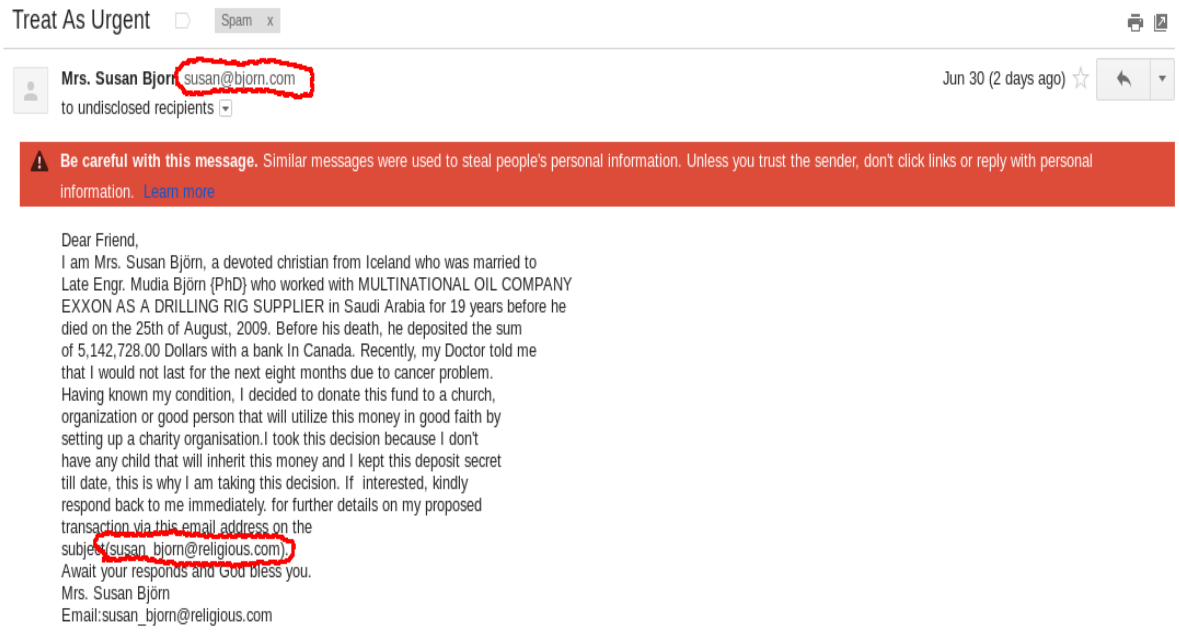
'From Address' Doesn't Match Reply Address

Pay attention to the 'From" field of an e-mail address & compare it to e-mail addresses provided in the body of the message.

Messages requesting that you reply to a different e-mail address from the original, should be considered highly suspicious.

E-mail messages coming from free e-mail services, claiming to be from a reputable business, are typically Scams. (Examples: AOL, hotmail, gmail, etc.)

Legitimate e-mail messages, from businesses and organizations, usually come from official e-mail accounts. (Examples: person@yourbank.com or someone@officialorganization.com.)[6]



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (111-118), Month: January - March 2015, Available at: www.researchpublish.com

2.2 Social Network Phishing:

The rise of social networks has given phishing new life. After all, social networks are all about sharing. It's not at all unusual for a friend to post a link to a nifty article, so users are less likely to be skeptical, and more likely to click on a phishing link.

That's the bad news. The good news is that phishing on social networks usually isn't as severe. Usually, the deception will be something like the recent Steve Jobs' death scams which are simply looking to harvest email addresses or send people to affiliate links. You might be annoyed by additional spam, but that's it.

Still, some of these attacks can be fairly harmful. Banks have Twitter feeds and Facebook pages too, and fake ones can be used to try and lure users to forged websites, just like a bogus email. These accounts can be hacked, too. The Bank of Melbourne experienced this, although as is often the case with phishers, the messages sent by the compromised account weren't of high enough quality to fool many people [5].

Phishing on social networks can be combated the same way as phishing through email. Security software and extensions can help. You can also use a link preview extension to see if an abbreviated link is sending you where it claims.

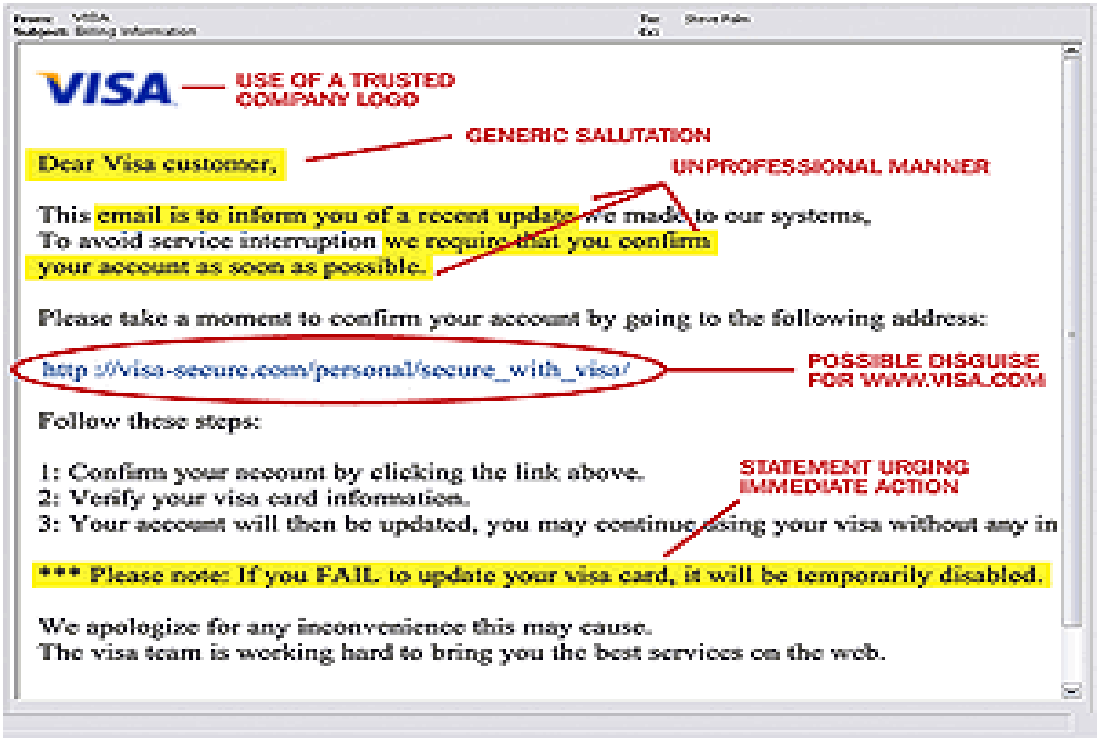
2.3 Deceptive Phishing:

A phisher sends bulk email with a message. Users are influenced to click on a link.

Examples: An email stating that there is a problem with recipient's account at financial institutions and requests 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 risk 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 impersonate the victim and transfer funds from his account, purchase merchandise, take a second mortgage on the victim's house or cause any other damage. In most of these cases, the phisher does not directly cause any economic damage, but sells the illegally obtained information on a secondary market.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (111-118), Month: January - March 2015, Available at: www.researchpublish.com

Below is an example of deceptive phishing



Be aware when submitting personal or financial information on Web sites. Before submitting financial information through a Web site, look for the "padlock" icon on your browser's status bar. This signals that your information is secure during transactions. To make sure you are on a secure Web server, check the beginning of the Web address in your browser's address bar. It should read https://, rather than just http://.

Look for misspelled words. Misspelled words either in the message, hyperlink or Web site often signal 'brand spoofing' scams. Leave suspicious sites. If you suspect that a Web site is not what it claims to be, leave the site immediately. Do not follow any of the instructions it presents [8].

2.4 Malware-based Phishing:

Malware-based phishing involves running malicious 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 threat for small and medium businesses (SMBs) who fails to update their software applications.

2.5 Session Hijacking Phishing:

Session Hijacking is a kind of phishing attack where user's activities are monitored clearly until they log into a target account like the bank account and establish their credentials. At that point, the malicious software takes control and can undertake unauthorized actions, such as transferring funds, without the knowledge of the user.

2.6 Hosts File Poisoning Phishing:

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

2.7 System Reconfiguration Attacks:

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

2.8 DNS-Based Phishing:

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

2.9 Content-Injection Phishing:

Content-injection phishing means inserting malicious 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. MITIGATING PHISHING

3.1 HTTPS instead of HTTP:

HTTPS is a more secure protocol than HTTP as it encrypts your browser and all the information you send or receive. If you are looking to make online payments or transactions, opt for an HTTPS website. Such HTTPS websites are equipped with SSL (secure socket layer) that creates a secure channel for information transition [2].

3.2 Website Reliability:

With Phishing, hackers can create a similar website with a normal-looking login page where users enter login details or even credit card details. Therefore, before entering login details users has to check the padlock appeared on the top or bottom of webpage.

It indicates that user is communicating with the real website. Many websites have EV (extended validation) SSL certificates that turn address bars into a green bar so users easily get idea about authenticate websites.

3.3 Hyperlink in Email:

Never click hyperlinks received in emails from an unknown or unverified source. Such links contain malicious codes and you be asked for login details or personal information when you reach the page you are led to from the hyperlink.

Always run a search of the association's name and click in from the search results.

3.4 Firewall:

With a firewall, users can prevent many browser hijacks. It is important to have both desktop and network firewalls as firewalls check where the traffic is coming from, whether it is an acceptable domain name or Internet protocol. It is also effective against virus attacks and spyware.

From the above discussion, it is sure that with some essential prevention steps users can secure their confidential information from phishing expeditions. SSL is also an important part of online security that protects user against phishing attacks.

3.5 Pay attention to Grammar & Spelling. Many scammers are not native English speakers and this can be very apparent in their messages. Official businesses, on the other hand, usually take special care to use correct grammar and spelling.

3.6 If you can determine a message is sent from a legitimate organization but you don't want to receive additional messages, you can often use an 'Unsubscribe' from a link at the bottom of the message. However you should not 'Unsubscribe' from scam messages. Many scam messages include this to make them appear more legitimate and use this information to identify 'active' email accounts or possibly obtain sensitive information from users.

3.7 As an act of retaliation, some users will attempt to respond in anger or string spammers along to waste their time. However, these actions could provoke spammers and attackers into attempting to send more advanced, targeted messages to the user or find other ways to outright attack the user. The best course of action when dealing with spam is to delete and ignore the messages entirely.

4. CONCLUSION

Phishing will always exist, because there will always be ways to trick people. The phenomenon of phishing is growing and the number of variations of techniques implemented demonstrates the high interest in these types of attacks by cybercrime. It's easy to look down upon the victims as being stupid, but often the people who fall for the tricks simply lack proper education about computers. The phenomena must be carefully studied. Fundamental is training people in the secure use of computer tools, the cyber threat that is looming, and how the user can recognize threats in order to avoid serious problems.

REFERENCES

[1] Phishing and Pharming: A Guide to understanding and mitigating the risks. http://www. cpni.gov. uk/ documents/ publications/2010/2010019phishing_pharming_guide.pdf?epslanguage=en-gb.

[2] Phishing Attacks and How to Prevent From Being Hooked. http://www.hongkiat.com/blog/phishing-reports-prevention/.

[3] Phishing: A Very Dangerous Cyber Threat. http://resources.infosecinstitute.com/phishing-dangerous-cyber-threat/.

[4] Phishing: http://labs.m86security.com/tag/phishing/.

[5] What Exactly Is Phishing & What Techniques Are Scammers Using. http://www.makeuseof.com/tag/phishing-techniques-scammers/.

[6] Security: Types of Phishing Scams & How to Recognize Them http://grok.lsu.edu/article.aspx?articleid=16680

[7] What are the Different Types of Phishing Attacks? http://www.innovateus.net/science/what-are-different-types-phishing-attacks.

[8] Cut the Line on Phishing Scams http://www.visa.ca/en/personal/securewithvisa/phishing.jsp.