Asian Journal of Information Technology 12 (3): 91-98, 2013
ISSN: 1682-3915
© Medwell Journals, 2013

Social Engineering in Phishing Attacks in the Eastern Province of Saudi Arabia

Jaafar M. Alghazo and Zafar Kazimi
Department of Computer Science and Engineering, Prince Mohammed Bin Fahd University,
P.O. Box 1664, 31952 Alkhobar, Kingdom of Saudi Arabia

Abstract: Many tools are used for phishing. Despite the different tools used in phishing, the key element involves convincing the user to give away their information willingly. In this study, researchers conducted an experiment on a small population of university students in the Eastern Province of Saudi Arabia. A group of 200 university students who had eBay accounts were recruited for the experiment. The experiment included designing a replica website for an online business and hosting it over the intranet. The students clicked on a desktop icon based on instructions from their trusted instructor and the icon took them to a phishing website where the students were asked to log in. The results indicate that 90% of the users who logged onto the website recognized only the look and feel of the login page and did not pay attention to important details such as the URL and the security features of the login page. Another important result showed that combining social engineering with phishing enhanced the experiment and influenced the user's perception of the fake website. The social engineering involved a trusted instructor who influenced their trust in the authenticity of the website.

Key words: Phishing, social engineering, Man in The Middle attack (MITM), Cross-Site Scripting (XSS), eBay

INTRODUCTION

Phishing is the process of using trickery or social engineering to convince customers to give away their confidential information for immoral use. Any business might find phishers masquerading as representatives of the business or find its customer base targeted by phishers. Phishing can be done in many different ways, such as through mass mailing worms involving spam or by targeting victims using bots (Ollmann, 2004; Jakobsson, 2005).

Phishing dates back to 1995 and it started with America Online (AOL). Programs such as AOHell automated the process of phishing for account and credit card information. In its infancy, phishing was primarily used on Internet Relay Chat (IRC) where the phisher would imitate or impersonate an AOL administrator and trick the user into revealing their credit card information by informing the user that there was a technical billing problem that required the user to renew their credit card and login information (Jakobsson, 2005).

According to the spam archives, the targets were primarily E-loan, E-gold, Wells Fargo and Citibank. None of the expensive firewalls, SSL certificates, IPS rules and patch management systems can stop the exploitation of online trust that not only compromises confidential user information but also has had a major impact on consumer confidence regarding telecommunication between an establishment and its client (Ollmann, 2004).

From a technical perspective, most antispam and email security experts were not surprised by the impact of the phishing threat because it had been well documented since RFC 2821, an updated version of RFC 821 written in 1982 (James, 2005).

A considerable amount of research has been carried out to study users' behavior in reaction to phishing. For example, a study was conducted by Downs *et al.* (2007) in which a pilot survey was given to 232 computer users to reveal predictors for falling prey to phishing email and for trusting legitimate email. A similar study was carried out by Sheng *et al.* (2010). In this study, a survey was carried out on 1001 users. The result was used to study the relationship between demographics and phishing susceptibility and the effectiveness of phishing educational materials. The results derived from this survey suggested that women between the ages of 18 and 25 years old were more prone than men to give out information (Dhamija *et al*., 2006). Schechter *et al*., 2007) carried out a similar study on 67 bank customers. The study was carried out to evaluate the website authentication measures that protect users from man in the middle phishing attacks and other forgery attacks.

Corresponding Author: Jaafar M. Alghazo, Department of Computer Science and Engineering,
Prince Mohammed Bin Fahd University, P.O. Box 1664, 31952 Alkhobar, Kingdom of Saudi Arabia

TOOLS FOR PHISHING

Generally, phishing uses a number of techniques. Some of the most common methods deployed in practice are as follows:

- Social engineering (FWI, 2012)
- Man in the middle attack (James, 2005; Ollmann, 2004)
- Cross-site scripting attack (Kirda *et al*., 2006)
- URL obfuscation attack (Milletary, 2005)

Social engineering attack: Phishing emails, a type of social engineering attack have subject lines that are very authentic and genuinely related to the supposed sender. Below is an example derived from (FWI, 2012) in which the email is supposedly sent from a reputable bank (Barclays). In this example, the email appears to becoming from user-supports4@barclays.co.uk. When analyzing the email, one can find minor mistakes such as the word Ibank in the subject. The wording is selected very carefully by the phishers to bypass the spam filter. Some of the common features of spam coming from a phisher are listed:

- Harassing the customer for a quick response
- Asking the customer not to reply to the email but rather to follow a hyperlink
- Threat of freezing the account

As can be noticed from Fig. 1, the following features are used to deceive the user:

- Forged sender address: forging an IP address is an easy deception method. Generally, a spam email can easily look like it has been sent from an authentic bank like Barclays, Citibank and others because the process of forging the email header is simple
- Genuine-looking content: phishing emails use images and text styles similar to the legitimate website in order to portray their emails as genuine. Some users are easily fooled due to the bank logo within the emails
- Email form: the email contains a form for the customer to enter their personal information and click submit, send or update. Forms within emails utilize scripts located on a remote server to receive information and either forward the information to the fraudsters or place the information in a database for the fraudster to pick up later (FWI, 2012)

Man in The Middle (MITM) attack: The phisher intercepts transmissions between the user and a legitimate website or business. There are different methods for performing MITM attacks with a range of complexity but in general, they are considered to be active attacks (James, 2005). An example of what the MITM attack looks like is shown in Fig. 2.

MITM attacks are generally successful in both HTTP and HTTPS communication. The user connects to the attacker's server (thinking it is the genuine site). Meanwhile, the attacker's server is connected simultaneously to the genuine (real) site. The attacker's server proxies all communication between the user and the

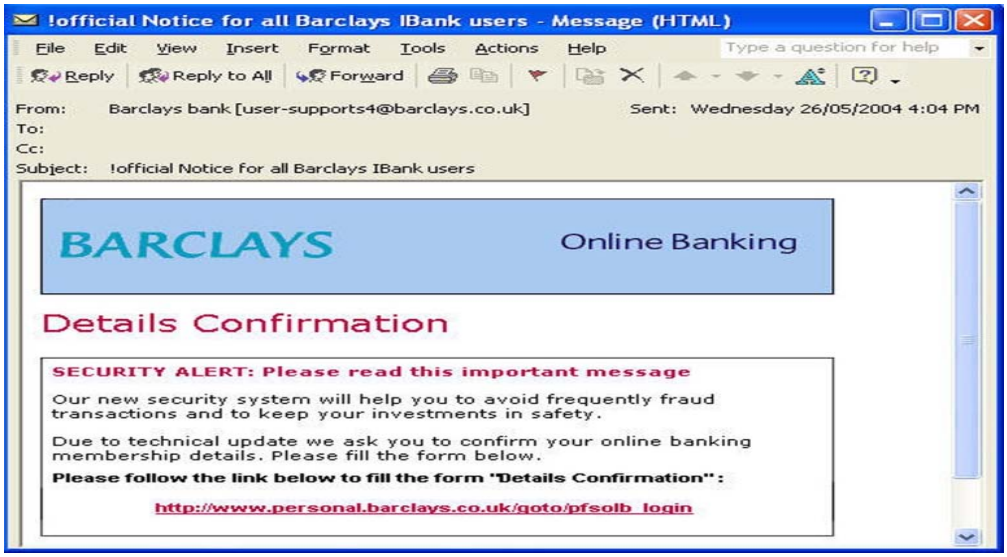

Fig. 1: Barclays Phishing Email (FWI, 2012)

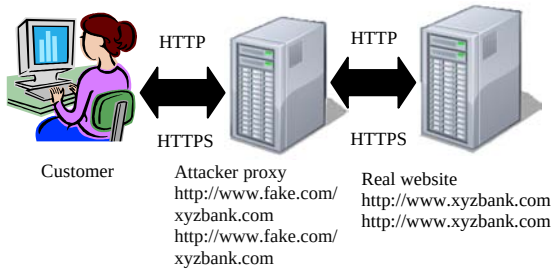

Fig. 2: Structure of the man in the middle attack

genuine server site in real time. The attacker is able to establish an SSL (Secure Socket Layer) connection between both the user and the genuine site (Ollmann, 2004).

In order for an MITM attack to be successful, the attacker must be able to establish a connection between the user and the genuine site. MITM attacks take various forms including the following:

- Transparent proxies: situated on the same network segment or located on route to the real server. A transparent proxy service can intercept all data by forcing all outbound HTTP and HTTPS traffic through it
- DNS Cache poisoning: disrupting the normal traffic routing by injecting false IP addresses for key domain names
- URL obfuscation technique: the attacker tricks the user into connecting to the proxy server instead of the real server. For example, the customer may follow a link to http://www.mybank.com.ch/ instead of http://www.mybank.com/.
- Browser Proxy configuration: overriding the user web-browser setup and proxy configuration options. An attacker can force all web traffic through their nominated proxy server (Ollmann, 2004)

Cross-site scripting: Cross-Site Scripting (XSS) is a method of phishing in which an attacker uses vulnerabilities in the code of a web application to allow them to send malicious code to the end user to retrieve information from the victim. In an XSS, an attacker sends a malicious script to a user. The browser has no reason to suspect the code because it comes from a genuine website. The malicious code can access the cookie and session token. These programs can be used to rewrite the HTML webpage.

The common programming language tools used for this purpose are scripting languages such as Javascript, VBscript and HTML. A typical scenario for an XSS attack is as follows:

- The hacker visits the target webpage, looks for vulnerabilities and injects the scripts into the webpage in the form of an image or a login script
- When a user visits the webpage, the user is unaware of the script that has already been placed by the hacker
- The injected script is downloaded in the client browser
- The browser then redirects the webpage to the hacker's webpage as shown in Fig. 3 (Kirda *et al*., 2006)

URL obfuscation attack: Milletary, in his study "Technical Trends in Phishing", explained how simple techniques are used for URL obfuscation. URL obfuscation is the process of tricking the user into thinking that he/she is browsing or logging onto a trusted website. URL obfuscation, though simple is a highly effective method of attack (Milletary, 2005). The following methods are used for URL obfuscation.

Simple HTML redirection: One of the simplest techniques for obscuring the actual destination of a hyperlink is to use a legitimate URL but have it point to a malicious site. Thus, clicking the legitimate-looking URL hyperlink actually sends the user to a phishing site. This deception can be detected because web browsers display the actual destination of a hyperlink when a user moves the mouse pointer over the link. However, users are still susceptible to this type of attack (Milletary, 2005).

Use of JPEG images: HTML-formatted emails are used by phishers as well. Phishers construct an email that contains a single image in JPEG format. The image appears to the user to be a legitimate email from a legitimate business. To add to the deception, phishers use official logos and add text directed to the customer that makes the email appear as if it were from the business. When the users click the image, they are directed to a phishing website (Milletary, 2005).

Use of alternate encoding schemes: Hostname and IP addresses can be represented in alternate formats that are less likely to be recognizable to most people. Additionally, IP addresses can be specified as hexadecimal numbers:

- IP address: 172.16.24.18
- Hexadecimal: AC101812

Registration of similar domain names: Usually, normal users verify the address displayed in the address or

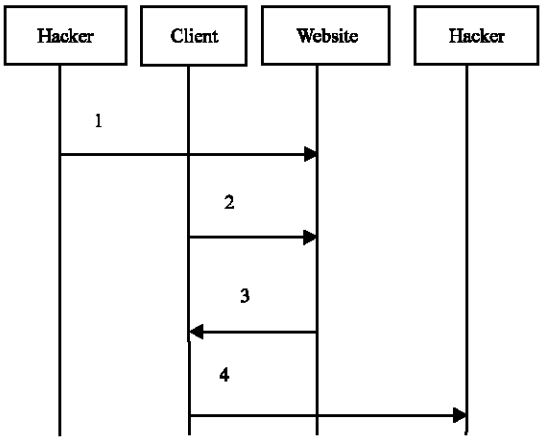

Fig. 3: Overview of how an XSS attack takes place (Kirda *et al*., 2006)

status bar of their web browser with only a brief glance. Phishers try to take advantage of this behavior by registering domains that are very similar to the domain of the target business. This usually works with the majority of users who are satisfied by simply seeing the legitimate name of the business appear in the address field.

As an example, a phishing site could be hosted at http://www.<bankname>-online.biz where <bankname> would be replaced by the name of the target bank. A widely implemented version of this attack uses parts of a legitimate URL to form a new domain name as demonstrated:

- Legitimate URL (http://login.example.com)
- Malicious URL (http://login-example.com)

When just brief glancing at the above two URLs, normal users can be easily fooled (Milletary, 2005).

Current status of URL obfuscation: According to the Anti-Phishing Working Group (APWG), there was a steep increase in URL obfuscation in the first quarter of 2012. Some of the forms of URL obfuscation attacks that took place in the first quarter of 2012 are shown in Table 1 (APWG, 2012).

According to the anti-phishing working group report for the first quarter of 2012, the number of unique URLs is greater than the number of brand/domain pairs, implying that many of these URLs are hosted on the same domain.

Examples of unique URLs:

- http://www.barclays.com.ch
- http://www.citibank-hr.com
- http://www.ebay-it.com

Table 1: Increase in the hijacking of brands and target names in URLs in the 2012 first quarter report from the APWG

Forums	January	February	March
Number of brands hijacked	370.000	392.000	392.000
Contains some form of target in URL	49.53%	45.39%	55.42%

APWG (2012)

Examples of brand hijacking:

- UPS
- FedEx
- Twitter
- Facebook

According to the anti-phishing working group report, the percentage of phishing attacks targeting the financial sector was 38.1% and the percentage of attacks targeting payment services was 21.5%. The other 40% of attacks targeted other sectors such as gaming, social networking and government websites. On average, a phishing website remains active for 62 h and it is generally found that the victim had never visited the website before the attacks (Dong *et al*., 2008).

EXPERIMENT AND BEHAVIORAL RESPONSE TO PHISHING

Recruitment process: An experiment was conducted to study the response to phishing of a population of 200 students from Prince Mohammed Bin Fahd University (Saudi Arabia). Two hundred male students participated in this experiment. The students were between 18 and 24 years old. The selection criterion for this study was that the student have an eBay account. The students were briefed in the class by explaining that this experiment was being conducted for research purposes to understand the human behavioral response to phishing. Most of the population had previously taken courses in the area of professional ethics in computers and network security. None of the students had undergone training on detecting phishing attacks. Prior to the experiment, students were asked the following two simple questions:

- How frequently do you visit the eBay website?
- How frequently do you purchase items from eBay?

Based on their responses, the chart shown in Fig. 4 was generated. Approximately 40% of the population frequently visited the eBay website and approximately 30% frequently purchased items from eBay.

Experimental process: The idea behind the experiment was to combine the social engineering aspect of phishing with technical phishing methods. The experiment is an

initial study of the behavioral aspects of internet users in the Eastern Province of Saudi Arabia. It is different from earlier research in the following ways:

- Most phishing techniques utilize email as a formal method of communicating with the user. In this study, researchers utilize a computer-specific approach. The phishing website was placed on the desktop as an icon of the eBay logo
- The cultural aspects of Saudi students was a key feature in this study; Saudi students highly respect and trust their instructors. It can be argued that students treat anything said by the instructor, being in authority, as a fact, though more research needs to be conducted to prove this statement
- The use of e-Commerce in Saudi Arabia is still very low and most users do not trust the system enough to use online payment methods. Thus, general users are not educated about phishing

The workflow of the experiment is shown in Fig. 5. The idea behind this experiment was to host a fake eBay login webpage similar to the real eBay login webpage on a local server and paste a shortcut icon on the desktop for users to click on. After the students access the fake webpage, they simply enter their username and password and click the login button. After clicking the login button, the user is redirected to the real eBay login webpage on the internet where the students are asked to reenter their username and password. In this example, a fake eBay login page was designed and hosted on a local server. To do this, researchers used ASP scripting to design the fake eBay login webpage and connected it to a database. A snapshot of the fake eBay login webpage is shown in Fig. 6. The fake eBay webpage contained the following major flaws:

- The graphics quality of the security logo was not good
- The URL was not complete when compared with the original eBay login website
- The icon and jargon were changed
- The SSL lock symbol is missing in the URL bar on the fake eBay login webpage

On clicking the Sign in button, the deception page redirects to the actual eBay login webpage. Thus, the user gets confused and thinks that he could not log in during the first attempt. However, the username and the password already entered by the user have been saved in the database.

After the participants enter their confidential information and it is saved in the database, the attack is complete and successful. After the completion of the experiment, the participants were informed about the purpose of the experiment and were advised to change the confidential information that was revealed during this experiment.

Behavioral response: After the experiment was conducted, the students were asked the following

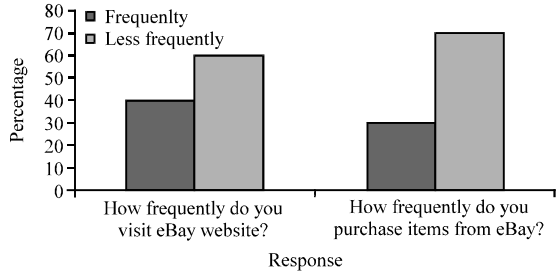

Fig. 4: Response to questions 1 and 2

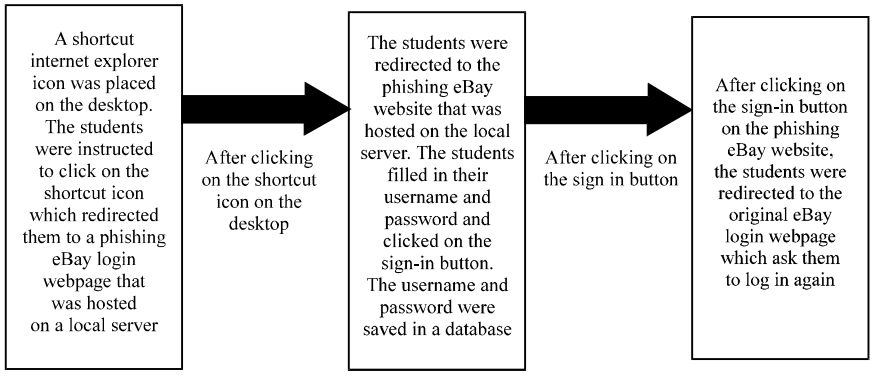

Fig. 5: Workflow of the experiment

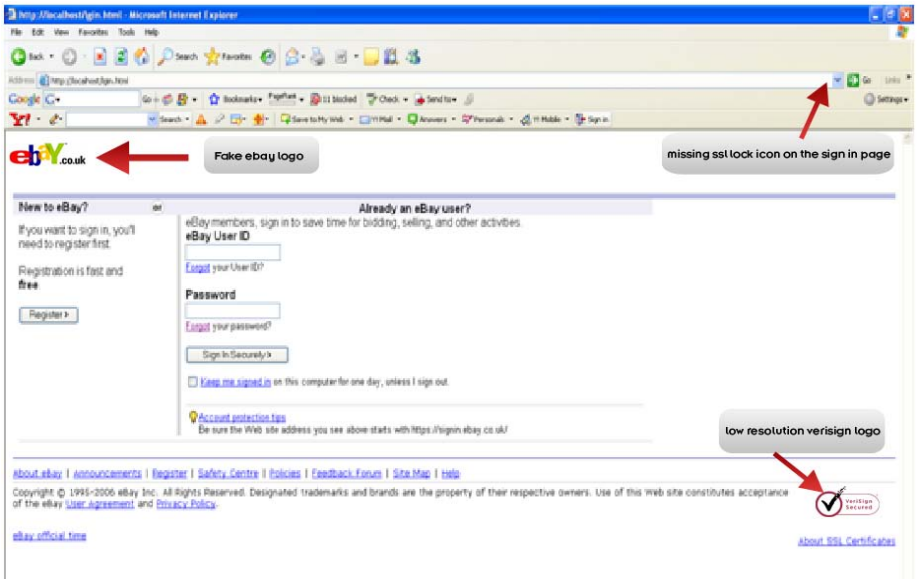

Fig. 6: Snapshot of the fake eBay login page designed to launch a deception attack

questions about the phishing webpage they had visited and they had to respond with an answer of yes, no or not sure (Fig. 7):

- Q.1 Does the webpage appear to be genuine?
- Q.2 Are the graphics and fonts of low quality?
- Q.3 Is the URL correct?

Over 90% of the population surveyed thought that the webpage appeared genuine and <10% thought the graphics and font were low quality. Only 5% of the population surveyed noted that the URL was incorrect.

Additionally, the students were asked the following questions after the experiment was completed about the fact that they were redirected to the genuine eBay webpage after their first attempt to log in (Fig. 8):

- Q.1 Do you think it was just a server error?
- Q.2 Did anything seems suspicious?
- Q.3 Will you change your password just to remain secure?

With regard to being redirected again to the original eBay website to log in after already attempting to log in on the phishing website, approximately 60% of the population responded that this occurred because of a server error. Approximately 35% thought that this process seemed suspicious, yet only 10% of the population thought that the webpage was not genuine and that the graphics were low quality. This has to do with human nature and behavior: the participants were asked directly

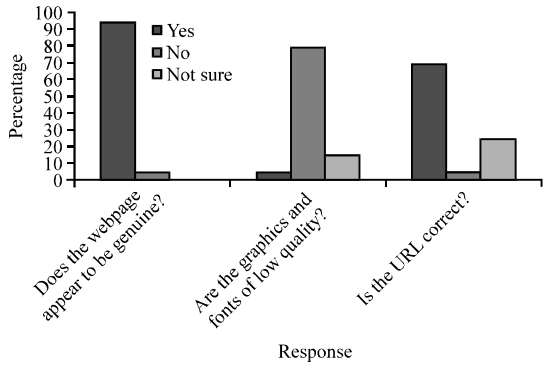

Fig. 7: Responses about the deception website

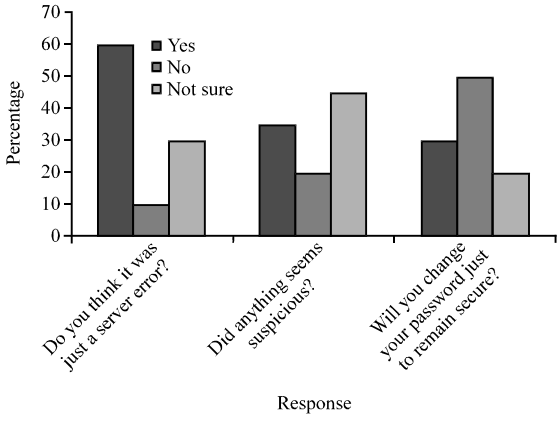

Fig. 8: Response to the phishing website

if anything seemed suspicious?, making them wonder why the question was asked in the first place and increasing

the number of Yes answers. This corresponds with the fact that approximately 30% of the population answered Yes to whether they would change their passwords. These are the same 30% who started suspecting the nature of the experiment from the questions asked.

RESULTS

Despite the fact that some users were frequent users of eBay, the results show that over 90% of the population thought the fake eBay webpage was genuine; 80% of the population responded that the graphics and fonts of the fake eBay webpage were genuine. Only 5% of the population noted that the URL was incorrect for the fake eBay webpage.

After the experiment was conducted and the students had reentered their username and password on the real eBay login webpage, the students were again questioned about the process. In response, 60% of the population responded that it was just a server error. Only 35% of the population thought something was suspicious about the website. Approximately 50% of the population responded that they would not change their password even after interviewing them and asking a question about the experiment that might raise doubts.

The fake eBay webpage contained flaws deliberately designed to study the behavioral aspect of users. The result based on the above finding clearly indicates that normal users were not concerned about identifying the flaws described.

CONCLUSION

The following conclusions can be made based on the above experiment:

- Users judge a website based on the look and feel rather than the security features and legitimacy
- Users do not pay attention to the icons and jargon on the webpage
- Users, even those aware of phishing are not educated about the methods used to detect phishing websites
- Users tend to pay less attention to the website and its features when the phishing is combined with social engineering (in this case, instructions coming from a trusted instructor)
- Users will suspect a phishing attack only after the fact and when directly asked questions that make them suspicious (Dhamija *et al*., 2006; Downs *et al*., 2006; Wu *et al*., 2006)

LIMITATIONS

- The study was only conducted on a population of male students
- The study was conducted on a population between the ages of 18 and 24 years old
- The students were not given training on phishing websites which might have yielded different results
- The study does not categorize the behavior of the users in a real-world phishing scenario

RECOMMENDATIONS

Educating users on phishing techniques is an important aspect of internet security. If users are educated about phishing, it can help them understand the different methods used to judge whether a website is a legitimate site or a phishing site. Therefore, the potential for future research in this area is significant. The study will be expanded to a larger geographical area and will use a larger population including both males and females. It will also include other phishing techniques. In addition, the future research will include a comparison of the behavior of users educated about phishing and techniques used to detect phishing with a population that has not been educated about phishing and phishing detection.

REFERENCES

APWG, 2012. Phishing activity trend report: 1st Quarter 2012. Anti-Phishing Working Group, http://docs.apwg.org/reports/apwg_trends_report_q1_2012.pdf?bcsi_scan_F40B836301B5827A=0&bcsi_scan_filename=apwg_trends_report_q1_2012.pdf.

Dhamija, R., J.D. Tygar and M. Hearst, 2006. Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 22-27, 2006, Montreal, Quebec, Canada, pp: 581-590.

Dong, X., J.A. Clark and J.L. Jacob, 2008. User behaviour based phishing websites detection. Proceedings of the International Multi Conference on Computer Science and Information Technology, October 20-22, 2008, Wisla, Poland, pp: 783-790.

Downs, J.S., M.B. Holbrook and L.F. Cranor, 2006. Decision strategies and susceptibility to phishing. Proceedings of the 2nd Symposium on Usable Privacy and Security, July 12-14, 2006, Pittsburgh, Pennsylvania, USA., pp: 79-90.

Downs, J.S., M.B. Holbrook and L.F. Cranor, 2007. Behavioral response to phishing risk. Proceedings of the Anti-phishing Working Groups 2nd Annual Ecrime Researchers Summit, Volume 269, October 4-5, 2007, Pittsburgh, Pennsylvania, USA., pp: 37-44.

FWI, 2012. Phishing email method. Fraud Watch International, http://www.fraudwatchinternational.com/phishing-fraud/phishing-email-methods/.

Jakobsson, M., 2005. Modeling and Preventing Phishing Attacks. In: Financial Cryptography and Data Security, Proceedings of the 9th International Conference, Roseau, The Commonwealth Of Dominica, February 28-March 3, 2005, Patrick, A.S. and M. Yung (Eds.). Springer Verlag, USA., ISBN: ISBN: 978-3-540-26656-3 pp: 5-10.

James, L., 2005. Phishing Exposed. Syngress Publishing, USA., ISBN-13: 9780080489537, Pages: 450.

Kirda, E., C. Kruegel and N. Jovanovic, 2006. Noxes: A client-side solution for mitigating cross-site scripting attacks. Proceedings of the 2006 ACM Symposium on Applied Computing, April 23-27, 2006, Technical University of Vienna, pp: 330-337.

Milletary, J., 2005. Technical trends in phishing attacks. US-CERT a Government Organization, Carnegie Mellon University, USA.

Ollmann, G., 2004. The phishing guide understanding and preventing phishing attack. IBM Internet Security Systems, pp: 3-23.

Schechter, S.E., R. Dhamija, A. Ozment and I. Fischer, 2007. The emperor's new security indicators. Proceedings of the Symposium on Security and Privacy, May 20-23, 2007, Berkeley, CA., pp: 51-65.

Sheng, S., M. Holbrook, P. Kumaraguru, L. Cranor and J. Downs, 2010. Who falls for phish: A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 10-15, 2010, Atlanta Georgia, USA., pp: 373-382.

Wu, M., R.C. Miller and S.L. Garfinkel, 2006. Do Security Toolbars Actually Prevent Phishing Attacks. In: Proceeding of the SIGCHI Conference on Human Factors in Computing Systems (Montreal, Quebec, Canada, April 22 -27, 2006, Grinter, R., T. Rodden, P. Aoki, E. Cutrell, R. Jeffries and G. Olsons (Eds.). ACM Press, New York, pp: 601-610.