Volume 6, Issue 3, March 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Analyzing the Impacts of Phishing and Vishing Attacks in Internet Banking

Dr. Amit Chaturvedi*
Assistant Prof., MCA Department,
Govt. Engineering College, Ajmer,
Rajasthan, India

Asha Meena
M.Tech. Scholar
Bhagwant University, Ajmer,
Rajasthan, India

Abstract— Presently all banks provide online banking facilities to their customers and customers are using these services undoubtedly. But still there are the chances of online frauds in internet banking. A typical phishing attack is made up of two components: an authentic-looking email and a fraudulent Web page. This form of spam frequently uses professional-looking, HTML-based emails that include company logos, colors, graphics, font styles, and other elements to successfully spoof the supposed sender. Vishing is very old scam or banking fraud. In this banking scam or fraud, the attacker phones the bank customers and uses social engineering to trick the bank customers into revealing secret information such as credit card information. The new is the use of voice-over-IP and how this changes the expected trust in the phone system. One of the major Vishing attack is cloned voice-banking systems. In this paper, we presented the analysis of impacts of phishing and Vishing attacks on Internet Banking.

Keywords— Internet Banking, Phishing, Vishing, online frauds.

I. INTRODUCTION

Phishing is a term used to describe spoof emails and other technical ploys to trick receipts into giving up their personal or their company's confidential information such as social security and financial account credentials and other identity and security information. This form of identity theft employs both social engineering and technical subterfuge to steal account access information, identity or other proprietary information that can be sold on to third party via specialized chat rooms established specifically for the purpose of selling such information. Social engineering schemes use spoofed emails to lead customers to counterfeit websites designed to trick recipients into divulging financial data. Technical subterfuge schemes plant crime ware onto computers to steal credentials directly using key logging systems. The term "phishing" evolved from the word "fishing" and follows a very similar approach. Some phishing emails look extremely professional and realistic, while others are crude and badly constructed but have a common goal-to steal information through deception. Phishing is a serious and increasingly prolific form of spam, and is one of the main tactics employed in business and consumer identity theft. Phishing actually comprises of two online identity thefts used together. In phishing scams, the identity of the target company-commonly a bank, online payment service, or other reputable business- is stolen first in order to steal even more identities: those of unsuspecting customers of the targeted company. [1]

A typical phishing attack is made up of two components: an authentic-looking email and a fraudulent Web page. This form of spam frequently uses professional-looking, HTML-based emails that include company logos, colors, graphics, font styles, and other elements to successfully spoof the supposed sender. The content of the phishing email is usually designed to confuse, upset, or excite the recipient. Typical email topics include account problems, account verifications, security updates/upgrades, and new product or service offerings. Recipients of the email are prompted to react immediately. They then click on a link provided in the email body, which actually directs them to the phishing Web page. The intent is to lure recipients into revealing sensitive information such as usernames, passwords, account IDs, ATM PINs, or credit card details. Like the phishing email, the phishing Web page almost always possesses the look and feel of the legitimate site that it copies, often containing the same company logos, graphics, writing style, fonts, layout, and other site elements. This spoofed Web page may also include a graphical user interface (GUI) intended to lure the user into entering their bank account information, credit card number, social security number, passwords, or other sensitive information. Either the phisher, or an anonymous remote user that sent the information, can then use the stolen information. The phishing "ecosystem" consists of a collection of individuals who play various roles within the phishing space, ranging from the financially- motivated botnet creators to those who actively pursue and prosecute the cybercriminals. In this ecosystem, a large industry of buying and selling- a "microeconomy" exists within the phishing underground, involving botnet (Biever 2004) creators, perpetrators, and enablers. However, these three player groups are complex and intertwined: a single individual or multiple perpetrators can play separate or simultaneous roles.

Vishing is very old scam or banking fraud. In this banking scam or fraud, the attacker phones the bank customers and uses social engineering to trick the bank customers into revealing secret information such as credit card information. The new is the use of voice-over-IP and how this changes the expected trust in the phone system. One of the major Vishing attack is cloned voice-banking systems.

II. EXISTING PHISHING METHODS

i) **Domain Spoofing:** Domain spoofing is famous technique in remote attacks, where attacker may use same website names as well as names that look similar to the actual domain to fool unsuspecting users into revealing bank's confidential information for example, in domain name they change few alphabets like lower case letter 'f' for capital letter 'F' because, they look similar but in domain names they are treat two different alphabets.

ii) **URL Modifying:** Uniform resource locator phishing technique is another way to redirect web-requests to their own URL. The '@' symbol lets attackers redirect traffic to their own url as web browsers truncate all character before the '@' symbol. For example yahoo.com@192.160.1.1 will redirect to 192.160.1.1 without regarding the yahoo.com URL.

iii) **Website layout similarities:** website layout similarities can also do the trick of phishing. Because of the same layout design, the user is not able to understand weather it is the same website or fake page with same design. For example if the attacker designs the same layout of facebook with same font size, color and same login details along with other backend facility. The common user will not understand that it the same page which he/she is using for social networking. Fake Website page is common trap for unprofessional users.

III. TYPES OF PHISHING ATTACKS

Phishing approaches used for identity thefts are constantly growing and new variants are tried and used to attack business organizations, financial institutions, and customers. Some of the most prevalent types of phishing attacks are presented hereunder.

a. Deceptive Phishing is the most common broadcast method today and involves sending messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected [3].

b. Malware-Based Phishing refers to scams that involve users to unknowingly running malicious software on their PCs. Malware isas an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities -a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

c. Keyloggers and Screenloggers are particular varieties of malware that track keyboard input in the backdoor and send relevant information to the hacker via the Internet. They embed themselves into web browsers as small utility programs known as helper objects that run automatically when the browser is started as well asinto system files as device driversor screen monitors.

d. Session Hijacking is that phishing attack in which users' activities are monitored until they sign in to a target account or transaction and establish their bona fide credentials. At that point the malicious software takes over and Undertakes unauthorized actions, such as transferring funds, without the user's knowledge.

e. Web Trojans are a type of popup running invisibly on user machines. When users are attempting to log in. they collect the user's credentials locally and transmit them to the phisher.

f. Hosts File Poisoning involves changing the host files of the operating system that contain the IP addresses corresponding to the web addresses. When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. The majority of SMB users' PCs running a Microsoft Windows operating system first look up for these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted, taking the user unwittingly to a fake "look alike" website where their information can be stolen. System Reconfiguration Attacks modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "mybank.com" to "my banc.com".[4]

g. Data Theft refers to stealing subset of sensitive information stored locally on unsecured PCs which actually is stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, and employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

h. DNS-Based Phishing also called Pharming is aterm given to hosts file modification or Domain Name System (DNS) based phishing. With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. This results in users falling unwarily victims by working on the websites controlled by hackers where they enter confidential information.

Content-Injection Phishing is used to describe the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.

i. Man-in-the-Middle Phishing is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

j. Search Engine Phishing occurs when phishers create websites with attractive offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks. Victims who use these sites to save or make more from interest charges are encouraged to transfer existing accounts and deceived into giving up their details.

k. Spear Phishing Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization [5].

Spear phishing is also being used against high-level targets, in a type of attack called "whaling". For example, in 2008, several CEOs in the U.S. were sent a fake subpoena along with an attachment that would install malware when viewed [6]. Victims of spear phishing attacks in late 2010 and early 2011 include the Australian Prime Minister's o_ce, the Canadian government, the Epsilon mailing list service, HBGary Federal, and Oak Ridge National Laboratory [7].

- Vishingor Voice phishing can work in two different ways. In one version of the scam, the consumer receives an email designed in the same way as a phishing email, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the email provides a customer service number that the client must call and is then prompted to "log in" using account numbers and passwords. Vishing poses a particular problem for two reasons. First, criminals can take advantage of cheap, anonymous Internet calling available by using Voice over Internet Protocol (VoIP), which also allows the criminal to use simple software programs to set up a professional sounding automated customer service line, such as the ones used in most large firms. Second, unlike many phishing attacks, where the legitimate organization would not use email to request personal information from accountholders, vishing actually emulates a typical bank protocol in which banks encourage clients to call and authenticate information (Schulman-2006).
- Growth of Phishing Scams An estimated one million computers are under the control of hackers worldwide. German security analysts at Aachen University reported more than 100 botnets in three months, which ranged in size from a few hundred compromised computers to 50,000 machines (Holz–2005). The effects caused by phishing on business and customers are far reaching and include substantial financial loss, brand reputation damage, lost customer data files, possible legal implications, significant decrease in employee productivity, improper IT resource utilization, and other administrators impacts. Besides direct financial loss, erosion of public trust in the Internet is a direct impact of fishing on electronic trading[8].

IV. PROPOSED SOLUTIONS FOR PHISHING ATTACKS

4.1 Stop phishing at the e-mail level:

Sending an e-mail and asking for somebody's bank account login details is a simple idea and its costs almost nothing. Each day more and more e-mails are sent with the aim of making the web users believe that the same is legitimate and from the trusted institutions. It asks the users to visit a spoofed site where they will be asked to provide their login credentials and at the end, the same will be used by miscreants for reaping financial and other benefits. As most phishing attackers send e-mails to lure victims to visit spoofed web site, one approach can be to stop this e-mail from getting delivered to the end-user. In another work, Bergholz et al. (2010) describes new approaches, including statistical models for the low-dimensional descriptions of e-mail topics, sequential analysis of e-mail text and external links, the detection of embedded logos as well as indicators for hidden salting. Hidden salting is the intentional addition or distortion of Content not perceivable by the reader. During experiments of their work authors found that their methods outperformed other published approaches for classifying phishing e-mails. Chandrasekaran et al. (2006) in their paper proposed a technique to discriminate phishing e-mails from the legitimate e-mails using the distinct structural features present in them. Their proposed solutions can be used to classify phishing e-mails before it reaches the user's inbox, essentially reducing the human exposure. However, the experiment base used during the work was not large enough to draw a broader conclusion. Also the classification approach adopted is only one of the many ways that could be employed, thus the choice of features plays an important role for the success of this approach. In another work Fette et al. (2007) proposed a machine learning approach to create a specialized filter named PILFER. In the new filter they used ten very specific features that are more directly applicable to phishing e-mails. They found their solutions to be more effective then available spam filters[10]. He et al. (2011) proposed a heuristic method to determine whether a web page is a legitimate or a phishing page. The solution is a combination of CANTINA (Xiang et al., 2011) method, anomaly method, and PILFER method (Fette et al., 2007), with several additions and modifications. The idea was that every web site claims a web page identity, either real or fake. If a web site claims a fake identity, abnormality may exist in a network space; therefore the proposed method could detect and differentiate between a legitimate and a phishing web site.

4.2 Security and password management toolbars:

HTTP basic authentication protocol is vulnerable to phishing attacks because a client needs to reveal his password to the server that he wants to login. Most users have multiple password protected accounts over the internet. To avoid the headache in remembering and managing a long list of different and unrelated passwords, most users simply use the same password for multiple accounts. A phisher can effectively steal users' passwords for high-security servers, such as an online banking web site by setting up a malicious server or breaking into a low-security server, such as a high-school alumni web site. Gouda et al. (2007) proposed anti-phishing single password protocol. Proposed protocol allows a client to securely use a single password across multiple servers, and also prevents phishing attacks. The protocol achieves client authentication without the client revealing his password to the server at any point. Therefore, a compromised server cannot steal a client's password and replay it to another server. Although password is one of the most commonly adopted means to protect user accounts, most users are used to giving away the same very easily. Most users disregard the security functionality; they do not have the knowledge and/or the motivation to configure or to use the existing security functions correctly. Some software based protections in the client computer can help in user password management. Whenever a user wants to submit login credential into any of the phishing sites, these tools can be useful in preventing such an incident. In the recent past various client side and browser based tools have been proposed as solutions to phishing attacks.[19]

It helped in improving web password security and defence against password phishing and other attacks. This browser extension applies a cryptographic hash function to a combination of the plaintext password entered by the user, data associated with the web site, and a private salt stored on the client machine. Theft of a password phished from one site will not yield a password that is useful at another site. As noted by the authors this approach may not be effective against a pharming or DNS attack or against any spyware or key logger. Chou et al. (2004) introduce a browser plug-in called SpoofGuard.

4.3 Application of Restrictions:

Malicious or the spoofed web sites are the core problem of the phishing activities. There have been various efforts to restrict users from visiting these sites. Blacklist is one such effort, where the web browsers check the URLs against a list of URLs of known phishing sites. Upon finding the requested URL on a blacklist, the system restricts access and/or generates a warning indicating the danger of a phishing site. These blacklists are constructed using a range of techniques including manual reporting, link analysis, honey pots, and web crawlers combined with site analysis heuristics (Ma et al., 2009; Zhang et al., 2008). Blacklist approaches have long been used in other areas such as detection of spam e-mail (Jung and Sit, 2004). A spam blacklist of IP addresses can restrict delivery of spam e-mail to large extent, but a similar restriction list is not possible in case of web site as there is a possibility that the IP address can have multiple domains hosted on the same. So a blacklist of specific URLs is a better solution in case of phishing or spoofed web sites (Sheng et al., 2009). However, blacklists have a major drawback; it is mainly a reactive approach. Blacklist maintainers learn of phishing web sites only after these sites have become active. Thus, a window of vulnerability remains during which users can suffer from malicious exposure because an active entity has not yet appeared on a blacklist (Felegyhazi et al., 2010). To solve this inherent problem of blacklist Prakash et al. They extended the source code for an open source Linux-based proxy server and added features to check the site's safety rating before allowing HTTP requests to be forwarded. Dong et al. (2010) proposed user-behaviour based phishing detection system (UBPD).

4.4 Visually Differentiate The phishing sites:

Detecting phishing web pages is similar to the problem of detecting duplicate documents and plagiarism, except that these focus on text-based features in similarity measurement, whereas phishing-page detection should focus more on visual similarities (Liu et al., 2006). To differentiate between the legitimate web site and the phishing one, dynamic security skins (DSS) a new class of human interactive proofs (HIPs) that allow a human to distinguish one computer from another, has been proposed which requires users to verify visual content from the server. The rationale is that the server should have the possibility to determine whether the SSL/TLS session in which it receives the credentials is the same as the one the user employed when he sent out the credentials in the first place. If the two sessions are the same, then a session is directly established between the user and the server, whereas if they are different, then an MITM attack is likely to be taking place. With the help of TLS-SA the server can recognize this and drop the session. Sakilkar and Saha (2008) presented a completely automated public Turing test to tell computers and human apart (CAPTCHA) solution as phishing defence which embed public key information inside CAPTCHA that client side can verify the public key as well as the destination server. However, if user is such unconscious, force validation is needed; their design requires client side installation.

4.5 Two-Factor and Multi-Channel Authentication:

Traditionally passwords are used for authentication in any online web sites. One has to memorize the password for that site and provide the same on demand by that web site. If a third party gets to know the password then the said account is compromised (Bose and Leung, 2007). In order to solve the problem faced with the usage of passwords researches have proposed two-factor authentication. In two-factor authentication process, user should prove "what he knows" and "what he has". Here what he knows is the password, and what he has is something that only the genuine user will have. This something can be a hardware token given by the institutions which can generate PINs (Nilsson et al., 2005), or a OTP (Molloy and Li, 2011; Yang and Choi, 2010) or some personal certificate or documents which only the user can have. Though the cost of implementation will be very high one can consider biometrics based authentication also (Zviran and Erlich, 2006). With the help of OTP and separate boot USB or CD, Martino and Perramon (2010) proposed multi-factor mutual authentication. First, the server is authenticated and next, if the result of the server authentication is successful, the user will provide his credentials. In this manner user credentials are prevented from being stolen by a hijacking server. In another work Adida (2007) proposed BeamAuth, a two-factor web authentication technique where the second factor is a specially crafted bookmark. While using BeamAuth user will be required to select a preconfigured bookmark in his client browser to authenticate himself. Many banks have altered their authentication mechanisms, suggesting their willingness to adapt and go beyond traditional and simple passwords (Herley et al., 2009). Mannan and Oorschot (2007) proposed to use mobile phone network to authenticate services on the internet through an un-trusted computer. On a similar line Mizuno et al. (2005) proposed user authentication using multiple communication channels. Their solution enables on-line service providers to strongly authenticate their users on a non-trusted communication channel via trusted communication channels.

4.6 Takedown, transaction anomaly detection, log files:

Banks and other organizations deal with fraudulent phishing web sites by pressing hosting service providers to remove the sites from the internet so that there is nothing there for a misled visitor to see. The procedure is commonly known as take-down (Moore and Clayton, 2007). Most banks and specialist take-down companies maintain their own feed. PhishTank the online web site asks the end-users to visit their site and contribute to their source list (PhishTank, 2010). Users are invited not only to provide the content but also to verify that the entries are correctly classified. In another work Moore and Clayton (2008) gathered phishing reports from the PhishTank. After analyzing the data received from PhishTank authors concluded that any crowd-based decision mechanism like PhishTank remains susceptible to vote rigging and manipulation that could undermine its credibility. Moore and Clayton (2007) studied the empirical data on phishing web site removal times and the number of visitors that the web sites attract, and concluded that web site removal is a part of the answer to phishing, but it is not fast enough to completely mitigate the problem. By the time they are removed, the fraudsters learn the passwords; PINs and other personal details of the users who are fooled into visiting them.

4.7 Anti-Phishing Training:

Core idea of anti-phishing training is that users can be trained to actively protect themselves from phishing threats. The United States Military Academy (USMA) has been very active in implementing hands-on exercises such as the cyber defence exercise (Dodge et al., 2003). They concluded that embedded training interventions helped teach people about phishing and how to avoid phishing attacks. In another paper Kumaraguru et al. (2007b) studied an embedded training methodology using learning science principles in which phishing education is made a part of a primary task for users . The goal is to motivate the users to pay attention to the training materials. In embedded training, users are sent simulated phishing attacks and trained after they fall for the attacks. They tested users to determine how well they retained knowledge gained through embedded training and how well they applied this knowledge to identify other types of phishing e-mails. They concluded that users learn more effectively when the training materials are presented after users fall for the attack (embedded) than when the same training materials are sent by e-mail (non-embedded). Kumaraguru et al. (2009, 2010) conducted research works which focuses on educating users about phishing and helping them make better trust decisions. They identified a number of challenges for end-user security education in general and anti-phishing education in particular. They developed an e-mail-based anti-phishing education system called "PhishGuru" and an online game called "Anti-Phishing Phil" that teaches users how to use cues in URLs to avoid falling for phishing attacks. Sheng et al. (2010) conducted a role-play survey among 1,001 online respondents to study both the relationship between demographics and phishing susceptibility and the effectiveness of several antiphishing educational materials. Their work shows that educational materials reduced users' tendency to enter information into phishing web pages by 40 percent, however, some of the educational materials they tested also slightly decreased participants' tendency to click on legitimate links. Another method for educating users is to send fake phishing e-mails to test users' vulnerability and then follow up with training. Subsequent fake phishing e-mails can be used to measure improvements in phishing detection abilities. This approach has been used by Jagatic et al. (2007) and has shown that education can improve participants' ability to identify phishing e-mails. They concluded that people can become less vulnerable by a heightened awareness of the dangers of phishing, the importance of reporting attacks to which they fall victims, the ease of spoofing, and the possible exploitation of personal information posted on the web.

4.8 Legal solutions:

It is clear that phishing has become part of our social and technological reality. Active development of the necessary legislation is desperately required. Bainbridge (2007) and Larcom and Elbirt (2006) in their work stated that the law, however, must take proper notice of current technical risks as well as measures taken to counter them. Granova and Eloff (2005) conducted a detailed study on phishing experience and available legal frame work in both the developing and the developed world. Mcnealy (2008) in his paper examines the existing state laws in USA aimed at stopping phishing as well as the proposed federal legislation. He concluded that adequate legal solutions would enable severe punishment of those caught phishing; the law also would allow both the victims of a phishing scam and companies whose informations were fraudulently used, to collect damages. Bose and Leung (2009) found that in Hong Kong Government advocacy for adoption of antiphishing measures influenced the adoption of two-factor authentication by banks. Larson (2010) in his paper recommended that courts should consider either large-scale damages against individual phishers or secondary liability against internet service providers (ISP) under the areas of either intellectual property (IP) or unfair competition law. The addition of secondary liability to anti-phishing efforts might motivate ISPs to become actively involved in anti-phishing efforts since ISPs are best positioned to prevent of phishing schemes (Calman, 2006). Additionally, trademark holders are also well positioned to deter phishing by asserting their IP rights against trademark infringing phishers and those engaging in unfair competition. The browser vendors, developers, CAs, web server vendors, web sites, regulators, and standards committees. It is not easy to reach to a timely agreement among them.

V. CONCLUSION

As there are various types attacks encountered in internet banking like phishing, vishing, cloned voice-banking systems, DNS Hijacking, DNS cache poisoning, and VoIP. Phishing attacks is very common category of attacks that Internet Banking Industry and its consumers face. Various solutions are proposed for the prevention from phishing like stop phishing at the e-mail level, Security and password management toolbars, Application of Restrictions, Visually Differentiate the Phishing Sites, Two-Factor and Multi-Channel Authentication, Anti-Phishing Training, and Legal Solutions. Applications of these solutions may provide a good level of security from hacking through phishing attacks.

REFERENCES

[1] New approach to Internet Banking, Matthew Johnson , September 2008 Technical report (UCAM-CL-TR-731 ISSN 1476-2986)Cambridge university.

[2] Firefox phishing protection bypass vulnerability. Securiteam, Jun 2006. http://blogs.securiteam.com/index.php/archives/467

[3] Banday, M.T., Qadri, J.A. (2007). “Phishing - A Growing Threat to E-Commerce,” The Business Review, ISSN: 0972-8384, 12(2), pp. 76-83.

[4] Dan Ferguson (2006),“ Phishing warning Beware e-mails asking for personal info, Peace Arch News”.

[5] Federal Bureau of Investigation. Spear phishers. http://www.fbi.gov/news/stories/2009/ april/spearphishing_040109.

[6] John Marko_. Larger prey are targets of phishing. http://www.nytimes.com/2008/04/16/ technology/16whale.html.

[7] J.Hong. Why have there been so many security breaches recently? http://cacm.acm.org/blogs/blog-cacm/107800-why-have-there-been-so-many-% security-breaches-recently/fulltext.

[8] KrCERT/CC, (2006) Korea Phishing Activity Trends Report”, Korean Internet Security Center

[9] Wenliang Du, Syracuse University. DNS Pharming Attack Lab, Copyright c 2006 – 2011.

[10] DNS Client Spoof: http://evan.stasis.org/odds/dns-client spoofing.txt.

[11] Roberto Barbieri, Danilo Bruschi, Emilia Rosti, Voice over IPsec: Analysis and Solutions.

[12] Bankash.A, For detailed information on PWSteal. http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bankash.a.html.

[13] For detailed information on PWSteal.Bancos.B, http://securityresponse.symantec.com /avcenter/venc/data/pwsteal.bancos.b.html.

[14] KeyGhost. KeyGhost SX. http://www.keyghost.com/keylogger.htm.

[15] For detailed information on Trojan.Qhosts, http://securityresponse.symantec.com/avcenter/venc/data/ trojan.qhosts.html.

[16] Tejinder Pal Singh Brar,** Dr. D Sharma, *** Dr. S Singh Khurmi, Vulnerabilities in e-banking: A study of various security aspects in e-banking.

[17] S Purkait, Phishing counter measures and their effectiveness – literature review, 380-420.

[18] Lazarus, David, (2006).“ Phishing expedition at heart of AT&T hacking”, San Francisco Chronicle.

[19] Alnajim, A.M. (2009), “Fighting internet fraud: anti-phishing effectiveness for phishing websites detection”, unpublished doctoral dissertation, Durham University, Durham.