ISSN 2278-3083
Volume 3, No.1, January - February 2014
International Journal of Science and Applied Information Technology
Available Online at http://warse.org/pdfs/2014/ijsait01312014.pdf

Protecting Customers Online: Response from Pakistani Banks

Amir Manzoor[1]
[1]Management Sciences Department, Bahria University, Karachi, Pakistan
amirmanzoor@yahoo.com

ABSTRACT

Phishing is a phenomenon that is affecting the financial industry worldwide. An increasing number of financial institutions, especially banks, are being targeted annually by phishing attack perpetrators. The objective of this study is to investigate the preparedness of Pakistani banks against phishing attacks. For this purpose, websites of licensed Pakistani banks offering online banking services were analyzed. The analysis showed that few banks providing online banking services to their customers provided phishing-related information to their customers and adopted anti-phishing measures. For banks not providing online banking services it was found that most banks didn't provide any phishing-related information to their customers.

Key words : Phishing, customer, online banking, website, ICT.

1. INTRODUCTION

Phishing is a relatively new type of identity fraud that refers to the act of trying to get information like username, credit cards details and passwords by pretending to be a reliable company [1]. In 1995, first phishing incident was observed [5] .However the growth of phishing attacks since then has been incredible. According to the report released by the Anti-Phishing Working group (APWG) in mid of 2012, the incidents of phishing have grown by 88.1% from last year. The most popular target of phishing is the financial sector and about 34 % of phishing frauds are associated with financial service companies. The second and third most popular target industries of phishing are payment services 32 % and Retail/service sector 9.9 % [2]. Rapid increase in Phishing has caused significant losses to business sector around the globe [17].In year 2004 there were about US$ 1.2 billion of financial loss that caused by 1.8 million phishing attacks [9] and more than 5 million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008 [8] .Phishing attacks around the world cost billions of dollars in loss every year [20]. With the widespread increase in online banking among customers phishing is becoming more common. In this study, we will discuss how well prepared the Pakistani banks are in protecting their customers against phishing attacks. The variety of information related to phishing and anti-phishing measures and their easiness to the banks of retrieving that information from websites of the banks will be discussed here.

2. RESEARCH OBJECTIVES

Nowadays phishing is becoming a serious crime. In order to deter such crime successfully, public awareness should be increased and the general public service provider should take effective measure. We are going to discuss what measures financial service providers have taken to protect customers from phishing attacks.

Banks are the top most targets of phishing and therefore, they should be more prepared because a single incident of phishing can cause a huge financial loss. Company's reputation can also be affected severely because of such incidents [16].In order to deter phishing it is necessary for banks to protect their electronic system effectively and to teach the customers about the best precautions to protect themselves from such crimes. As the company's web site is the major means of communication between the company and the public therefore, all the measures adopted by banks and advices are expected to be available on the web sites. This can depict how well prepared company is in protecting the customers from the phishing attacks.

In this study, we look for the different information about general phishing advice and anti-phishing measures and the access to the information available on bank's web sites. We strive to provide an overall view of the banks' preparedness against phishing attacks and approaches that can be used by banks to make improvements and making the best anti-phishing strategies by adopting more anti-phishing measures and improving the accessibility to the information available on the websites.

3. LITERATURE REVIEW

Phishing attacks have many variations such as, malware, bogus web sites, phishing e-mail and identity theft. Malware is the program that is made particularly to perform unauthorized action deliberately [12]. Malware can contain viruses that cause harmful effects on the personal computers

by spreading through the internet and Trojan that opens a backdoor for far-off access and control to an illegal third party. Java script is also considered to be a type of malware, which performs cross-scripting attack [10]. Malware is generally used to steal victim's personal information secretly. They are usually embedded in phishing web sites or attached in e-mail. It will automatically get installed in the personal computer of the user once he visits the site or opens the e-mail. As the user enters his confidential information, it will be leaked out to an eavesdropper. Users should install anti-malware software such as firewall and anti-viruses to protect their computers from such types of phishing attacks. In a malware growth analysis, it was found that decline in e-mail worms in the first quarter of 2005 is due to the improvement in the anti-virus products [18]. In order to deter the malware related phishing attacks anti-Trojan and anti-key logger software programs are used [24].

Another channel for proliferation of phishing messages is phishing e-mail. By pretending to be a trustworthy party phishers send many e-mails and ask receivers to respond with their confidential information or click onto an attached hyperlink which leads to a phishing web site where users are requested to enter their private information or malware is delivered to their personal computers. It is reported in a study conducted by Gartner that 57 million internet users in US received phishing frauds related emails and phishers successfully attracted about 2 million people to release their confidential information [13]. Adopting authentication of incoming e-mails is one of the effective methods to deter such phishing attacks [3]. From a company's perception, one may regard using digitally signed e-mail for company identity confirmation [7]. A lot of companies such as Cisco systems, Microsoft, and Yahoo support the idea of mechanisms to authenticate source of incoming email. Various companies have suggested mechanisms such as Sender Policy Framework, SenderID and DomainKey. Alias email addresses is also very constructive to reduce the potential consequences of disclosing the genuine emails of the customers [15].This is because acquiring e-mail addresses of intended victims is the initial step in any phishing attack [19].

The third channel of phishing attack is through fake web sites. Firstly, phishers make a web site, which has the same look as a trustable third party, and then general public is invited to log on and give away their confidential information for confirmation. A possible way to deter this attack is to make sure that digital server certificate exists of the visited web site. Measures such as trusted path ensured could be taken to combat phishing attacks.

Once they obtain the entire user's confidential data such as username and password from an online banking through any of the above-mentioned methods, they commit identity theft by taking off the victim to deceive the online banking system of the corresponding bank that they impersonate. It was found that one of the major issues for online banking users is the authentication mechanism [21] [14] . For true verification of user's identities, many banks adopt measures such as 2-factor authentication and zero knowledge proof. Although an adversary intercepts a password sent by a customer to a company and imitates the customer by using the same password for the next transaction those measures can effectively combat such phishing thefts [25]. Most common measures are one time password, hardware security box and personal digital certificates [22]. Figure 1 shows various types of phishing attacks and protective measure against them.

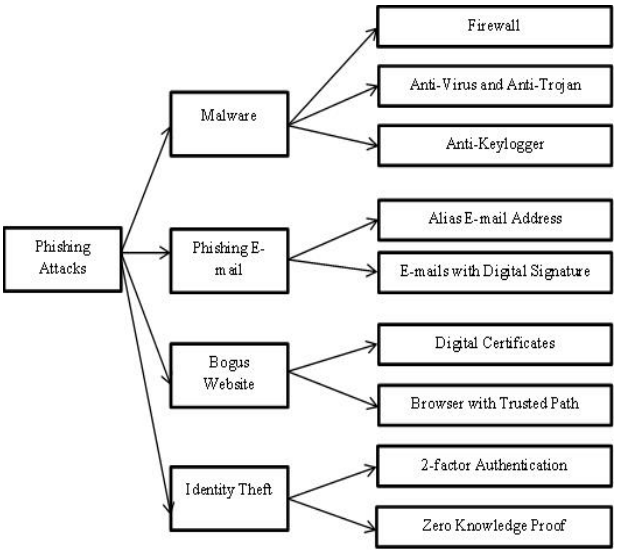

Figure 1: Phishing Attacks and Protective Measures

In a study of Bangladesh banking sector [11] found that the banking sector was vulnerable in terms of information security despite the fact that every bank had its own ICT risk management guideline formulated by the regulator Bank of Bangladesh. A study of Internet banking by mainland China banks found that all the selected banks websites lacked related internet banking security information [23]. While in the case of Hong Kong banks research indicate a partial lack of related internet banking security information in all the selected Hong Kong banks' websites. It was also found that banks placed more weightage on providing information about anti-phishing measures taken by bank than providing phishing-related information to their customers [6]. A study of Internet banking in India found that while all the banks studied used the latest technology for the online security feature they still have small loop holes in their information security infrastructure. Further they don't have any user awareness program to spread phishing-related information [4]. In this research, we will analyze the Pakistani banks websites for relevant phishing-related information and anti-phishing measures adopted as shown in Figure 1.

4. RESEARCH METHODOLOGY

We investigated websites of licensed Pakistani websites offering online banking services. In the first step we identified the banks to be investigated. According to State Bank of Pakistan, the regulatory authority of Pakistani banks, the banks operating in Pakistan can be classified as public sector banks, specialized banks, private sector banks, foreign banks operating in Pakistan, Islamic banks, and micro finance banks. This research was restricted to all banks described above except the micro finance banks. That restricted our selection of banks to 34. Among 34 banks, all except one had their official website. Therefore our subject of study was 33 banks to assess the preparedness of banks against phishing attacks. Each bank was given a unique identifier that varied from 1 to 33. The assignment of identifiers was based on the alphabetical list of banks names (Table 1).

ID	Name of Bank	Online Banking Available
1	Al-Baraka Bank (Pakistan) Limited	No
2	Allied Bank Limited	Yes
3	Askari Bank Limited	Yes
4	Bank AL Habib Limited	Yes
5	Bank Alfalah Limited	No
6	BankIslami Pakistan Limited	Yes
7	Barclays Bank PLC	Yes
8	Burj Bank Limited	Yes
9	Citibank N.A.	Yes
10	Deutsche Bank AG	No
11	Dubai Islamic Bank (Pakistan) Limited	Yes
12	First Women Bank Limited	No
13	Faysal bank	
14	Habib Bank Limited	Yes
15	Habib Metropolitan Bank Limited	Yes
16	HSBC Bank Middle East Limited	Yes
17	JS Bank Limited	Yes
18	KASB Bank Limited	Yes
19	MCB Bank Limited	Yes
20	Meezan Bank Limited	Yes
21	National Bank of Pakistan	No
22	NIB Bank Limited	Yes
23	Samba Bank Limited	Yes
24	Silkbank Limited	Yes
25	Sindh Bank Limited	Yes
26	SME Bank Limited	No
27	Soneri Bank Limited	Yes
28	Standard Chartered Bank (Pakistan) Limited	Yes
29	Summit Bank Limited	Yes
30	The Bank of Khyber	No
31	The Bank of Punjab	Yes
32	United Bank Limited	Yes
33	Zarai Taraqiati Bank Limited	No

Table 1: List of Pakistani Banks

In the second step, we identified banks offering online banking services. Out of 33 banks, 10 banks didn't offer online banking services. Therefore, our assessment of these banks was limited to analyzing the extent to which their websites provided relevant security information against phishing attacks. For remaining 23 banks with online banking services, our investigation is focused on assessing the adequacy of information about phishing, anti-phishing measures related information, and ease of accessibility and anti-phishing phishing related information[1]. As shown in Figure 1, we grouped Information on measures phishing and anti-phishing found on the websites of banks into different groups namely, malware, phishing e-mail, fake Web sites and identity theft. To measure ease of access to anti-phishing information available on bank websites, we counted the minimum number of clicks from the home page to the page containing phishing-related information. In case relevant phishing-related information existed on many pages we counted the average number of clicks. For the analysis of overall preparedness of Pakistani banks in protecting customers online we assessed the phishing-related information and anti-phishing measures adopted along with the facility to retrieve this information, which is measured by the number of clicks required to get this information from the official homepage of the bank [6]. In each category of anti-phishing measures, a score was assigned to each bank on the basis of phishing-related information and information on anti-phishing measures provided on bank website. Finally we calculated a quantitative score that takes into consideration both factors i.e. phishing-related information and information on anti-phishing measures to evaluate the overall preparedness of banks. We used the following formula to calculate the quantitative score.

$$\text{Overall Score} = \sum \text{PRIi} / \text{CPRIi} + \sum \text{APMIi} / \text{CAPMi}$$

Where:

PRIi = Score on phishing related information provided by the bank i

APMIi = Information on Anti-phishing measures provided by bank i.

CPRIi = Clicks required to access phishing related information provided by the bank i.

CAPMi = Clicks required to access information on anti-phishing measured adopted by the bank i.

A score of 1 indicated the availability of information on bank website while a score of 0 indicted the absence of such information. This formula takes into consideration both the availability of phishing-related information and accessibility of such information. Thus the formula provides a detailed situation of overall preparedness of banks to prepare their customers online.

5. RESULTS AND DISCUSSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

5.1 Banks without Online Banking Services

For 11 banks without online banking, we determine the preparedness of the bank by evaluating the extent to which relevant information related to phishing available on their official websites. None of the banks provided information on phishing and relevant safety tips on their websites. Table 2

[1] There could be multiple paths to the same page.

lists the names of banks and the degree of preparedness against various categories of access to phishing-related information.

ID	Security tips against phishing or other online fraud	Information related to various categories of phishing attacks	Promotional activities with anti-virus and anti-spyware vendors
1	X	X	X
5	X	X	X
10	X	X	X
12	X	X	X
21	X	X	X
26	X	X	X
30	X	X	X
33	X	X	X

Table 2
Anti-phishing measures adopted by Pakistani Banks with official web site but no online banking service

5.2 Banks with Online Banking Services

For the 25 banks with online banking services, we reach the readiness of banks using the following criteria.

Information on phishing	Brief safety tips to protect online banking, glossary related to phishing, security alerts and information about phishing, fake websites or spam e-mails
Anti-phishing measures	Firewalls, Anti-virus, Anti-keylogger, Anti-Trojan, Alias e-mail, e-mails with digital signature, trusted path browsers,128-bit SSL encryption, Digital Certificates, Automatic disconnection after a few minutes of inactivity, Account suspension after several failures account login, Customer Service / incident safety hotline, Last login timestamp, The security team to keep track of attempts to break the security system, Two-Factor Authentication (Personal digital certificate, One time password (OTP), hardware device), Random session key, Zero Knowledge Proof

In terms of information dissemination phishing we find that about 90% of banks provide safety tips related to online banking on their official websites. About 40% of banks provide security alert related to phishing, fake Web sites, or spam. No bank provided a glossary of jargon to facilitate the understanding of phishing jargons related to security or related online.

In terms of anti-phishing all banks provide measures such as SSL 128-bit data encryption (100% adoption) and digital certificate server (100% of adoption). Other measures such as self-disconnection (100% adoption), account suspension (80% adoption), customer service / hotline to security incidents (90% adoption), and the timestamp of the last connection (45% adoption) have average adoption rate. In addition, we find that 70% of banks say they have a firewall and anti-virus software installed on their servers. Measures such as the security team to keep track of the entire online banking system are less popular, with only an adoption rate of 25%. For the mechanism of protection against identity theft as two-factor authentication (more than 45% adoption) and the random session key (3% adoption), the adoption rate is generally slightly less than 50%. In the category of two-factor authentication, personal certificates to verify the identity of users are most popular with adoption rates of 45%.

In terms of ease of access to information about phishing, it appears that on the websites of around 17% of the banks relevant information can be found on a special page devoted to online safety. 20 % banks put this information in the form of frequently asked general questions (FAQ). Almost all banks make this information with a general description of the online banking on the same page. To measure the accessibility of information phishing and anti-phishing measures we then counted the number of clicks required to travel to the home page of the bank to the page containing the information. We used the following criteria to assess the accessibility of phishing information and anti-phishing measures.

Number of Clicks Required	**Level of Accessibility**
1-2	Easy
More than 2	Difficult

It was found that in terms of accessibility of information about phishing most banks require 2 clicks from the home page to the page containing official information. In terms of accessibility of measures of anti-phishing, it is found that most banks require between 1to 2 clicks from the home page to the page containing official information.

It is also found that very few banks provide information related to identity theft on their websites. This information includes tips on preventing information from being slipped to third, two-factor authentication and online security jargons related to identity theft. For other types of phishing very few banks provide relevant information. Very few banks provide information related to malware (such as virus and Trojan) alerts, information related to phishing e-mail such as phishing e-mail alert and ways to identify phishing e-mail and bogus websites.

ID	Malware			Phishing E-mail			Bogus Websites			Identity Theft		
	Security Tips	Security Alerts	Security Jargon	Security Tips	Security Alerts	Security Jargon	Security Tips	Security Alerts	Security Jargon	Security Tips	Security Alerts	Security Jargon
2	1	1		1	1		1	1		1	1	
3	1	1		1	1		1	1		1	1	
4		1		1			1			1		
6	1						1					
7	1			1			1			1		
8												
9	1	1		1	1		1	1		1	1	
11	1			1								
14	1	1		1	1		1	1		1	1	
15	1			1			1			1		
16				1							1	
17	1			1			1			1		
18	1			1			1			1		
19	1			1			1			1	1	
20	1	1		1	1		1	1		1	1	
22	1			1			1			1		
23	1	1		1	1		1	1		1	1	
24	1			1			1			1		
25											1	
27	1	1		1	1		1	1		1	1	
28	1	1		1	1		1	1		1	1	
29	1			1			1			1		
31												
32	1			1			1			1		

Table 3
Phishing-Related Information Provided By Banks with Online Banking Services

ID	Malware				Phishing E-mail		Bogus Websites			Identity Theft								
	Fire wall	Anti-Virus	Anti-key logger	Anti-Trojan	Alias E-mail	Digital Certificates	Trusted Path Browser	Security Response Service	Digital Certificate	Hardware Device	One-time password	Digital certificates	Random Session Key	Zero Knowledge proof	Auto Logout	Auto Suspension	Last Logon time stamp	SSL	Security Team
2	1	1				1			1		1	1			1	1	1	1	1
3	1	1				1			1						1	1	1	1	
4	1	1				1			1			1			1	1	1	1	1
6	1	1				1			1						1	1	1	1	1
7	1	1				1			1			1			1	1	1	1	
8	1	1				1			1			1			1	1	1	1	1
9	1	1				1			1						1	1	1	1	
11	1	1				1			1						1	1	1	1	1
14	1	1				1			1								1	1	
15	1	1				1			1						1	1	1	1	
16	1	1				1			1			1			1	1	1	1	1
17	1	1				1			1			1					1	1	
18	1	1				1			1						1	1	1	1	1
19	1	1				1			1						1	1	1	1	
20	1	1				1			1								1	1	1
22	1	1				1			1			1			1	1	1	1	
23	1	1				1			1			1					1	1	1
24	1	1				1			1						1	1	1	1	
25	1	1				1			1			1			1	1	1	1	1
27	1	1				1			1						1	1	1	1	
28	1	1				1			1			1			1	1	1	1	
29	1	1				1			1						1	1	1	1	1
31	1	1				1			1						1	1	1	1	
32	1	1				1			1						1	1	1	1	1

Table 4
Anti-Phishing Measures Information provided by Banks with Online Banking Service

In the category of identity theft banks generally provide several alternative control measures against phishing such as SSL 128-bit encryption, automatic account disconnection after a set period of inactivity, account suspension after several unsuccessful attempts, the timestamp of the last connection, digital certificate, and SMS-based alerts. For action against fake websites, the most common measures are digital server certificate and incident report service. The third most common measure is the installation of firewall and anti-virus. It is not surprising that almost all banks say they have adopted these measures. For the category of phishing e-mail, banks rely primarily on educating clients. In addition to providing relevant information about phishing measures, the Pakistani banks do not adopt other possible measures against phishing attacks.

ID	Total Score for Phishing-Related Information	Total Score for Information Related to Anti-Phishing Measures	Sum of Two Scores
2	8	11	19
3	8	10	18
4	4	10	14
6	2	10	12
7	4	10	14
8	0	10	10
9	8	10	18
11	2	10	12
14	8	8	16
15	4	10	14
16	2	10	12
17	4	8	12
18	4	10	14
19	5	10	15
20	8	8	16
22	4	10	14
23	8	8	16
24	4	10	14
25	1	10	11
27	8	10	18
28	8	10	18
29	4	10	14
31	0	10	10
32	4	10	14
Mean	4.7	9.7	14.17
S.D	2.72	0.8	2.46

Table 5
Overall score of banks with Regard to Preparedness for Protecting Customers Online

As shown in Table 5, an imbalance of information provided by bank websites related to measures of phishing and anti-phishing exists. The average score of information relating to anti-phishing measures is 9.7, which is higher than the average of the information on phishing, which is 4.7. This indicates that banks are more willing to provide information on the anti-phishing that information related to phishing. On the other hand, a smaller variation in the information relating to anti-phishing measures between Pakistani banks as revealed by the standard deviation (which is 0.8), while the variation is large compared with information on phishing (standard deviation 2.72). When taking into consideration the overall preparedness based on two types of information provided by the banks, most banks achieve a score of about 12 with 14.17 as the average of the overall score. However, the number of banks that provide only information on anti-phishing measures related information without any phishing-related information is high which leads to a large change in the overall score (standard deviation 2.46).

6. FUTURE RESEARCH

In this research, we analyzed the preparedness of the Pakistani banks to protect their customers online by assessing the variety of phishing-related information and ease of access to this information from the websites of banks. This study gives an insight to individual banks to better design their websites and prepare for responding well to protect their customers from increasing phishing threats. However, this study does not take into account the influence of information on the behavior of bank customers. One of the objectives of providing information about phishing and anti-phishing measures on bank websites is to inform customers about potential phishing attacks and possible strategy to prevent

such offenses occurs. To obtain a more complete picture of the overall success of the anti-phishing preparedness of banks, it is necessary to assess whether awareness of end-users in terms of phishing is actually improved through information provided by the website of each bank or not.

5. CONCLUSION

From this research, it is found that most Pakistani banks that offer online banking services are concerned about phishing and provide necessary anti-phishing measures to protect its customers. None of the banks which do not provide online banking inform their users about potential phishing attacks on their official websites. Among the banks that offer online banking, it is found that most of the banks inform their customers about the security of online transactions (90%). In addition, about 40% of banks provide a whole page dedicated to online security, which reflects concern of most banks. In addition, most web pages that provide information related to phishing is easily accessible by visitors, with only two clicks are needed on average to get these pages from the official homepage of the bank. In terms of mechanism against phishing all banks with online banking services adopt anti-phishing measures such as SSL 128-bit encryption and digital certificates. The adoption of other anti-phishing techniques varies from bank to bank. Common measures adopted include automatic logout, account suspension, the last stamp of the connection, and the security incident response team. While the adoption rate of other measures is high, the rate of adoption for security incident response team is less than 50%. Two-factor authentication is considered the most sophisticated anti-phishing measure. However, few banks providing online banking services adopted such anti-phishing measures. The rate of adoption of two-factor authentication is approximately 40%. This may be due to higher operating expenses related to the adoption of such a measure. This seems to imply that the cost is an important factor in the choice of a specific measure of deterministic two-factor authentication. Many banks advise their users online banking to install firewalls and anti-virus protection against phishing, 100 % of banks say they have installed these programs on the server side. It indicates that banks view these anti-phishing measures to be valid enough to be mentioned in their official website. In terms of access to anti-phishing measures adopted by banks, it is much easier to access the information as information about phishing. It seems that banks favor anti-phishing measures more than phishing related information. In summary, the Pakistani banks with online banking services are quite aware of the problem of phishing than banks without banking online. In terms of accessibility of anti-phishing information and anti-phishing measures on banks' websites compatible electronic banking, anti-phishing measures are much more easily accessible. We also observe that the measures against identity theft are most commonly adopted by banks than measures against other types of phishing attacks. It is encouraging to see that measures such as 128-bit SSL encryption are adopted by all banks, measures relating to the two-factor authentication have an adoption rate of about 50%, and the digital certificate server is adopted by all banks.

REFERENCES

[1] Abdullah, A.-K. (2004). "*Protecting your good name: identity theft and its prevention*". In Proceedings of the 1st annual conference on Information security curriculum development (pp. 102–106). New York, NY, USA: ACM. doi:10.1145/1059524.1059547

[2] Anti-Phishing Working Group. "*Phishing activity trends report*" June 2012. (2012). Retrieved from http://anti-phishing.org/reports/apwg_trends_report_q2_2012.pdf

[3] Bellovin, S. M. (2004). "*Spamming, phishing, authentication, and privacy*". Communications ACM, 47(12), 144–. doi:10.1145/1035134.1035159

[4] Bhutt, S. C. (2011). "*Study of Indian Banks Websites for Cyber Crime Safety Mechanism*". International Journal of Advanced Computer Science and Applications, 2(10). Retrieved from http://thesai.org/Downloads/Volume2No10/Paper%2014-Study%20of%20Indian%20Banks%20Websites%20for%20Cyber%20Crime%20Safety%20Mechanism.pdf

[5] Bose, I., & Leung, A. C. M. (2007). "*Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities*". Communications of the Association for Information Systems, 19(1). Retrieved from http://aisel.aisnet.org/cais/vol19/iss1/24

[6] Bose, I., & Leung, A. C. M. (2008). "*Assessing anti-phishing preparedness: A study of online banks in Hong Kong*". Decision Support Systems, 45(4), 897–912. doi:10.1016/j.dss.2008.03.001

[7] Garfinkel, S. L., Margrave, D., Nordlander, E., Miller, R. C., & Wa, S. (2005). "*How to make secure email easier to use*". In In Proceedings of the Conference on Human Factors in Computing Systems (CHI (pp. 701–710). ACM Press.

[8] Gartner. (2009, April). "*Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008"*. Retrieved from http://www.gartner.com/newsroom/id/936913

[9] Geer, D. (2005). "*Security technologies go phishing*". Computer, 38(6), 18 – 21. doi:10.1109/MC.2005.201
James, L. (2006). *Phishing Exposed* (1st ed.). Syngress.

[10] Johns, M. (2008). "*On JavaScript Malware and related threats*". Journal in Computer Virology, 4(3), 161–178. doi:10.1007/s11416-007-0076-7

[11] Khan, M., & Barua, S. (2010). "*The Status and Threats of Information Security in the Banking Sector of Bangladesh: Policies Required*" (SSRN Scholarly Paper No. ID 1569207). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1569207

[12] Kienzle, D. M., & Elder, M. C. (2003). "*Recent worms: a survey and trends"*. In Proceedings of the 2003 ACM workshop on Rapid malcode (pp. 1–10). New York, NY, USA: ACM. doi:10.1145/948187.948189

[13] Kirda, E., & Kruegel, C. (2005). "*Protecting Users Against Phishing Attacks with AntiPhish*". In Proceedings of the 29th Annual International Computer Software and Applications Conference - Volume 01 (pp. 517–524). Washington, DC, USA: IEEE Computer Society. doi:10.1109/COMPSAC.2005.126

[14] Lao, G., & Wang, X. (2010). "*Study of Security Mechanisms in Personal Internet Banking - Take China Merchants Bank as an Example*". In 2010 International Conference on Computational Intelligence and Software Engineering (CiSE) (pp. 1 –4). Presented at the 2010 International Conference on Computational Intelligence and Software Engineering (CiSE). doi:10.1109/CISE.2010.5676896

[15] Lawton, G. (2005). "*E-Mail Authentication Is Here, but Has It Arrived Yet*?" Computer, 38(11), 17–19. doi:10.1109/MC.2005.377

[16] Lenton, D. (2005). "*Bigger phish to fry"*. IEE Review, 51(10), 26 –27. doi:10.1049/ir:20051001

[17] Lininger, R., & Vines, R. D. (2005). "*Phishing: Cutting the Identity Theft Line*" (1st ed.). Wiley.

[18] Mannan, M., & Van Oorschot, P. C. (2005). "*On instant messaging worms, analysis and countermeasures*". In Proceedings of the 2005 ACM workshop on Rapid malcode (pp. 2–11). New York, NY, USA: ACM. doi:10.1145/1103626.1103629

[19] McAfee. (2004). "*Anti-phishing: Best practices for institutions and consumers*". Retrieved from http://docs.apwg.org/sponsors_technical_papers/Anti-Phishing_Best_Practices_for_Institutions_Consumer0904.pdf

[20] McCombie, S., Pieprzyk, J., & Watters, P. (2009). "*Cybercrime attribution : an Eastern European case study*" | Macquarie University ResearchOnline, Cybercrime attribution : an Eastern European case study. Retrieved from http://www.researchonline.mq.edu.au/vital/access/manager/Repository/mq:12626

[21] Nilsson, M., Adams, A., & Herd, S. (2005). "*Building security and trust in online banking*". In CHI '05 Extended Abstracts on Human Factors in Computing Systems (pp. 1701–1704). New York, NY, USA: ACM. doi:10.1145/1056808.1057001

[22] Purkait, S. (2012). "*Phishing counter measures and their effectiveness – literature review*". Information Management & Computer Security, 20(5), 382–420. doi:10.1108/09685221211286548

[23] Subsorn, P., & Limwiriyakul, S. (2012). "*A Case Study of Internet Banking Security of Mainland Chinese Banks: A Customer Perspective"*. In 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN) (pp. 189 –195). Presented at the 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN). doi:10.1109/CICSyN.2012.43

[24] Tang, Y. (2006). "*Defending against internet worms*". University of Florida, Gainesville, FL, USA.

[25] Viega, J. (2005). Security – "*Problem Solved?*" Queue, 3(5), 40–50. doi:10.1145/1071713.1071728