International Journal in Advances in Information Sciences and Service Sciences 2011; 3(10.61):505-509.

ELECTRONIC BANKING FRAUD; THE NEED TO ENHANCE SECURITY AND CUSTOMER TRUST IN ONLINE BANKING

Rashad Yazdanifard[1], Wan Fadzilah WanYusoff [2], Alawa Clement Behora[3]¸ Abu Bakar Sade[4]

[1, 2, 4] Faculty of management, Multimedia University, Cyberjaya Malaysia
rashadyazdanifard@yahoo.com , wanfadzilah@mmu.edu.my, absade@mmu.edu.my

[3] Faculty of Business studies and Globalization, Limkokwing University of Creativity Technology, Cyberjaya, Malaysia
albudus@yahoo.com

Abstract

The online banking industry has grown rapidly over the past years, and will continue to experience increase as financial institutions continue to encourage customers to do online banking transactions such as money transfer, access information about the account or otherwise as well as payment of monthly bills. During this time Internet criminals and fraudsters attempting to steal customer's personal information have hunted down the online banking. This paper took the liberty to look into the means by which fraudulent activities are committed and what banks are doing to stop these activities as well as the new security measures that the banks are using to increase customers trust. This Article is based on electronic banking fraud and the need to enhance security and customer trust in online banking.

Keywords: *ELECTRONIC BANKING, FRAUD, SECURITY, CUSTOMER TRUST*

1. Introduction:

Electronic banking is also known as internet banking or e-banking, it has rapidly grown in the passed years [1] the electronic banking offers variety of banking services which include (EFT), electronic transfer of funds, automatic teller machine, (ATM) services and direct deposits automatic bill payment, (ABP) [2]. It is also a good profitable medium for financial institution. This banking system is cheaper when compared with the traditional banking system and it offers the customer the flexibility and comfortability. The increase in growth of online banking now suffers challenges due to attacks and the risk of fraud (phishing) data compromise [3]. The increase in the attack has led to decrease in the use of online banking and has negatively reduced consumers' trust in the ability of financial bank institution to protect them. Consumers are now worried about the safety of their money and information and are expecting the bank to find a solution that can protect them [3][21].

2. Methods of Online Banking fraud

Ways that are involved in conducting online banking fraud; first customers account access data [4] log on name and password are obtained. The criminals withdraw any funds transfer (money) to other accounts using the information.
Since the introduction of online banking in many years ago, there has never been a case reported on online banking fraud until early 2004 [4] where cases reported on fraud nearly exploded and banks are finding the means of securing their online banking activities. The fraudsters use various means to obtain customer's personal bank details and information [4].

Phishing[5] RSA, [6]BundesverbanddeutscherBanken, using a false web site, address or name for fraudulent purposes, [4], fake e-mail or fake websites send to customers that looks as if its from their banks that lead customer to a fake website. The fraudsters are able to access customers data by impersonating the bank website by asking customers to provide their access code or details. [4],

[7].Online banking fraudsters also have new tools in their possession that is suitable to use with any advance crime ware.
Well established cyber criminals conduct a full scale impersonation in authentication influence and widespread of virus into end user's computer with banking Trojan to sneak into online banking account successfully and undetected [8] [9]. They also have a new form of attack spyware, Trojan horses, as well as kelloggers.It causes customers to unwillingly download Malware, a computer code download with bad intention to harm customer by collecting customers' information [10].

Data released by FFA UK[11] has indicated that there has been a 14 per cent increase in on line banking fraud, $53million in 2008 to $60million 2009, which summed up to overall total of increase of $48million since [12] the first time online banking fraud case was reported in the year. This increase is due to a rise in usage of more sophisticated tool by the criminals to target online banking customers through malware which aim at vulnerabilities in consumer's computer instead of the bank's own system which attacks are more difficult. [12]. The amount of committed online fraud attacks identified by RSA [8] was 18,079 worldwide and there was 11 per cent increase from January. The number of fraud for the first time close to a year has reached up to 18000 in one month.

3. What to expect 2011 reported by Cybercrime.

Cybercrime trend; Trojan Wars[8] RSA. [6] Trojans are programs that without the knowledge of the user, compromises computer. [8] New features are shorter and develop cycle in competition between malware developers in the black market [8] cybercrime trend.
The number one worldwide-recognized malware in the online banking fraud is known as the Zeus Trojan "defacto"[8] RSA. It is responsible for about 90 per cent online banking fraud worldwide after estimate was done since its introduction into the black market. Zeus has become like almost a brand version of a Trojan. Spyeye author Hardeman has already declared his plans of the new Trojan 2011 a Ring-o or Kernel mode (which been seen only in sinowal)[8].

Accepting the fact that Zeus Trojan HML infection is stronger, Hardeman the producer of spyware said to study more to be able to implement new hybrid Trojan. If Hardeman successfully completed his plan that proves that new malware will be commercially available and be sold underground 2011. The new Zeus 2.1 will have the capability to keep data in different language.

4. Improve on Business Online Banking Trust And Security Against On Line Fraud.

Trust refers to a decisive instrument in stimulating purchase over the internet [13]. According to [6] Suh and Han trust is the most important factors that determines customers acceptance of online banking, that is why it is very important to maintain customers confidence at all times. [14] Maria Bruno-britz

A clear detailed arrangement can bring increase in customer's trust and beliefs in relation to bank and its intention to trust, therefore, reading security declaration will enhance perceived trust in electronic banking.

i. Enhancing Communication And Transparency About Bank Fraud And Security, According to research survey [9] 24 percent of customers said their banks do not present them with a policy explaining its duties to secure and provide protection companies account from fraud, 39 per cent are not so sure if such a policy even exist. Clarity security expectation [10] is very important to successful relationship with customers. Banks should take the time to ensure their customers know their policies and understand how to protect them. [15] Aweb page should be created to educate customers on online banking in particular with the rights and responsibilities protecting their information when executing a transaction [22].

ii. Refund, Arrangement Effectiveness on trust: By being given a refund guarantee, the risk of threat is transferred to the bank providing the online services. This state's clearly that guarantee by which the bank takes responsibility for any unauthorized online transactions to increase customers 'trust. This type of approach is used by Barclays Bank [13].

iii. Introduce a Layered Security Strategy [16] And Analyze Solutions That Will Help Deliver on Proactive Security And Customer Comfortability Without Overburden: There is no Amount of Solution target that will stop online banking fraud activities, an expert suggest a layered method using transaction solution [4] that complement existing security solutions. Banks should look for methods that can increase detection with the lowest false positive alerts. Solution that can predict and survey users online sessions to differentiate between fundamental and legitimate activities that provide highest degree of protection without any overburdening [9].

5. Dualing For Control Prevention Tips And Enhancing Security In On Line Banking:

In 2009 record about fraud attacks [17] against electronic banking business show no sign of stopping, online criminals have increase their technologies and methods to continue to obtain millions from online accounts, even with the effort by banks to improve security measures. Research from the 2010 online business banking [17] trust study states that 80 per cent fraud attacks, money has already left the bank before realizing it, leaving banks confused on how to fight against online frauds.

a. KeCrypt-Not Possible To Forge, Fake or Fool:
The KeCrypt security measure is different in identity management in the sense that it never records the image or template of signature. This means that there is nothing to steal or copy. This is possible by recording the dynamic biometric component of the signature pressure and speed. It is impossible for someone else to recreate dynamic biometric, it doesn’t matter how much time they have, the KeCrypted signature cannot be fooled as it has been tried and proved, the patented solution is 100 per cent [18].

b. Multifactor Authentication:
Based on risk other banking institutions have introduced multifactor authentication by providing a token for online business banking customers for cash management system. Here if a consumer requested a transaction that is unusual “high risk” the electronic banking system will challenge the person with more additional questions that were asked at the time of account opening but this method is not deployed globally by banks because it will be very costly [16].

c. New Users Who Approve or Request Large Transfer Immediately:
New account users who request or approve large amount are usually associated with high risk, banks should be aware of them, identify and investigate account with new users added. Accounts associated with a lot of high-risk behavior should be on top list of banks investigation [18].

d. Spyware Protection:
To help protect one’s computer from spyware, an anti spyware program can be used .A program called window defender, a version of windows has built-in antispyware, which can be turned on by default. This program alerts you when spyware tries installation by itself in the computer. It can also scan the computer for existing virus spyware and remove it [19].A personal Firewall, is another way of protecting users PC from attacks, This program monitors all outgoing and incoming information between PC and the internet and only familiar authorisedconnections are allowed [6].However Consumers will only acknowledge security measures presented in the right manner [20].

6. Discussion

A literature review of electronic banking and the need to enhance security and customer trust in online banking. In the digitalized world of today, we can all see how important this issue has become in our society. This discussion review some activities or transactions that are perfumed via online banking. The means through which fraudulent activities are committed and how to avoid them as well as to enhance customer trust in online banking.

Electronic banking performs different type of activities ranging from paying bills online, fund transfer and using the ATM to deposit and make cash withdrawals. It has changed the behaviors of people and even how they spend money and the nature of some businesses, and money can be transferred from any part of the world for business purposes, by just a click on your computer at home.

Since the introduction of online banking, there have been rapid increases in its growth until 2004 when the first case of online fraud was reported, which is now causing a decline in the nature of online banking. The criminals' uses different methods or software such as Fishing; accessing into customers account by sending them fake e-mails telling them to submit their personal information. They use Trojan Zeus, which is the latest one and the most powerful tool to infect virus into users computer stealing their data and information that will enable them to carry out their fraudulent activities. The online banking business has suffered great decline because of these flatulent activities.

This attacks has also affected customer trust to online banks and their confidence that the banks are unable to protect their assets and money which now lead banks to spend extra money seeking for solution in other to gain back their customers trust. The numbers of fraudulent activities committed identified by RSA was 18079 worldwide with 11 per cent increase from January 2011.Saveral banks and institution has come up with new approach in developing customer trust which includes enhancing communication and transparency about banks fraud and security, refund arrangement effectiveness on trust and introducing layered security strategy as well as analyzing solution that delivers customers trust and comfortability. In order to achieve this the banks were able to introduce some security measures that are able to reduce fraudulent activities like the implementation of KeCript- not possible to fake, forge or fooled tested and proved100 per cent protection, multifactor authentication that challenge suspected transaction by asking the user for additional questions. The use of spyware software to protect computers against Trojan virus and removing them from infected computers as well. All of the discussion and the improvements are to encourage people to bank online and to increase security against fraud criminals as well as customers trust.

7. Conclusion

In conclusion this article reveals the major activities of online banking, how people's attitudes can cause an increase or decrease in the banking sector, for example there were rapid increase growth in online banking since it started until the first fraudulent case were reported in 2004, the criminals trick customer to submitting their bank personal details by the use of Trojan software fishing, sending fake e-mails which they later use to steal the customers money. This activities has negatively affected customer trust in the ability of banks to protect customer's money and asset that's why today there is a great decline in the online banking operation. But with the increase in this fraudulent activities the online banking sectors are working so hard to reduce this activities by implementing unique security protection like the KeCrpt which provide 100 per cent protection against fraudsters, as well the introduction of spyware that protect ones computer against computer hackers. With this researchers think adding Refund Arrangement Effectiveness on trust Enhancing Communication And Transparency About Bank Fraud And Security will help gain back customers trust. So the threat of online banking fraud still remains active as Hardeman is studying hard to deliver the 2011 Trojan Zeus which is considered the most strongest. The fight for protection, improving security and enhance customers trust continues in online banking sector still continues.

8. References

[1] Kennet B. yap, H. Wong Claire Loh, Yuan-shuh Lii. A Model of customer e-loyalty in the online banking. Feng Chia University, Taiwan and University of westren Australia, Perth Australia. Volume 29, no.2 pp.891-902. Published : May 06, 2009.

[2] Jane.M.Kolodinsky, Jane M.Hoenth and Mariam A. USA the adoption of electronic banking technology by US consumer. University of verment, Burlinton, verment, Higert federal reserve board, Washington DC, USA. March 2004.

[3] Gregory D. Williamson, GE Money- America's . Enhance authentication in online banking. Journal of economic crime management, volume 4 issue 2, Fall 2006.

[4] Jarek Nabrzyski, Jannifer M.Schopf and Jan Weglarz. Gread Resource Management State of the Art and Future Trends. ISBN 1-4020-7575-8, Published on 2003.

[5] Allan Friedman, PatrickCroweley and Daniel West. Online identity and consumer trust assessing online risk. Center for technology innovation at brooklings , 11th January, 2011.

[6] Bo Xu and Surya Yadav. Effect of onine Reputation service in electronic markets: A trust-Based empirical study. Ninth Americas Conference on Information Systems. 2003.

[7] James T.Hamilton. All the news that's Fit To Sell: How to market transforms information into news. (ISBN 0-691-11680-6 alk. Paper) Published on 2004.

[8] Lewis, Charley. Empowering regulators to protect consumer rights in the ICT sector: Final technical report. Published on 12th February 2011.

[9] Stelios C.Zyglidopoulos. Framing the corporate world : The impact of corporate Social Performance on Media Attention and Prominence of Business Firms. University of Cambridge, 16th International Conference on Corporate and Marketing Communicatios.

[10] Press Release, Metavate Introduces New Onine Fraud Solution, In December 2005 RSA Security acquired Cyota. A New York-based anti-fraud company. Wednesday, March 15, 2006.

[11] Bernard Herdan, National Fraud Authority, Annual Fraud Indicator, AFI, Published January 2011.

[12] A Monthly Intelligence Report from the RSA Anti-Fraud Command Center. RSA onine fraud report. Published on February2010.

[13] Franco-leviaTeodoroleque, Martinez Juan Sanchaze-Fernadaz. How to improve trust towards electronic banking. Department of marketing and market research, University of Granada, Granada, Spain. 14th March, 2010.

[14] Maria Bruno Britz. Banks Using Security to Increase Customer Trust and Their BottomLines. 24th May, 2007.

[15] Larry Ponemon. Business Case for Data Protection and Datamonitoring. Strategic Focus Report, Ponemon Institute Private and Condifential Document. Security in online Banking. July 31, 2009.

[16] TrustCC. Safer Onine Banking New Guidance , Publication date 26th Feb 2011.

[17] Dualing for control and fraud information. Guardian annalistic, August 2010.

[18] KeCrypt System Ltd. Category: Unique Biometric Security. Unique biometric security option to solve online banking Fraud. 27th April. 2010.

[19] Windows understanding security and safer computing. Windows, Microsoft Corporation , 2011.

[20] George Tubin Senior Analyst. The Sky Is Falling: The Need for Stronger Consumer Online Banking Authentication. Publication date, April 2005.

[21] Joseph Cosmas Mushi, Guan-zheng Tan, Felix Musau, Cheruiyot Wilson, "Performance Analysis of Recharging Scheme of M-SaaS through M-banking", JCIT, Vol. 6, No. 7, pp. 140 ~ 153, 2011

[22] Zhiyong Li, Sedeka Mahmoud El Shamy, Tamer Galal, , "A Novell Security Framework for Web Application and Database", JDCTA, Vol. 5, No. 10, pp. 190 ~ 198, 2011