Impact of Online Threats on Usage of E-Banking

Tejinder Pal Singh Brar[1], Dr. Dhiraj Sharma[2], Dr. Sawtantar Singh Khurmi[3]
[1]*Research Scholar, Punjab Technical University, Kapurthala*
[2]*School of Management Studies, Punjabi University, Patiala*
[3]*Bhai Maha Singh College of Engineering, Kotkapura Road, Muktsar*

Abstract - This study is an attempt to dissect the impact of online threats that affects on the usage of E-banking by retail customers. In general, it seeks to examine customer's perspective towards fear of various online threats. The data for this study are collected from retail customers. The sample consists of 240 retail customers from public and private sector banks. Data was collected through pre-tested questionnaires. All the retail customers were based in northern India. It has been found that after providing different security mechanisms, customers are still feared about online threats and hence hesitate to transact through online mediums. It is vital to provide robust security mechanisms while conducting transactions via electronic means.

Keywords: *Retail customers, Security, E-banking, Trust*

I. INTRODUCTION

The unabated plundering of E-banking accounts belonging to retail customers are raising doubts about the authentication and fraud-detection mechanisms now used by banks. In most of those cases, online criminals obtained a retail customer's valid banking log-in credentials by illegal means. Such online threats have prompted government regulators to call on banks to improve their security systems. Most of the online thefts occurred because the customers failed to adequately protect their banking credentials. These kinds of online thefts have impact on public relations because banks are not required to reimburse stolen amount. According to [Yousafzai et al. (2009); Pieters (2010); Avizienis et al. (2004)], trust in the banking sector has not yet been fully translated in the online environment because trust is difficult to achieve without face-to-face interaction and it is doubtful that artificial agents are capable of trusting and/or being trusted. Technology-related variables are also imperative as traditional factors in predicting customer's behaviour in online environment. Online threat landscape has been changed because online attackers have adopted more intricate methods to break online verification techniques.

Advanced levels of security may make online banking more useful**, [Alnsour and Al-hyari (2011); Friedman et al. (2000)**; **Gefen et al. (2003); Jarvenpaa et al. (2000); Ponemon (2005)**]. With higher belief in online banking, the more a customer trusted the bank and its website. [**Yousafzai et al. (2003)**; **Grewal et al. (2004); Avizienis et al. (2004)**] found that customers have not adopted B2C e-commerce in the same way primarily because of risk and trust related issues. After examining E-banking risks **Goetz E. (2003)** reported that banking industry faces a massive amount of physical and cyber threats from hackers and malicious insiders. Vishing and phishing attacks can easily steal passwords. When we examined social networking websites, we found that a large number of answers to challenge questions can be easily found from these online resources.

According to a survey conducted by Kaspersky Lab and B2B International, around one third of customers in America users do not feel safe when conducting financial transactions, **Alfreds (2013)**. Despite adoption and growth of online transactions by retail customers, the customer base is still low when compared to traditional banking. **Calonia (2014)** reported four biggest fears customers have about online banking. It includes identity theft, technology hiccups, misuse of information and lack of documentation.

NCRB (2013) reported state-wise scenario in India; 4,356 cases were registered under IT Act during the year 2013 as compared to 2,876 cases during 2012, thus showing an increase of 51.5% in 2013 over 2012. Similarly, according to **Gurung (2014)** there is an increase in the cyber crime by 51%. Table 1.0 shows incidences of registered cases in top 10 states of India during 2013 and their comparison with cases registered in 2012.

TABLE 1.0: YEAR WISE COMPARISON OF DIFFERENT CRIME HEADS IN INDIA

Number of authors argued that despite ongoing security efforts, banking sector remains vulnerable to a variety of events [**Goetz (2003); Dapp (2012); Chickowski (2006); Klein (2007)**; **Aladwani (2001); Bradley and Stewart (2003)].** Customers are worried about security and ready to move to another bank after only a single security breach. **Sathye (1999)** conducted study in Australia and found that security concerns and lack of awareness about the internet banking were the two main obstacles for the non-adoption and less usage of E-banking. **White and Nteli (2004)** found that UK customers ranked the security of bank's website as the most important attribute of internet banking service quality. Similarly, Indian customers are concerned about security and privacy issues, **Malhotra and Singh (2009)**. Online security

is the most important factor in adoption and usage of E-banking [**Liao and Cheung (2002); Mukti (2000)]**.

[Dinesh (2011); Kitten (2014); Schwartz (2014); Karimi (2014); Finkle and Henry (2013); Kumar (2014); Tripathy (2014)] reported data breaches that are happening around the world. While analyzing Indian scenario **Bipindra (2014)** mentioned Defense Research and Development Organization's (DRDO) computers were hacked by Chinese hackers and The malware collected and transmitted confidential files and documents to Chinese IP addresses, **[Information Age (2012)**]. Similarly a report from the University of Toronto in 2010 alleged that Chinese hackers had accessed Indian military systems. Nearly 80% of U.S. banks think that malware is a top security risk. Indeed this seems justified because U.S. consumers lost over US$ 2 billion and 1.3 million PCs to malware in 2010.

Solutions and recommendations for safe E-banking were offered by several studies like **Infosys (2010)** insisted on implementation of mandatory and strong controls whereas **Alsajjan and Dennis (2006)** advised banks should publicly advertise the safety and informative issues. **Fatima (2011)** suggests that banks must be more responsive towards security requirements while **Dandash et al. (2008)** on the other hand proposed an efficient new scheme which can prevent fraud by applying different security algorithms, generating and updating limited-use secret keys. It uses advanced authentication technologies and is well adapted to any possible future technology. [**Bala and Norita (2011)**; **Viega and McGraw (2001)]** suggests developers have to incorporate security during the development process itself in order to produce software assurance systems. Infect, no single security solution is enough to defend against today's versatile attacks. In spite of innovation in security technologies, fraudsters still manage to breach banks' resistance from time to time.

II. RESEARCH OBJECTIVES AND METHODOLOGY

The primary objective of this research study is to inspect the impact of online threats that affects usage of E-banking by retail customers. This section represents research methodology. Section-3 primarily deals with customers' perspective towards online banking security and statistical analysis.

A. Sample Description

This study attempts to examine the retail customers towards E-banking security threats in the urban north India (Patiala, Chandigarh and Mohali). The universe of population is the 240 retail customers (120 each from public and private sector banks) that are using bank services for the last one year at least. Customers who belong to rural areas have not considered for this study.

III. ANALYSIS

This section deals with analysis of customer perceptions with respect to E-banking security.

TABLE 1.1: REASONS FOR SELECTING THE BANK

During the survey, it has been found that the main reasons while selecting the bank includes privacy and trustworthiness and assurance of secure online transactions (refer Table 1.1). The assurance provided by banks about secure online transactions makes a difference in customer's perceptions about bank and its services. Moreover, bank's brand name and availability of various online security measures are also important factors while selecting the bank. Statistical results are insignificant and show that customer respondents have similar perception irrespective to their bank group, and few variations are due to sample fluctuations.

TABLE 1.2: PROTECTING CUSTOMER INFORMATION

Table 1.2 presents majority of customers of public sector banks reported that they don't know whether their banks are putting efforts in order to protect their online account information. On the other hand, percentage of customers who think that their banks provide better protection to them is somehow low in case of respondents from private sector banks, 40.0% respondents having account in private sector banks have agreed that bank is doing enough protecting their on-line information. Significant statistical of Chi-square results proved that respondents' perception varies with respect to bank groups.

TABLE 1.3: BANK REGULARLY UPDATES SECURITY INFORMATION

Table 1.3 shows among the two bank groups, 60% customers having account in public sector banks agreed that bank generally provides updates about changes in security measures while 75.9% customers with account in private banks agreed that bank usually updates about changes in security measures and 4.9% customers denied about any information regarding updating changes in security. Insignificant statistical results (Chi-square and Cramer's V) concluded that respondents have similar opinion regarding updating security information irrespective of their bank group, and few variations are due to sample fluctuations. This shows percentage of respondents from private sector banks were get regular updates from banks as compared to respondents from public sector banks.

TABLE 1.4: SECURITY MEASURES PROVIDED BY BANKS

According to the majority of respondents among the two bank groups, 3D secure pin and OTP were found to be commonly provided by public and private banks. On the other hand some of the advanced security mechanisms like USB token and biometric scans were still not introduced by both

public and private sector banks. Statistical results of Chi-square and Cramer's V conclude that respondents all the banks provide almost same security measures while they lack in the adoption of advanced mechanisms.

TABLE 1.5: FEAR ABOUT ONLINE THREATS AND FRAUDS

It is evident to Table 1.5 that customers are increasingly worried about online threats and frauds. Moreover, during the survey it was found that besides adopting latest security measures, customers still think that online channels are not secure. Insignificant statistical results verify that customers from all the bank groups are worried about online threats and frauds.

TABLE 1.6: FRAUD/FINANCIAL LOSS

Maximum number (35%) of cases related to financial loss has reported by customer respondents' public sector banks (table 1.6). According to 59% respondents from private sector banks, they never experienced fraud or financial. Hence it is proved that highest number of fraud-related cases reported by respondents from public sector banks as compared to private sector banks.

TABLE 1.7: SHIFTING OF BANK ACCOUNT

It has been found that there are a considerable percentage of respondents who believe that they will shift their account to some other bank if in case of financial loss/fraud (table 1.7). Significant statistical results of Chi-square proved that respondents may shift their account when faced financial loss or online frauds. Few variations are due to sample fluctuations. All in all, if banks want to retain their customers then they need to completely satisfy customers in every respect.

TABLE 1.8: TRADITIONAL BANKING IS BETTER

From Table 1.8 it has been found that less percentage of respondents were reported that traditional banking is better. Significant statistical results of Chi-square proved that respondents have same views on better mode of banking. Few variations are due to sample fluctuations.

IV. CONCLUSION

Retail customers avoid transacting through E-channels due to insecure online environment and exposure to online threats. For E-banking to be successful, they need to satisfy customer. This approach plays a critical role for success in E-banking. Earlier research studies showed concerns over security and trust that constituted an obstacle in the adoption of E-banking. It is also significant that customers should be assured of privacy of their data and that also in a problem-free web environment. In the present set-up, customers want secure online environment in which they can conduct transactions, and banks must provide best in the class services in safe environment.

This study tried to investigate various threat-related aspects from retail customer view point. The study analyzed that privacy and trustworthiness and secure online transactions along with availability of online services are the strongest determinants for selecting the bank. It has been found that majority of customers feel that their banks did not regularly update them regarding various security measures and also they feel that banks were not successful in protecting their information. Also they feared online threats and financial losses. Even after providing various security techniques, numbers of cases have been reported by customers from all the two bank groups. Further, it has been found that customers prefer online banking rather than traditional mode of banking.

It is essential for the banks to offer security considerations as part of their service offerings. The level of authentication used by the financial institution should be suitable to the risks associated with online products and services.

V. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

This study primarily concentrates on retail customer's aspects and the study was confined to retail customers from northern part of India. Inclusion of other areas in India might have different and/or remarkable findings. Moreover, studies with much larger sample size would be required for more appropriate results.

VI. REFERENCES

[1] Aladwani, M. (2001). Online banking: a field study of drivers, development challenges, and expectations. International Journal of Information Management, pp. 213-225.

[2] Alfreds, D. (2013). Security fear limits online banking – survey. Accessed online at http://www.news24.com/Technology/News/Security-fear-limits-online-banking-survey-20131203, March 2015.

[3] Alnsour, M. and AL-hyari, K. (2011). Internet banking and jordanian corporate customers: issues of security and trust. Journal of Internet Banking and Commerce, vol. 16, no.1. Retrieved from http://www.arraydev.com/commerce/jibc, November 2012.

[4] Alsajjan, B. A. and Dennis, C. (2006).The impact of trust on acceptance of online banking. European Association of Education and Research in Commercial Distribution, 27-30 June 2006. Brunel University – West London, United Kingdom.

[5] Avizienis, A., Laprie, J., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 1(1), 11–33.

[6] Bala, M.S. and Norita, M.N. (2011). Secure E-commerce web development framework. Information Technology Journal 10(4):769–779.

[7] Bipindra, N. C. (2013). Chinese 'hack' DRDO computers. Retrieved online at http://www.newindianexpress.com/nation/article1500336.ece, July 2014.
[8] Bradley, L. and Stewart, K. (2003). A Delphi study of internet banking. Marketing Intelligence and Planning, 21 (5), 272-281.
[9] Calonia, J. (2014). The-6-biggest-fears-americans-have-about-online-banking. Accessed online at http://money.usnews.com/money/blogs/my-money/2014/10/30/the-6-biggest-fears-americans-have-about-online-banking, March 2015.
[10] Chickowski, E. (2006). Web security fears cause $2 billion online commerce loss in 2006, SC Magazine. Retrieved from http://haymarket.ec-messenger.com/re?l=1hmb1qIfvmdmdIe, March 2012.
[11] Dandash, O., Wang, Y., Le, P. D. and Srinivasan, B. (2008). Fraudulent internet Banking Payments Prevention using Dynamic Key. Journal of Networks, Vol. 3, No. 1.
[12] Dapp, T.F.(2012). Online article "Growing need for security in online banking, biometrics enjoy remarkable degree of acceptance", Banking and Technology Snapshot Digital economy and structural change, Deutsche Bank; Retrieved from www.dbresearch.com, Dec, 2012.
[13] Fatima, A. (2011). E-Banking security issues – is there a solution in biometrics? Journal of internet Banking and Commerce, August 2011, vol. 16, no.2. Retrieved from http://www.arraydev.com/commerce/jibc/, May 2012.
[14] Fitzergelad, K. (2004). An Investigation into people's perceptions of online banking. Retrieved from http://staffweb.itsligo.ie/staff/eward/ebus%200203/Discussion%20topics/Online% 20Banking.ht, March 2011.
[15] Friedman, B., Kahn, P. and Howe, D.(2000). Trust online. Communications of the ACM 2000; 43:34-40.
[16] Gefen, D., Karahanna, E., and Straub, D.W. (2003). Inexperience and experience with online stores: The importance of TAM and trust. IEEE Transactions on Engineering Management, 50(3), 307-321.
[17] Goetz, E. (2003). Survey and analysis of security issues in the U.S. banking and finance sector. Retrieved from www.ists.dartmouth.edu, November 2012.
[18] Grewal D., Iyer G. and Levy M. (2004). Internet retailing: enablers, limiters and market consequences. Journal of Business Research, 57(7), pp. 703-7013.
[19] Gurung, V. (2014). Latest Cyber Crime Reports of India. Retrieved online at http://www.cyberkendra.com/2014/07/latest-cyber-crime-reports-of india.html#.U_aF_8WSySo, July 2014.
[20] Information age (2012).Chinese hackers' access Indian navy systems. Retrieved online at http://www.information-age.com/technology/security/2110843/%22chinese%22-hackers-access-indian-navy-systems, June 2014.
[21] Infosys (2010). FINACLE strengthens data security using oracle database vault, audit vault and advanced security. Retrieved from http://www.infosys.com/finacle/, November,2011.
[22] Jarvenpaa, S.L., Tractinsky, N., and Vitale, M. (2000). Customer trust in an internet store. Information Technology and Management, 1, 45-71.
[23] Keffala, M. (2010). Barriers to the Adoption and the Usage of internet Banking by Tunisian Customers. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566719, August, 2011.
[24] Klein, A. (2007). The new front line in defending against online threats. ''E-Commerce Times, Retrieved from http://www.technewsworld.com/rsstory/55686.html, March 2012.
[25] Kumar, V. (2008). Alternative perspectives on service quality and customer satisfaction: the role of BPM. International Journal of Service Industry Management Vol. 19 No. 2, pp. 176-187, 2008.
[26] Liao, Z., and Cheung, M. T. (2002). Internet based e-banking and customer attitudes: An empirical study. Information and Management, 39, 283–295.
[27] Malhotra, P. and Singh, B. (2009). Analysis of internet banking offerings and its determinants in India. internet Research, 20 (1), 87-106.
[28] McAfee, Inc. (2007). Online identity theft trends. Retrieved from http://www.mcafee.com/us/about/press/corporate/2007/20070115_182020_r.html, February 2013.
[29] Mukti, N. (2000). Barriers to putting businesses on the internet in Malaysia. The Electronic Journal of Information Systems in Developing Countries, 2(6), 1–6.
[30] NCRB (2013). Cyber crimes. Retrieved from http://ncrb.gov.in/CD-CII2013/Home.asp, May 2014.
[31] Pieters, W. (2010). Explanation and trust: what to tell the user in security and AI? Published with open access at Springerlink.com, December 2014.
[32] Ponemon (2005). Privacy trust survey for online banking. Retrieved from http://www.watchfire.com/news/whitepapers.aspx#finserv, December 2011.
[33] Qiu, X. L. (2008). Chinese customers' banking habits and e-banking barriers. International Journal of Business and Management Vol. 3, No. 2.
[34] Sathye,M.(1999).Adoption of internet banking by Australian customer: An empirical investigation. International Journal of Bank. Vol. 17 (7), 324-334.
[35] Shalhoub, K.Z. (2002). Trust and loyalty in electronic commerce: An agency theory perspective. Quorum Publishing, New York, NY.
[36] Stewart, K.J. (1999). Transference as a means of building trust in World Wide Web sites. Proceedings of the 20th International Conference on Information Systems, pp. 459–464.
[37] Viega, J. and McGraw, G. (2001) Building secure software. Addison-Wesley, Boston.
[38] Washkuch, F. (2006). Web fraud cost more than $200 million in 2006. Retrieved from
[39] http://scmagazine.com/us/news/article/645020/fbi-web-fraud-cost-200-million-2006/(2007), December 2012.
[40] White, H. and Nteli, F. (2004). Internet banking in the UK: why are there not more customers? Journal of Financial Services Marketing, 9 (1), 49-56.
[41] Young T. (2006). Cost of ID fraud could reach £3.8bn in four years. Retrieved from http://www.vnunet.com/computing/news/2168208/cost-id-fraud-reach-8bn-four, February 2013.
[42] Yousafzai, S., Pallister, J. and Foxall G.(2003). A proposed model of e-trust for electronic banking Technovation 847–860.

Retreived from www.elsevier.com/locate/technovation, December 2012.

[43] Yousafzai, S., Pallister, J. and Foxall, G.(2009). Multi-dimensional role of trust in internet banking adoption. The Service Industries Journal Vol. 29, No. 5, May 2009, 591–605.

Tejinder Pal Singh Brar is a research scholar. He is post graduate in computer applications and also a Microsoft certified technology specialist.

NOTE: *I wish to acknowledge inspiration and support provided by department of Research, Innovation and Consultancy (RIC),* ***Punjab Technical University,*** *Kapurthala (Punjab), India during writing this research article.*

VII. LIST OF TABLES

TABLE 1.0: YEAR WISE COMPARISON OF DIFFERENT CRIME HEADS IN INDIA

S. no.	Crime heads	Cases Registered				% Variation in 2013 over 2012
		2010	2011	2012	2013	
1.	To assist in decrypting the information intercepted by govt. agency	1	3	3	6	100.0
2.	Unauthorized access to protected computer system	3	5	3	27	800.0
3.	Failure of compliance of certifying authority	2	6	6	13	116.7
4.	Breach of confidentiality /privacy	15	26	46	93	102.2
5.	Fraud of digital signature certificate	3	12	10	71	610.0
6.	Hacking	164	157	435	550	26.4

Source: NCRB (2013)

TABLE 1.1: REASONS FOR SELECTING THE BANK

Reasons	Bank group	Yes	No	Total	Statistical Results
Availability of various online security measures	Public	77.00%	23.00%	100%	χ^2=1.543 , DF=2, CRV=.142
	Private	74.10%	25.90%	100%	
Brand name	Public	80.00%	20.00%	100%	χ^2=.660 , DF=2, CRV= .114
	Private	88.60%	10.40%	100%	
Privacy and trustworthiness	Public	96.00%	4.00%	100%	χ^2=.250 , DF=2, CRV=.067
	Private	97.10%	2.90%	100%	
Assurance of secure online transactions	Public	93.00%	7.00%	100%	χ^2=.250 , DF=2, CRV=.067
	Private	96.10%	3.90%	100%	

Source: Developed by the researchers

TABLE 1.2: PROTECTING CUSTOMER INFORMATION

Group	Sub-Group	Yes	No	Don't know	Total	Statistical Results
Bank group	Public	40.0%	10.0%	50.0%	100%	χ^2= 0.047, DF=6, CRV= .161
	Private	30.5%	11.9%	57.6%	100%	

Source: Developed by the researchers

TABLE 1.3: BANK REGULARLY UPDATES SECURITY INFORMATION

Group	Sub-Group	Yes	No	Don't know	Total	Statistical Results
Bank group	Public	60.00%	15.00%	25.00%	100%	χ^2= 5.321, DF=4, CRV=.132
	Private	79.9%	4.9%	15.20%	100%	

Source: Developed by the researchers

TABLE 1.4: SECURITY MEASURES PROVIDED BY BANKS

Security measures	BG	Yes	No	Don't Know	Total	Statistical Results
3D secure pin	Public	80.40%	10.60%	9.0%	100%	χ^2= 1.192, DF=2, CRV= .342
	Private	87.10%	10.90%	2.0%	100%	
OTP	Public	77.40%	12.60%	10.0%	100%	χ^2= 3.388, DF=2, CRV= .892
	Private	80.10%	5.90%	14.0%	100%	
USB Token	Public	0.0%	51.60%	48.40%	100%	χ^2= 1.008, DF=2, CRV= .621
	Private	0.0%	45.90%	54.10%	100%	
Biometric scans	Public	0.0%	42.60%	57.40%	100%	χ^2= 2.908, DF=2, CRV=.447
	Private	0.0%	50.90%	49.10%	100%	

TABLE 1.5: FEAR ABOUT ONLINE THREATS AND FRAUDS

Group	Sub-Group	Yes	No	Don't know	Total	Statistical Results
Bank group	Public	98.0%	2.0%	-	100%	χ^2= 6.057, DF=3, CRV= .243
	Private	92.9%	5.0%	2.1%	100%	

Source: Developed by the Researchers

TABLE 1.6: FRAUD/FINANCIAL LOSS

Group	Sub-Group	Yes	No	Don't know	Total	Statistical Results
Bank group	Public	35.0%	40.0%	25.0%	100%	χ^2= 7.564, DF=3, CRV= .041
	Private	23.8%	59.0%	17.2%	100%	

Source: Developed by the researchers

TABLE 1.7: SHIFTING OF BANK ACCOUNT

Group	Sub-Group	Yes	No	Don't know	Total	Statistical Results
Bank group	Public	50.0%	35.0%	15.0%	100%	χ^2= 6.782, DF=3, CRV= .143
	Private	30.5%	51.7%	17.8%	100%	

Source: Developed by the researchers

TABLE 1.8: TRADITIONAL BANKING IS BETTER

Group	Sub-Group	Yes	No	Don't know	Total	Statistical Results
Bank group	Public	30.0%	60.0%	10.0%	100%	χ^2= 0.325, DF=6, CRV=.320
	Private	20.5%	51.9%	27.6%	100%	

Source: Developed by the researchers

Note: χ^2= Chi-square; DF= Degree of freedom; CRV= Cramer's V