Internet Banking Security Strategy: Securing Customer Trust

Frimpong Twum
Department of Computer Science
Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Kwaku Ahenkora (Corresponding author)
Christian Service University College, PO Box 3110, Kumasi, Ghana
E-mail: k.ahenkora@yahoo.co.uk

Received: August 22, 2012 Accepted: September 17, 2012 Online Published: October 31, 2012
doi:10.5430/jms.v3n4p78 URL: http://dx.doi.org/10.5430/jms.v3n4p78

Abstract

Internet banking strategies should enhance customers' online experiences which are affected by trust and security issues. This study provides perspectives of users and nonusers on internet banking security with a view to understanding trust and security factors in relation to adoption and continuous usage. Perception of internet banking security influenced usage intentions. Nonusers viewed internet banking to be insecure but users perceived it to be secure with perceived ease of use influencing continuous usage. Perception of internet banking security was positively influenced by trust in the internet banking system, trust of the provider, threat awareness, availability of information and education but showed a negative relationship with age. The study suggests that internet banking security strategy may consider the generation gap in adoption and should continuously aim at securing customers' trust of the providers' online brand's security, including the provision of security information and education.

Keywords: Internet banking, Strategy, Customer trust, Usage intention, Non users

1. Introduction

Banking institutions invest heavily in information technology and efficient information systems to enhance business processes and strategies with the aim of gaining competitive advantage. Internet banking is an information technology infrastructure which banks currently use in addition to other well-known channels such as telephone banking and branch banking. Internet banking is offered by almost all UK high street banks or building societies with physical branches (e.g. Barclays, Lloyds, Natwest, etc.) as an alternative to branch banking where a customer physically visits the bank to transact business (White and Nteli, 2004). Internet banking is also offered by banks that operate wholly as "virtual, branchless, or internet-only" banks without a single physical branch (e.g. Firstdirect, Ingdirect, Smile, etc.). The provider creates a website to meet customers' banking needs from accounts opening through to complex financial transactions such as funds transfers and loan transactions (White and Nteli, 2004). At the basic level, it involves the setting up of a web page by a bank to provide customers with information about its products and service offerings while at an advance transactional level it involves provision of facilities such as accessing accounts, funds transfer, and buying or signing up for a bank's financial products or services online (Sathye, 1999).The internet banking customer uses internet connection to remotely access personal bank accounts information and to carry out transactions electronically.

Internet banking research has been of particular interest to both researchers and bank management. Trethowan and Silicone (1997) and Daniel (1999) mentioned convenience, sales, orientation and lower costs as advantages. Sathye (1999), Rotchanakitumuuai and Speece (2003), and Cheng et al., (2006), noted banks' claim of reduced or lower operating costs and competitive advantage over rivals as some of the benefits. Gerrard and Cunningham (2003) and Lichtenstein and Williamson (2006) also identified convenience, speed, 24 hour banking, as benefits. However, some customers remain skeptical due to the additional costs such as the security threat it poses to their financial and confidential information (Sathye 1999; Rotchanakitumuuai & Speece, 2003; White & Nteli, 2004; Cheng et al., 2006; Lichtenstein & Williamson, 2006). Studies in Europe have shown that organisations tend to be less optimistic about future security management, given the general upward trend and complexity of security incidents (Anderson, 2006;

DTI, 2006; Ernst & Young, 2006). Such views are likely to affect consumer perception of internet security. While internet banking continues to gain global grounds, there are non users in the UK, where customers tend to be early adopters of technology, and it is argued that e-commerce cannot fulfill its potential without securing customer trust (Jones et al., 2000; Farhoomand and Lovelock, 2001; Raisch, 2001; Lee and Turban, 2001) and addressing security management issues (Koskosas and Koskosas, 2011). While general factors affecting trust have been identified there is scant information on factors affecting customer perception of internet banking security (Prins et al., 2002; Salam et al., 2005; Pi, Liao and Chen, 2012). This study fills the gap. Such information is also needed as security of services and safety of costumers' sensitive information are important considerations in gaining customer confidence to use internet banking (Kasemsan and Hunngam, 2011). The study, therefore, addresses the questions; how does customer perception of internet banking security affect usage and how is perception of internet banking security influenced by personal awareness of security threats, trust in the internet banking system and the provider?. The study addresses these questions from the perspectives of some users and nonusers of UK internet banking services. For the purposes of this paper, the internet banking system refers to the hardware, software, networks or inter networks (internet) that make internet banking possible and the internet banking provider refers to the financial institution, i.e. the bank.

1.1 Theoretical Background

Although there has been dramatic rise in the number of Internet users all round the world, security and trust issues still persist (Suh and Han, 2003). The background information fundamental to this study, therefore, includes technology acceptance model (TAM), system security concepts and trust and their effects on usage. Davis' (1989) work has shown that user acceptance of information technology is determined by two influential factors; perceived usefulness and perceived ease of use. Perceived usefulness is defined as the degree to which a person believes that using a particular system would enhance performance while perceived ease of use refers to the degree to which a person believes that using a particular system would be free from effort. Perceived usefulness and perceived ease of use are known to positively affect the acceptance of internet banking services (Kasemsan & Hunngam, 2011).

Although service providers, financial institutions, the media, security organisations, and security experts have continually provided technical information and verbal assurances on dealing with online security threats, consumers are fearful of the intruder getting hold of their accounts and other confidential information and hence security preys heavily on consumers' minds (White & Nteli, 2004). The fear is heightened by the nature of recent trends of security breaches and attacks reported by the media which computer security experts have found highly complex and sophisticated to comprehend; e.g. the surfacing of the recent "Zeus v.3 botnet trojan", which was reported by the media to have been used by attackers to raid and steal thousands of pounds from UK internet banking customers (McGuinness, 2010), the 'Mariposa' botnet attack, which cyber criminals used to infect 13 million computers in one of the biggest cyber crimes ever detected in Europe (Steele, 2010), the reported regular snooping of UK internet users to help companies target their advertising campaigns, which amount to a massive intrusion on consumers online privacy (Smith, 2010). In addition, pronouncements on internet banking security by high profile officials that internet banking is less safe than having a traditional account (Cecil, 2010) heightens consumer concerns of internet banking security. Risk is a critical factor in adopting technology (Sathye, 1999; Salisbury et al., 2001) and is defined in relation to internet banking as the security and reliability of transactions over the Internet (Sathye, 1999). Customer acceptance is a key indicator of technology usage (Sathye,1999) and barriers to internet banking adoption include consumer concerns of media information on security breaches, the reliability of online transactions, the security of the internet banking system and banks capability of protecting customers' accounts and privacy (Rotchanakitumuuai & Speece,2003; Wang et al., 2003). Consumers, therefore, are more likely to use internet banking when they perceive no risk to their bank accounts and other confidential information and are aware of security measures (Sathye, 1999; Salisbury et al., 2001; Cheng et al., 2006). These observations suggest that perception of internet banking security is likely to influence usage intentions and also customer awareness and knowledge of security are likely to influence their views on internet banking security.

Studies on factors that affect consumers' trust and usage of financial services have shown that trust of the website influences usage intentions; transaction security, website and company awareness influence cognitive trust while transaction security influences affective trust (Pi, Liao & Chen, 2012). Online trust has been defined as the internet user's psychological state of risk acceptance based on the positive expectations of the intentions or behaviours of an online service provider (Rousseau et al., 1998). Beyond satisfaction, repeat purchase is highly influenced by trust of the provider (Liang & Wang, 2008). While most studies on trust and internet banking or online financial services have established direct effects between trust and usage intentions, there are attempts to explore internet banking security management through trust management (Koskosas & Koskosas, 2011). Security appears to be an important factor related to mistrust of internet banking services (Kasemsan & Hunngam, 2011). These observations suggest

that perceptions on internet banking security are likely to be affected by trust of the system and trust of the provider; these relationships are worth exploring to enhance our understanding of internet banking security through trust management.

This study, therefore, is premised on the following perspectives emerging from the review of the related literature on technology acceptance model (TAM), system security concepts, trust and usage intentions:

Perception of internet banking security has influence on internet banking usage

Awareness of internet security threats influence perceptions of internet banking security

Knowledge (availability of security information and education) influence perceptions on internet banking security

Trust of the system has influence on perceptions of internet banking security

Trust of the internet banking provider has influence on the perceptions on internet banking security.

2. Method

The research sought to identify users and nonusers' perceptions on internet banking security and to determine the nature and extent to which factors such as trust of the internet banking system (security, reliability of transaction, privacy), trust of the internet banking provider, awareness of internet security threats and knowledge of protective measures influence customer perception of internet banking security. Rating scale questions were used. The study was conducted among students and staff of Roehampton University, UK and simple random sampling was used to select a sample size of 300, 150 students and 150 members of staff. There were equal number of males and females in the study. Participants indicated their opinion by circling a number, one to five, on a five point likert scale with response categories ranging from strongly disagreeing to strongly agreeing. Out of the 300 questionnaires distributed, 238 usable responses were received which consisted of 168 internet banking users (users) and 70 non-internet banking users (nonusers). In terms of respondent's 'gender', 59% were females and 41% males and the range of respondents' age was 19-60. Participants had access to computer and 95 % of respondents use internet regularly (almost every day), and the rest occasionally (once or twice a week). They access the internet from home, office, the University's premises (64%) and from other locations e.g. from mobile devices on the move. Tests of significance and correlations were conducted.

3. Results and Discussion

3.1 Perceptions on Internet Banking Security and Usage

The results of users and nonusers' perception of internet banking security are shown in Table 1 and indicate that while over 60% of users either agree/strongly agree that internet banking is secure, over 50% of nonusers disagree/strongly disagree. An independent sample t-test conducted resulted in significantly different ($p<0.05$) mean values of 3.57 for users and 2.51 for nonusers. It suggests that users hold a more positive view about the security of internet banking than nonusers. However, ranking of their reasons for continuous usage of internet banking (Table 3) shows that convenience (53%) and ease of use (29%) are more important factors than safety and security (5%). Tu (2012) reported similar findings that perceived ease of use had a greater effect on customer satisfaction than trust. On the contrary, the primary reason for nonusers not choosing internet banking but preferring traditional high street banking (33.2%) is not that it is difficult to use (5.8%) but that they perceive internet banking as still unsafe and insecure (52.2%). For both users and nonusers there is no significant effect of their awareness of online security threats on their ratings of how secure they perceive internet banking to be (Table 2). The observed differences corroborate previous views based on qualitative studies that suggested that users of internet banking services generally have more trust in the system than nonusers and that trust of the system is a crucial factor related to unwillingness to adopt service via the internet (Rotchanakitumnuai , 2004; Rotchanakitumnuai & Speece, 2003).

3.2 Perceptions of Trust, Awareness and Knowledge on Internet Banking Security and Usage

The relationships among the various factors chosen for the study are shown in Table 2. There was strong and significant positive relationship (0.610, $p<0.01$) between consumer trust of the bank and trust of the internet banking system. Similarly, there were significant positive relationships between perception of internet banking security and trust of the system (0.556, $p<0.01$), information and education (0.299, $p<0.01$).Threat awareness did not have any observable significant relationship with perception of internet banking security or the other factors. There were significant positive relationships between internet banking usage and information and education (0.460, $p<0.01$), trust of system (0.555, $p<0.01$) and trust of bank (0.610, $p<0.01$).These relationships suggest that factors that positively enhance customer perception of internet banking security may invariably influence internet banking usage. Hence, customers are more likely to use or continue to use internet banking when they perceive internet banking as a

secure way of banking and when this perception is reinforced by trust of the bank, trust of the internet banking system, the provision of security information and education. The Banks' security management strategy is, therefore, more likely to enhance online experience when it addresses customer perceptions of internet banking security. Security management strategy should also consider transporting the bank's trusted 'branch banking' image online. Such strategic approach should underpin previous suggestions that internet banking providers should seek to visibly demonstrate concern for security by putting in place measures and policies that might enable them win their customers trust such as regularly providing them with easy to read (no computer jargons) information on how to be safe online and how to keep their computers and other equipment they use for online banking updated (Rotchanakitumuuai and Speece, 2003).

3.3 Age and Internet Banking Security

The ratings of internet banking security by different age groups are shown in Table 1 and show that over 50% of people in the age groups 19-29 and 30-39 years agree/strongly agree that internet banking is secure while 50% of people over 60 years disagree. Results from the ANOVA test showed significant difference ($p<0.05$) in the ratings of internet banking security of 19-29 and ≤60 age groups (Games-Howell Test, $p = 0.036$, $n = 268$). The correlation matrix (Table 2) also shows a significant negative relationship (-0.202, $p<0.01$) between age and internet banking security ratings but similar relationship between age and usage was not significant. The results suggest the influence of age on perceived internet banking security and possibly also on technology acceptance.

4. Conclusions

This study has provided perspectives on internet banking in relation to usage intentions and factors that contribute to customers' perception of internet banking security. The localised nature of the study may limit generalisation.The findings, however, contribute to our understanding of cyber security management through trust management. They also have implications for managerial practice, particularly in ways in which internet security strategies should take on board customer perception of internet banking security and factors that influence it. In our study, we found that customer perception of internet banking security is significantly related to usage and is significantly affected by trust of the system and trust of the provider. The study concludes that customer perception of internet banking security is influenced by customers' trust of the bank and the internet system and this subsequently influences usage intentions.

References

Andersen, I. T. (2006). Security barometer survey: The psychology of security. *Quocirca.*

Cecil, N. (2010). Internet banking is 'less safe', says police chief. *Evening Standard*, 19th Nov. p. 8.

Cheng, T. C. E., Lam, D. Y. C., & Yeung, A. C. L. (2006). Adoption of Internet banking: An empirical study in Hong Kong. *Decision Support Systems*, *42*(3), 1558-1572. http://dx.doi.org/10.1016/j.dss.2006.01.002

D. T. I. (2006). *Security Special Report; The internal threat 2006*. Technical Report, April, Department of Trade and Industry, London.

Daniel, E. (1999). Provision of electronic banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing*, *17*(2), 72-82. http://dx.doi.org/10.1108/02652329910258934

Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. http://dx.doi.org/10.2307/249008

Ernst and Young. (2006). *Global Information Security Survey*. London: Ernst and Young.

Farhoomand, A., & Lovelock, P. (2001). *Global E-commerce-Texts and Cases*. New York: Prentice Hall.

Gerrard, P., & Cunningham, J. B. (2003). The diffusion of Internet banking among Singapore consumers. I*nternational Journal of Bank Marketing*, *21*(1), 16-28. http://dx.doi.org/10.1108/02652320310457776

Kasemsan, M.L., & Hunngam, N. (2011). Internet banking security guideline model for banking in Thailand. *Communications of the IBIMA*, 1-13.

Koskosas, I., & Koskosa, M.M. (2011). Internet banking security management through trust management. *World of Computer Science and Information Technology Journal, 1*(3), 79-87.

Lee, M.K.O., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce, 6*(1), 75-91.

Lichtenstein, S., & Williamson K. (2006). Understanding consumer adoption of Internet banking: an interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, *7*(2), 50-66.

McGuinness, R. (2010), Hackers' cash raid on 3,000 accounts. *Metro*, 11th Aug. p. 1.

Pi, S-M., Liao, H. L., & Chen, H. M. (2012). Factors that affect consumers' trust and continous adoption of online financial services. *International Journal of Business and Management*, *7*(9), 108-119.

Prins, J. E. J., Ribbers, P. M. A., van Tilborg, H. C. A., Veth, A. F. L., & van der Wees, J. G. L. (2002). *Trust in Electronic Commerce: The role of trust from a legal, an organizational and technical point of view.* The Hague: Kluwer Law International.

Raisch, W. (2001). *The E-marketplace-strategies for success in B2B ecommerce*. London: McGraw-Hill.

Rotchanakitumnuai, S. (2004). Corporate customer perspectives on business value of Thai Internet Banking. *Journal of Electronic Commerce Research, 5*(4).

Rotchanakitumnuai, S., & Speece, M. (2003). Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand. *International Journal of Bank Marketing*, *21*(6/7), 312-323. http://dx.doi.org/10.1108/02652320310498465

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: a cross-discipline view of trust. *Academy of Management Review, 23*(3), 393-404. http://dx.doi.org/10.5465/AMR.1998.926617

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management and Data Systems*, *101*(4), 165-176. http://dx.doi.org/10.1108/02635570110390071

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing*, *17*(7), 324-334. http://dx.doi.org/10.1108/02652329910305689

Smith, H. (2010). Online snoops put Britain in the dock. *Metro*, 1st Oct. p. 1.

Steele, J. (2010). Cyber Criminals took over 13m computers. *Metro*, 4th Mar. p. 14

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of Electronic Commerce. *International Journal of Electronic Commerce*, *7*(3), 135-161.

Trethowan, J., & Scullion, G. (1997). Strategic responses to change in retail banking in the UK and the Irish Republic. *International Journal of Bank Marketing*, *15*(2), 60-68. http://dx.doi.org/10.1108/02652329710160475

Tu, C.C., & Lin, C. Y. (2012). Perceived ease of use, trust, and satisfaction as determinants of loyalty in e-Auction marketplace. *Journal of Computers, 7*(3), 645-652. http://dx.doi.org/10.4304/jcp.7.3.645-652.

Wang, Yi, Wang, Yu, Hsin-Hui, L., & Tzung-I, T. (2003). Determinants of user acceptance of Internet banking: an empirical study. *International Journal of Service Industry Management*, *14*(5), 501-519. http://dx.doi.org/10.1108/09564230310500192.

White, H., & Nteli, F. (2004). Internet banking in the UK: Why are there not more customers? *Journal of Financial Services Marketing*, *9*(1), 49-56.

Table 1. Perceptions on internet banking security

Usage	IB Security Ratings (Internet banking is secure)				
	Strongly Disagree (%)	Disagree (%)	Neither Agree nor Disagree (%)	Agree (%)	Strongly Agree (%)
Users (N=167)	0.06	10.1	25.6	58.9	4.8
Nonusers (N=69)	12.85	40	32.86	11.43	2.9
Age Group (yrs)					
19-29 (N=114)	5.3	13.1	24.6	50.0	7.0
30-39 (N=46)	2.1	23.9	21.7	47.8	4.3
40-49 (N=48)	2.1	16.7	41.6	39.6	0.0
50-59 (N=20)	10.0	30.0	20.0	40.0	0.0
≤60 (N=10)	0.0	50.0	40.0	10.0	0.0

Table 2. Pearson's correlation matrix

Variables	1	2	3	4	5	6	7
1. Age Group	1.000						
2. Knowledge of Security	0.018	1.000					
3. Threat Awareness	0.071	0.015	1.000				
4.Trust of System	-0.272 **	0.276**	-0.085	1.000			
5. Trust of Bank	-0.188**	0.274**	0.77	0.610**	1.000		
6. Internet Banking Security Rating	-0.202**	0.299**	0.027	0.556**	0.501**	1.000	
7.Internet Banking Usage	-0.092	0.460**	0.060	0.555**	0.417**	0.506**	1.000

**Significant, $p<0.01$

Table 3. Ranking of reasons for use and nonuse of internet banking

	Factors (%)				
	Cost effective	Ease of use	Safe and secure	Convenience	Other
Users	4.2	26.9	5.4	56.3	7.2
	Factors (%)				
Nonusers	Expensive	Difficult to use	Unsafe and insecure	Prefer Traditional Banking	Other
	1.4	5.8	52.2	33.3	7.2