The Impact of Customer Knowledge on the Security of E-Banking

Nabeel Zanoon *dr.nabeel@bau.edu.jo*
Aqapa College , Balqa Applied University
Aqapa, Jordan

Natheer Gharaibeh *nkgharaibeh@bau.edu.jo*
Ajloun College , Balqa Applied University
Ajloun, Jordan

Abstract

In this paper one of the most affective factors on security of e-banking will be discussed, by accepting the use of information technology for the execution of the Traditional e-banking, As we know that e-banking is done online and the customers are considered the active element and the other party in e-banking operations. So if the level of customer knowledge in the use of IT ص low, then this points that customers are not professional in the execution of the traditional e-banking using IT , furthermore this create flaws in the security of e-banking by facilitating the sneaking into the personal information and distrust in customer confidence of the e-banking security. which leads to reject the use of technology in e-banking, And this is what will be discussed in this paper by offering some security gaps which is resulting from the low level of customer knowledge in information technology, and that will be studied through Technology Acceptance Model and In light of this we will suggest some solutions.

Keywords: Trust, E-Banking, Customer Knowledge, Information Technology, Technology Acceptance Model.

1. INTRODUCTION

Due to the important role of commercial banks in this era both in terms of economic or social factors, the need has increased to use modern technology of computers, e-service systems electronic banking basic and secondary rather than traditional information systems, and as a result started the need to learn scientific methods to study these systems and can be introduced and implemented in order to make them more efficient , effective , accurate and reliable information for the beneficiaries.

The new information technology (IT) is turning into the most important factor in the future development of banking, influencing banks marketing and business strategies. In recent years, the adoption of e-banking began to occur quite extensively as a channel of Distribution for financial services due to rapid advances in IT and intensive competitive banking markets [1] While the use of online banking services is fairly new experience to many people [2] Carry with them the underlying assumption that designs should encourage exploration or, at least, allow for a trial-and-error approach to learning how to use systems. However, for e-banking and other security-sensitive systems, a trial-and-error approach is generally not acceptable because a security breach caused by an error may be exploited by an attacker before the error is revoked by the user [3].

User adoption of a technology has become a crucial measure for the success of that technology [4] For carrying out Internet banking properly, a basic knowledge of computers and the Internet is required, which limits the number of people willing to gain this facility. Many people, who are not familiar with computers and the Internet, often find it difficult to use Internet banking. Therefore, for beginners, Internet banking is really time-consuming. In addition to this, people also find a difficulty in trusting a completely mechanized system like Internet banking, in case of financial matters. In many instances, a simple mistake, like clicking a wrong button, may create a big problem [5].

Technology is evolving every day and in almost in every aspect but not everything that is coming in the way is being accepted. Before anyone adopt a technology, all the Information about the technology will be collected and combined to develop a belief about using the technology and that belief will in turn make the individual to accept or reject the technology [6] when users are satisfied with a technology the technology adoption is likely to be higher. In addition, Technology Acceptance Model (TAM) asserts that users'. Decision to use a technology depends on two factors: perceived ease of use and perceived usefulness [7]. Understanding users' attitude towards the adoption of new technologies has proved to be one of the most challenging issues in technology adoption literature [8].

The increasing number of internet banking users indicates that the internet backing's acceptance level has improved. Internet baking's acceptance level can be influenced by several factors. One model that is often used to describe acceptance level of information technology is TAM (Technology Acceptance Model) (Davis, 1989).perceived usefulness and perceived ease of use is believed to be the basis in determining acceptance of information technology. Both of these factors influence intention to use information technology before it can finally create the actual usage in daily life [9].

This paper will discuss affective factors on security of e-banking in addition to the main factors that affect e-banking security; the remainder of this paper is structured as follows: Section 2 describes Knowledge and skills of IT. Section 3 shows the threats to the security of e-banking.. Section 4 discusses Technology Acceptance Model (TAM) which used in this research. our preposition to solve the problem and RESEARCH MODEL are given in section 5 , and we conclude and present future work in Section 6.

2. KNOWLEDGE AND SKILLS OF IT

Knowledge and skills improve people's ability to meet their needs, extend the variety of options open to them in all areas of their lives. The skills people possess can also enhance their sense of self-worth, security and belonging. We live in a society where access to information and proficiency with technology are becoming more important. An inclusive society will increasingly require everybody to have high levels of knowledge and skills. Knowledge and skills include education and training, as well as abilities gained through daily life [10] Individuals who are skilled and always using the internet significantly affect the acceptance of Internet banking services. Users who are knowledgeable in using computers and the Internet will influence them to use Internet banking services [11]

Internet banking helps banks in cost saving, increase customer base, enable mass customization for e-Business services, extend marketing and communication Channel, search for new innovation services, and explore and develope of non-core business. However, customers' ability to subscribe to the Internet-base banking services depend on several factors such as user-friendly interface, level of Internet experience, types of services provided, (for example e-mail, file transfer, news, online financial services, shopping and multimedia services), attitude and perception, access and delivery time and experience with the Internet [12]

3. THREATS TO THE E-BANKING SECURITY

Online banking is a main step for many customers as it is popular for customers to just go onto their computers at home or work and log onto the online banking site, the customers will then be able to exchange money from one account to another and pay bills with a press of a button. As more technology for online banking is increasing and the security seems to be getting tighter there are still possibilities that the accounts that you are going on can get hacked. There are always chances to reduce the risk of fraud [13].Each and every time you log onto the internet your computer is at risk of various threats with the aim of getting your personal details and accessing your money. Behind the scenes we use various security measures to ensure that your transactions and personal information are protected and safe. However, you as a customer can also play a big part in protecting your banking and personal information. The first step in that process is to understand the main threats to your computer [14]Unawareness of threat - If users are unaware that their personal information is actively being targeted by criminals, they may lack the standpoint needed to identify phishing threats and may not take the proper defense when conducting online activities[15].

Many factors affecting why customers are concerned about their online banking security. The same factors are also driving the need for enhanced authentication for online banking solutions. These factors include the growing number of phishing attacks, the increased usage of pharming and malware, and widespread data security breaches [16]

3.1 Cookies

A cookie is a small chunk of data generated by a web server and stored in a text file on your computer's hard disk. Cookies allow a web site to store information on a client computer for later retrieval [17] furthermore Cookies are used as an authentication tool to allow users automatically access certain web sites without asking the server to look at authorized users at the database .the user's log in name and password are stored in the cookie so that the user can access a subscribed web site automatically each time the user clicks on the web page. The use of cookies has privacy concerns because cookies contain information about the URL of the web page you accessed [18]. Therefore Cookies have become a source of privacy concern in recent years .as with most technologies in the computer industry ,this reputation has been earned by the misuse of the technology more than the technology itself. Many web browsers have the use of cookies enabled by default (without user caution), and many people have taken advantage of this situation by profiling customer tendencies, collecting unnecessary personal information, and so on .the semantics of cookies are fairly well designed for the task they are intended to accomplish. The abuse, however, has resulted in cookies having a rather negative connotation [19].

3.2 Phishing

The term 'phishing' has its origins from the analogy that identity thieves who are using lures usually in the form of e-mails to 'fish' for passwords and financial data from the 'sea' of Internet users, [20] Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures [21] Phishing threat, instead a comprehensive education and awareness program should be devised to go hand in hand with other technical countermeasures to minimize the impacts of phishing to the Internet banking sector and regain users trust[22] a phishing website is a broadly launched social engineering attack that attempts to defraud people of their personal information including credit card number, bank account information, social security number and their personal credentials in order to use these details fraudulently against them. Phishing has a huge negative impact on organizations' revenues, customer relationships, marketing efforts and overall corporate image [23].

3.3 Key Logging

Keystroke logging which is often called key logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored [24] a keystroke logger on a consumer's personal computer. It may create security risks if it exposes communication channels to hackers. Spyware also may adversely affect the operation of personal computers, including slowing processing time and causing crashes, browser capturing, home page resetting, installing dialers, and the like. These harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce [25] unfortunately for consumers; key loggers are becoming very sophisticated. Once on a PC, they can track websites visited by the user and only log the keystrokes entered on the websites that are of particular interest to the cyber criminal; for example online banking websites [26] the principal problem with internet banking is that customers use acknowledged untrusted systems in gaining access to the bank internet facilities Trojan horse key loggers can, as has been identified in the scarfo case be lurking on a customer's own computer collecting relevant information which can later be used for nefarious activity[27].

3.4 Padlock

A common mistake made by end users believes that their online banking session is perfectly safe when they use an SSL connection. Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window But SSL is designed as a secure tunnel from the end user computer to the bank mainframe and does not protect the end points such as the end user’s computer [28]

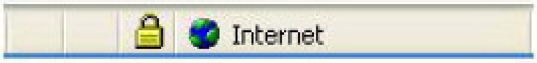

FIGURE 1: The Yellow Padlock Symbol as Displayed in Internet Explorer.

External trust seals are items of a general nature that are used to engender trust, such as the VeriSign symbol and the padlock representing security. Internal regulatory seals include the banks’ own policy declarations, and corporate branding. The wide-ranging nature of the referenced phenomena demonstrates the differing ways in which the subjects are choosing to interpret the signs of trust embedded within the e-banking home-pages [29].

4. TECHNOLOGY ACCEPTANCE MODEL

The technology acceptance model (TAM), developed by Davis, F., et al., (1989),is one of the most widely used and influential models in the field of information systems, technology and services. It has been validated to be powerful as a framework to predict user acceptance of new technology. The goal of TAM is to predict information system acceptance and diagnose design problems before users have any noteworthy experience with the system. TAM measures the determinants of computer usage in terms of perceived usefulness and perceived ease of use. TAM has been effective in the modeling of acceptance of IT and has received extensive experimental support through the studies predicting the use of information systems [30] TAM has proven to be a theoretical model in helping to explain and predict user behavior of information technology [31] User acceptance remains a obstacle to the success of new information technologies (IT). In an attempt explain this, Davis (1989) a thorough understanding of the TAM model may help us to analyze the reasons for resistance toward the technology and would further enable us to take efficient measures to improve user Acceptance of the technology. TAM used in several IS studies and proved useful determining technology acceptance, especially to explain computer usage behavior. Technology Acceptance Model (TAM) has been widely used to predict user acceptance and use based on perceived usefulness and ease of use [32]. In our research we will update the TAM into more suitable model for security of e-banking , we will show that in the next section in figure 2.

5. RESEARCH MODEL AND HYPOTHESES

When the information technology began the development of information systems, the users believes it is difficult to deal with these systems and the prospect of facing a problem in the daily implementation of e-banking. So, we must take into account the fact that the failure use of information technology in the application of banking are often due to lack of users acceptance and the lack of knowledge in the use of banking applications using information technology, the lack of knowledge indicator leads to falling into some flaws This flaws and gaps are recorded against the negative use and because it deals with the systems that contains financial values, and this generates among customers who are not familiar with information technology fears of using e-banking, and these fears pointer to the lack of confidence in the application of e-banking.

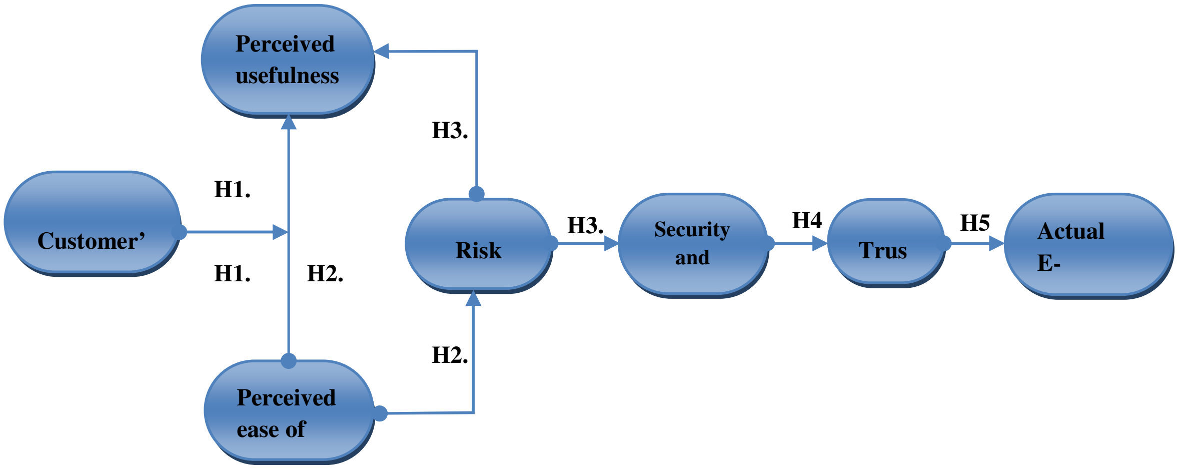

FIGURE 2: Research Model (Technology Acceptance Model).

TAM shows the situation of the user to the technology in general, our updated model shown in figure 2 adds several factors such as the extent of knowledge of users in the use of e-banking , risk factor that affects the security and confidence factor, as all these factors affect the acceptance of the use of technology in e-banking . The study used a model to accept an expanded technology shown in the figure 2 so as to examine the factor customer knowledge in information technology affecting the use of IT in the banking applications. Accordingly, the following subsections will express the propositions emerged from our model:

5.1. Customer's Knowledge of IT

In general the customers know the low-level techniques lead to the appreciation of the potential added value that is inherent in the technology. Experience with the use of the computer, such as the practice of some online business, correspondence and communicate with friends, may affect customers' attitudes towards online banking [33] Therefore the skills to use computers and the Internet for customers of the basics of online banking and this, some countries in Europe worthwhile to develop individual abilities and skills to use the Internet users have Increasing the skills of the individual lead to a trend in most of the application of online banking services [34] In addition, the Some users who do not have a good knowledge about the security risks of online banking, although they are aware of the risks, or perhaps because they know that there is a danger or just ignore the risk [35] In spite of this, people want to use and benefit of technology, including, but cannot ignore the effects and risks that may result from it, however, remains lack of knowledge of an obstacle to the use of technology [36] Although the electronic banking process enables customers to control banking operations. Clients such as students, who are familiar with the internet, you should not find electronic banking processes are complex, however, and efficiency. Customers can also find some difficulties with the service and personal computers and the Internet (such as security and safety concerns complexity, and distrust of regulations and standards, and traditional principles) [37].

H1a: The level of knowledge a customer's has about IT affects on Perceived ease of use.

When the level of customer's knowledge in information technology is high this will lead to high understanding of the banking procedures and doing them faster and thus will be reflected positively on the ease of use, leading to the benefit from the use of information technology in the Daily banking practices.

This proves that the customer will evaluate e-banking easy to use if they have experience of computer use .The experience on the use of computers owned by the customer, will make customers more familiar in using e-banking . Customers who have experience on the use of computers will be easier in the use of e-banking, compared with customers who do not have experience on the use of computer [38].

H1b: The level of knowledge a customer's has about IT affects on perceived usefulness.

5.2 The Perceived Ease of Use and Perceived Usefulness

Earlier research suggested two determinants that are especially important. First, people tend to use or not use an application to the extent they believe it will help them perform their job better. We refer to this first variable as perceived usefulness. Second, even if potential users believe that a given application Is useful, they may, at the same time [39]

For studying the acceptance of e-banking, the general TAM is inadequate because the technology used and the transaction environment in e-banking are different from that of conventional IT and the normal business environment. Before accepting e-banking services, users should be aware about benefits, security issues and the risk associated with it [40]. Perceived ease of use was observed to have no direct effect on behavioral intention but have an indirect effect influence on behavioral intention through its effect on perceived usefulness and perceived risk this result probably is caused by the fact that a big portion of our sample consists of mature internet banking user who are not facing problems in using the system given the usefulness of the system properties .the impact of Perceived ease of use on perceived risk is appeared to be significant meaning that the system friendliness Lowers customers fears about the problems that may have about their transactions security and personal privacy .finally perceived risk was observed to negatively affect usage continuance[41].

H2 a: Perceived ease of use effect on perceived usefulness.

H2 b: Perceived ease of use effect and create security risks.

When customers believe in ease of use of information technology in the implementation of banking, this is indicator to the absence of any risks that may arise from doing business banking, hence the customers underestimate the risks that threaten the security of banking which leads to the low probability of risk through belief in ease of use. Accordingly customers reassure and do not take any degree of security interest and this may lead to security threats

5.3 Perceived Risk

Perceived risk is defined as a consumer's perceptions of the uncertainty and the possible undesirable consequences of buying a product or service [42]. It's only human. People make mistakes, learn from them, and move on to the next challenge usually without dire consequences. But in business, particularly in information technology, mistakes can be costly. From information theft to lost worker productivity to missed sales opportunities, technology errors can put your business at risk. [43]

Legal risk becomes an important issue in internet banking, and one aspect of this is how any losses from security breaches should be apportioned between banks and their customers. Customers should be responsible for any security breach or system problem that is due to negligence on their part, and this should be reflected in the contractual agreements for internet banking services. But if the damage is occurred for system breakdown, negligence of bank employees, attack by hacker or any other parties; the bank must be liable to cover the damage [44] this also results in large security risks imposed on users that have little or no knowledge about the risks and damage that can be inflicted by using the Internet.[45] In history of IT especially security incidents, the biggest mistake has always been to rely on the trust of the other systems and assume the systems are not compromised.

H3 a: the Perceived risks have a negative impact on perceived usefulness.

H3 b: the Perceived risks have a negative impact on Security and privacy

As Koller (1988) wrote, the level of the significance of a decision specifies the influence of the potential risk. It is obvious that the acceptance of electronic trading is a long-term important decision for most of the customers and that is the reason why the role of risking is so important here [46]. Lim also indicated that the perceived risks are so important in explaining the customers' behavior, in that, the customers are willing to increase their satisfaction from on-line purchase to its maximum rate by stopping making mistakes. Regarding the theory of the perceived risk, the customers perceive the risk because they face a kind of uncertainty and potential dissatisfaction. Such feelings originate from the consequents of their purchase [47] the risk perception of thee. Banking customers primarily grows out of the IT lapses and the resultant losses incurred in fraudulent access to customer accounts [48] the main components of Perceived Risk are perceived security and trust, which have emerged as the top issues in banking adoption. This construct reflects an individual's subjective belief about the possible negative consequences of some type of planned Action, due to inherent uncertainty which is likely to negatively influence usage intentions. Trust is at the heart of all kinds of relationships [49] there are still customers who fear to make use of IB, as they are concerned with security aspects of such a system. Previous research has found the risk associated with possible losses from the online banking transaction is greater than in traditional environments [50]

5.4 Security and privacy

Security Privacy is an indicator used to measure the perceived security and privacy of e-banking [51]. It consists of five elements namely the financial security of e-banking, the trust which individuals have in the service, privacy protection of the customer, security level password and the presence of a third party to validate the Bank's identity. Ease of Use is also an index based on Davis (1989), which contains 4 elements namely e-banking is easy to use, simple, has a user-friendly website and is a flexible system for interaction [52].

Concept of perceived security may be useful to capture the user's subjective perception of the security risks involved in e-banking. Several studies including Jih et al. (2005) indicate that user adoption of e-banking is affected by perceived security. This supports a view of security as crucial to the overall usability of e-banking systems [53] Security issues are a major source of concern for everyone both inside and outside the banking industry. E-banking increases security risks, potentially exposing hitherto isolated systems to open and risky environments [54] the importance of security and privacy for the acceptance of online banking has been noted in many banking Studies [55]

H4. Security and privacy have a negative impact on trust

If the index of security and privacy is low, it generates fears among customers leading to reduced customer Trust indicator; in this case the customer will go to non-use of electronic banking

5.5 Trust

Trust can be defined as "function of the degree of risk involved in the e-banking transaction ,and the outcome of trust is proposed to be reduced perceived risk ,leading to positive intention towards adoption of e -banking [56].Trust and security have always been essential features of the banking system and protection of information assets is necessary to establish and maintain trust between the bank and its customers [57] Lack of Customer trust is a major hurdle in the growth of e-banking although winning consumer trust is more important in online environment; online trust does share a number of characteristics with the offline trust [58] Customer trust in the technology of e-banking is a huge hurdle given the intangible nature of the service .trust includes essential notions of technology security Reliability and protection against hackers and theft of client identity or financial information [59] added that to increase external validity of TAM, it is necessary to further explore the nature and specific influences of technological and usage–context factors that may alter the user's acceptance. For instance, recent research has indicated that "trust" has a striking influence on users' willingness to engage in online exchanges of money and sensitive personal information [60] The use of this new technology is too new to the developing countries, and this may be a cause of the lack of trust from the customers in using the internet banking or e-banking as a whole. When the customers have a feeling of no trust and uncertainty for the phenomena, it is believed that they look at it as a risk [61] numerous studies have tried to find correlations between trust and experience with a new system, concept, or relationships, including a correlation to the frequency of e-commerce Activity, and as such, other researchers have noted that trust may be significantly influenced by the culture of a given society [62] the importance of trust and security as direct or indirect influencing factors in an individual's intention to engage in online transactions. Trust refers to a degree of an individual willingness to be vulnerable to the actions of others [63].

H5. Lack of Trust has a negative impact on actual e-banking Use

6. CONCLUSION AND FUTURE WORK

Through this study we conclude that the level of customer knowledge in information technology is important factor influencing the security of banking, in other words the higher the level of customer knowledge in information technology the fewer security flaws that may occur, and this is an indicator that the banking security risks will be reduced and increase the degree of safety , this shows that increase the degree of safety generate confidence among customers who use banking applications through the Internet, We conclude that the high level of customers knowledge leads the customers to take precautions and follow the correct behavior to protect their data from attack. When users become more familiar with a technology and Internet, in this case, they tend to have higher expectations towards the technology. This research is initial step for future work; in the future we will conduct experimental studies to test our model.

7. REFERENCES

[1] Mahdi, S. and Mehrdad, A. E-Banking in Emerging Economy: Empirical Evidence of Iran, International Journal of Economics and Finance, Vol. 2, No. 1, February 2010, pp. 201-209.

[2] Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. International Journal of Bank Marketing, Vol. 17 No. 7, pp. 324-34.

[3] Hertzum, M., Juul, .N.C., Jorgensen N., Usable Security and E-Banking: ease of use vis-a-vis security, Australasian Journal of Information Systems, Vol 11, No 2 (2004).

[4] Rahmath Safeena, Hema Date and Abdullah Kammani , Internet Banking Adoption in an Emerging Economy: Indian Consumer's Perspective , International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011.

[5] http://www.buzzle.com/articles/internet-banking-problems.html.

[6] Akhlaq, Mohammed ather and Shah, Asadullah (2011) Internet banking in Pakistan: finding complexities. Journal of Internet Banking and Commerce, 16 (1). pp. 1-14.

[7] Davis, F.D, A technology acceptance model for empirically testing new end-user information systems: Theory and results, Doctoral Dissertation, Sloan School of Management, Massachusetts Institute of Technology, 1986.

[8] Tan, M. and Teo, T. (2000) Factors Influencing the Adoption of Internet Banking, Journal of the Association for Information Systems, 1, 5, 1-42.

[9] Davis, F 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly. Vol. 13 No. 3, pp 319 –340.

[10] http://socialreport.msd.govt.nz/documents/knowledge-skills-social-report-2010.pdf.

[11] Lassar, W.M., Manolis, C. and Lassar, S.S., (2005). The relationship between consumer innovativeness, personal characteristics, and online banking adoption. International Journal of Bank Marketing, 23 (2), pp 176-199.

[12] Ongkasuwan M, Tantichattanon W (2002). A Comparative Study of Internet Banking in Thailand. Retrieved on [May, 2010] from World Wide Web: http://www.ecommerce.or.th/nceb2002/paper/55- A_Comparative_Study.pdf.

[13] http://www.ukessays.com/essays/information-systems/information-security- crime-management.php.

[14] http://www.anz.com/personal/ways-bank/security/online-security/threats-banking-safety/computer-threats/.

[15] Jason Milletary, Technical Trends in Phishing Attacks, CERT Coordination Center1, (2005), pp. 1-17.

[16] Williamson, Gregory D. Enhanced Authentication In Online Banking, Journal of Economic Crime Management, Vol. 4, Issue 2, 2006.

[17] New Perspectives on Computer Concepts 2013: Introductory, June Jamrich Parsons, Dan Oja – 2012.

[18] Internet GIS: Distributed Geographic Information Services for the Internet. Zhong-Ren Peng, Ming-Hsiang Tsou - 2003 - 679 :عدد الصفحات

[19] HTTP: Developer's Handbook ,Chris Shiflett – 2003.

[20] S. Kierkegaard, "Swallowing the bait, hook, line and sinker: Phishing, pharming and now rat-ting!," in Managing Information Services in Financial Services H. R. Rao, M. Gupta, and S. J. Upadhyaya, Eds. USA: IGI Publishing, 2008, pp. 241-253.

[21] Auburn University, http://www.auburn.edu/oit/phishing/

[22] Gerald Goh Guan Gan, Tan Nya Ling, Goh Choon Yih and Uchenna Cyril Eze; Phishing: A Growing Challenge for Internet Banking Providers in Malaysia Communications of the IBIMA Volume 5, 2008 133 Phishing: A Growing Challenge for Internet.

[23] R. Dhanalakshmi, C. Prabhu, C. Chellapan , Detection Of Phishing Websites And Secure Transactions , International Journal of Communication Network and Security(IJCNS-2011), Volume. 1 Issue. 2.

[24] http://educationinfree.wordpress.com/2012/05/31/what-is-keylogger-2/.

[25] http://www.iwar.org.uk/comsec/resources/spyware/thompson.htm#_ftnref6.

[26] http://www.antivirusworld.com/articles/keylogger.php.

[27] Adrian McCullagh, William Caelli ,Who Goes There? Internet Banking: A Matter of Risk and Reward, Information Security and Privacy - ACISP 2005, 4-6 July 2005, Australia, Queensland, Brisbane.

[28] For detailed information on PWSteal.Bankash.A (MCID 4326), see http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bankash.a.html.

[29] French, T. K. Liu, K. and Springett, M. , 'A Card-Sorting probe of E-Banking Trust Perceptions', Proceedings HCI 2007, BCS, (2007) ISBN 1-902505-94-8.

[30] Juliet Bugembe , Perceived Usefulness, Perceived Ease Of Use, Attitude and Actual Usage Of A New Financial Management System: A Case Study Of Uganda National Examinations Board, JUNE 2010.

[31] Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. Information & Management, 40, 191–204.

[32] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of Information technology. MIS Quarterly, 13(3), 319-340. http://www.jstor.org/pss/249008.

[33] Wadie Nasri, Factors Influencing the Adoption of Internet Banking in Tunisia, International Journal of Business and Management, Vol. 6, No. 8; August 2011.

[34] syed shan e raza, impact of user it and internet skills on online banking, Input to innovative banking strategies, international journal of social sciences and humanity studies Vol 3, no 1, 2011 issn: 1309-8063 (online).

[35] Sam Ian , Online Banking and the role of CRM: The impact of the internet as online business platform on CRM (Study of Online banking in the UK).

[36] Muhammad Muazzam Mughal, Muhammad Farhan, Kamran Ali, Abdul Jabbar Khan, Accepting of E-banking among Banking Customers of Pakistan, Information Management and Business Review Vol. 4, No. 6, pp. 332-339, June 2012.

[37] Raphaël K. Akamavi, (2005) "Re-engineering service quality process mapping: e-banking process", International Journal of Bank Marketing, Vol. 23 Iss: 1, pp.28 – 53.

[38] Henny Medyawati 1, Marieta Christiyanti 2 and Muhammad Yunanto, e-banking adoption analysis using technology acceptance model (tam): empirical study of bank customers in bekasi city , 2011 International Conference on Innovation, Management and Service IPEDR vol.14(2011).

[39] Fred D. Davis , Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly, Vol. 13, No. 3 (Sep., 1989), pp. 319-340.

[40] Geetha Kallamarthodi, Malarvizhi Vaithiyanathan; Empirical Assessment of a Modified Technology Acceptance Model in Emerging Economy: An Assessment from the Perspective of Indian Consumers", 2011 International Conference on E-business, Management and Economics IPEDR Vol.25.

[41] Apostolos Giovanis, Spiridon Binioris; factors affecting internet banking usage behavior: an empirical investigation of Greek customers, Proceedings of the 2nd International Conference: Quantitative and Qualitative Methodologies in the Economic and Administrative Sciences.

[42] Littler, D., Melanthiou, D. (2006) ‘Consumer perceptions of risk and uncertainty and the implications for behavior towards innovative retail services: the case of internet banking’, Journal of Retailing and Consumer Services, 13, 431-43.

[43] Intel Top 10 Technology Risks http://www.nor-tech.com/solutions/dox/Top_10_Technology_Risks.pdf.

[44] Khan, A.R. and Karim, M. (2010). E-Banking and extended risks: How to deal with the challenge, Paper Presented to the Department of Finance and Banking, Rajshahi University, pp.17.

[45] André L.M. dos Santos, Richard A. Kemmerer, Safe Areas of Computation for Secure Computing with Insecure Applications, 15th Annual Computer Security Applications Conference (ACSAC '99).

[46] Koller M (1988). Risk as a determinant of trust. Basic Appl. Soc.Psychol., 9(4): 265–276.

[47] Lim N (2003). Consumers'' perceived risk: sources versus consequences. Electron. Commer. Res. Appl., 2: 216–228.

[48] Littler, Dale and Melanthiou, Demetris (2006), “Consumer Perceptions of Risk and Uncertainty and The Implications for Behavior towards Innovative Retail Services: The Case Of Internet Banking, Journal of Retailing and Consumer Revices, Vol: 13:431-443.

[49] AL. Zhao, NK. Lewis, SH. Lloyd, and P. Ward, (2010), “Adoption of internet banking services in China: is it all about trust?” International Journal of Bank Marketing, vol. 28, no. 1, pp. 7-26.

[50] L. Bradley and K. Stewart, “Delphi study of Internet banking,” Marketing intelligence and planning, vol. 21, no. 5, pp. 272-281,2003.

[51] Taylor, S. and Todd, P.A. (1995). Understanding information technology usage: a test of competing models. Information Systems Research, 6(2), 144-176.

[52] Tandrayen-Ragoobur, Verena; Ayrga, Anisha, Is Mauritius Ready to E-Bank? From A Customer and Banking Perspective, SOURCE Journal of Internet Banking & Commerce; Apr2011, Vol. 16 Issue 1.

[53] Morten Hertzum, Niels Jorgensen, Mie Norgaard: Usable Security and E-Banking: ease of use vis-a-vis security. Australasian J. of Inf. Systems 11(2) (2004).

[54] Carol Sergeant, Director, Banks & Buildings Societies, Financial Services Authority, http://www.fsa.gov.uk/library/communication/speeches/2000/sp46.shtml.

[55] Sathye, M. (1999), "Adoption of Internet banking by Australian consumers: an empirical investigation", International Journal of Bank Marketing, Vol. 17 No. 7, pp. 324-34.

[56] Hamid Reza Peikari ,A Study on the Interrelations between the Security-Related Antecedents of Customers’ Online Trust, Global Communications in Computer and Information Science Volume 92, 2010, pp 139-148.

[57] Jayaram Kondabagil , Risk Management in Electronic Banking: Concepts and Best Practices, Ch7, P-69- 2007.

[58] Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior, 21.

[59] Jennifer Isern,A cross-country analysis of the effects of e-banking and financial, Nova Southeastern University – 2008.

[60] Hoffman, DL, Novak, TP & Peralta, M 1999, ‘Building consumer trust online’, Communications of the ACM, vol. 42, no. 4, pp. 80-85.

[61] Reza Shafei , Vala Mirani, Designing a model for analyzing the effect of risks on e-banking adoption by customers: A focus on developing countries, African Journal of Business Management Vol. 5(16), pp. 6684-6697, 18 August, 2011.

[62] McKnight, D. and N. Chervany. (2001). “What trust means in e-commerce customerrelationships: An interdisciplinary conceptual typology.” International Journal of Electronic Commerce 6: 35-59.

[63] Mayer, R. C., Davis, J. H. & Schoorman, F. D.(1995). 'An Integrative Model of Organizational Trust,' Academy of Management Review, 20(3):709-734.