USER AWARENESS OF SECURITY FEATURES IN INTERNET BANKING – AN EMPIRICAL INVESTIGATION

[1]Prof. Ajimon George, [2]Dr. G.S Gireeshkumar

Abstract

In the banking sector, technology and competition have increased the choice of customers regarding banking products and providers. As a result various electronic delivery channels are increasingly used by banks for delivering their products and services at the convenience of customers at low cost. Internet Banking (IB) is one among them. IB refers to a banking transaction routed through internet. It is a method of banking that allows a customer to perform banking transactions through a bank's website hosted in the internet. The objective of the study was to understand customer awareness of IB security features adopted by banks and to investigate whether there is any association between customer awareness and their level of computer knowledge. Respondents were asked to state whether they are aware or not of the ten security features used by banks to safeguard their customers from the risk of fraud associated with the use of IB. It is found that majority of the respondents have awareness of all the security features except padlock symbol. Significant association is also found between awareness of VeriSign, Padlock Symbol, The letter 's' in the URL, Virtual Key board and level of computer knowledge of the respondents.

Key Words: E-Banking, Internet Banking, Padlock Symbol, VeriSign, Virtual Key Board.

INTRODUCTION

Information Technology has transformed every spectrum of human life including the provision of banking services. In the banking sector, technology and competition have increased the choice of customers regarding banking products and providers. As a result various electronic delivery channels are increasingly used by banks for delivering their products and services at the convenience of customers at low cost. Delivery of banking services to customers at their office or home with the help of electronic technology is termed as e-banking. E-banking has facilitated bank customers by providing anytime and anywhere banking service. According to Karjaluoto (2002) electronic banking is a construct that consists of several distribution channels. E-banking may be identified with three channels viz., ATM, Internet Banking and Tele banking (Kapoor and Dhingra, 2007).

Internet is gaining popularity as a delivery channel in the banking sector. Internet Banking (IB) has become a competitive necessity for banks as competitors are just one click away. With the increasing use of

Prof. Ajimon George
Associate Professor
Marian college
Kuttikkanam–685 531, Kerala
E-mail: georgeajimon@rediffmail.com

Dr. G.S. Gireeshkumar
Associate Professor
Nirmala College
Muvattupuzha – 686 661
E-mail: gireeshkartha@yahoo.com

technology in the banking sector, customers can change their banking service provider much faster than in the traditional banking set up if they are not satisfied with the products, prices or services offered by a particular bank. Therefore banks are competing with one another to reach more and more customers through electronic channels particularly IB. IB refers to a banking transaction routed through internet. It is a method of banking that allows a customer to perform banking transactions through a bank's website hosted in the internet. It is also called virtual banking or online banking. It is a form of self service banking technology. IB can be defined as the use of technology to communicate instructions and receive information from a financial institution where an account is held. IB includes the system that enables financial institution, customers, individuals or business to access accounts, transact business or obtain information on financial products and services through a public or private network, including the internet. (Prakash and Malik, 2008)

REVIEW OF LITERATURE

A survey of existing literature revealed that a flurry of studies on IB has been undertaken. Adoption, risk perception, usage and service quality of IB are the topics heavily examined in e-banking literature. In many studies, consumers security and risk concerns is found to be a major inhibitor for the adoption of IB (for e.g. Geetika et al., 2008; Guangying 2009; Laukkanen et al., 2008; Manzano-Aldas et al., 2009; Ozdemir and Trott 2009; Philip et al., 2006; Ramayah et al., 2002; Srivastava 2007; Sujana 2008, Winnie and John 2002; Yiu et al., 2007). Sylvie Laforet (2005) found that hackers and fraud were found to be one of the main barriers of online banking adoption in China. Ahmad and Saima (2008) states that 'chances of fraud' and 'lack of information security' to be vital risks associated with electronic banking in Pakistan. . In the IB context, as customers perform banking transactions using internet, they perceive certain element of risk. Peter and Ryan (1976) defined perceived risk as a kind of subjective expected loss. Ming (2009) defined perceived risk in the context of IB as "the subjectively determined expectation of loss by an online bank user in contemplating a particular online transaction". Polatoglu and Ekin (2001) found that perceived risk was one of the major factors affecting consumer adoption as well as customer satisfaction of IB services. The psychological discomfort and anxiety caused by perceptions about risk are likely to devalue perceived usefulness of the e-service (Mauricio Featherman and Mark Fuller, 2003 – cited in Rejikumar and Sudharani, 2012) and can adversely influence continuance intentions as well as satisfaction. Ming (2009) studied the risk factor in detail and identified that security risk, financial risk, performance risk, time/convenience risk have negative effect on the intention to the adoption of on line banking in Taiwan. The security of internet access to client accounts is the biggest challenge that banks are facing (Denny, 2000). Malicious 'Spyware' and 'Trojan Programs' which catches the user id and password, increasing cases of 'Phishing attacks' cause big headaches to both banks as well as customers. For example, more than 15,000 online tickets of Kingfisher Airline were purchased by fraudsters who got credit card information of Indian and foreign nationals. The loss to the carrier was ` 17 crores (Singh, 2007). A study conducted by Egwali Annie (2009) found that 27 per cent of the IB users in Nigeria did not understand the full meaning of the security indicator noticed in the banking sites.

RESEARCH GAP AND OBJECTIVE

For safe banking over internet, it is essential that both customers and banks should take certain precautions to avert the risk of fraud. When customers travel the internet to access IB, they want to be assured that effective safeguards are in place to make their visit safe, secure and reliable. Therefore banks use very secure and hack proof servers and database for the safety of customers besides other security features. But the benefit of security features adopted by banks will go futile if the customers are not aware of various security features. Though there are plenty of literature that examined the risk perceptions of IB users, studies that investigates customer awareness of security features adopted by banks are scant in the literature. This study thus aims to fill the gap in the literature and hence the study is quite relevant and timely from the point of view of both academic and banking industry. The study raised the following pertinent questions for enquiry. Are the customers aware of security features used by banks for protecting them from the risk of fraud? Is there any association between their awareness and level of computer knowledge? Based on the above research questions, the specific objective of the study was to understand customer awareness of IB security features adopted by banks and to investigate whether there is any association between customer awareness and their level of computer knowledge.

METHODS AND MATERIALS

The study is empirical in nature and survey method has been used to collect primary data from 406 IB users from public sector, old private sector and new generation banks in the state of Kerala, India. State bank of India, State Bank of Travancore, Canara Bank and Punjab National Bank were selected from the public sector. Federal Bank and South Indian Bank were selected from the old private sector. HDFC Bank, ICICI Bank and Axis Bank were selected from the new generation banks. These banks were selected because they are in the forefront in harnessing technology and have won accolades for their excellence in banking technology from Institute for Development and Research in Banking Technology (IDBRT) in various years. A combination of convenience and random sampling method were used because of the difficulty in obtaining from banks a sampling frame which contains the contact details of IB users. The respondents were contacted from institutions/offices/ companies/associations/small scale industrial units etc which were conveniently selected because some of the institutions/offices etc. denied permission to approach their employees. From the selected institutions/offices etc., responses from IB users were obtained on a random basis. The questionnaire was piloted on 40 respondents. Respondents were asked to state whether they are aware or not of the ten security features used by banks to safeguard their customers from the risk of fraud associated with the use of IB. Since IB services are delivered through the medium of internet, customers have to be familiar with a set of accompanying technologies such as a personal computer and a web browser (Lee et al., 2005). Customers' prior experience in using computer and internet ease the complexity of using IB services. Proficient users of the internet will consider accessing IB services to be less complex and will therefore show a greater proclivity to use it (Black et al., 2001). Therefore, respondents were asked to rate, as their own, working level of computer knowledge as average or advanced. Of the total

406 respondents, 56 per cent rated their working level of computer knowledge as 'average' and 44 per cent rated as "advanced'.

DESCRIPTION OF SECURITY FEATURES IN INTERNET BANKING

The various security features incorporated by banks to protect IB users from various risks associated with IB are given below. The item code used to denote each of the security features are given in brackets.

VeriSign (S1) – VeriSign symbol is found on the index page of the Internet banking website of banks, which guarantees that users are dealing with a secure website. VeriSign is world's leading Internet Certification Authority.

Padlock Symbol (S2) - Padlock symbol on the net banking screen is an indication that the website is legitimate. There is a de facto standard among web browsers to display a "lock" icon somewhere in the window of the browser. For example, Microsoft Internet Explorer displays the lock icon in the lower-right of the browser window. Double clicking on it will display the VeriSign Certificate authenticating the site.

The letter 's' in the URL (S3) - IB users will know that they are at a secured site when they see https:// in the address field on the internet browser. It means that the user name and password typed will be encrypted before sent to bank's server. The letter 's' in the URL indicates that the web site is 'secured'.

Virtual Keyboard (S4) - The Virtual Keyboard is an onscreen keyboard which provides a mouse based alternative, for entering IB username and password, instead of using the actual physical keyboard. A virtual keyboard prevents IB username or password from being stolen, especially while using public computers, such as those available in Internet cafes. Public computers may have software installed over them known as "Keylogger" which stores the information about the keys pressed and the pages accessed. IB users use the mouse to enter the username and password by clicking on the keys of the Virtual Keyboard rather than typing them using the keyboard.

SMS Alert (SS) – IB users receive regular SMS alerts from the bank when their account is credited or debited. Any unauthorized transactions happened in an account is immediately brought to the notice of the IB user through SMS alerts.

Sign on Password Expiry (S6) – If an IB user is not changing his/her password within a specified period of time (e.g. 180 days for Federal bank and South Indian bank) IB password expires as per the Security Policy of banks. This security feature forces IB users to change their passwords.

Automatic Lockout on Multiple Incorrect Password Entry (S7) – To prevent somebody from guessing any of the IB user's password and getting unauthorized access to IB account, the user ID is locked immediately in case of a specified number of (usually 3 times) wrong password entries.

Automatic Timeout if Account not Operated for Specified Time (S8) - To prevent an unauthorized person from viewing someone's net banking account in case an IB user leave his/her computer idle, the internet session is closed in case of inactivity for a specified period of time (usually 5 minutes).

Mandatory Use of Special Characters in Password (S9) – To prevent somebody from

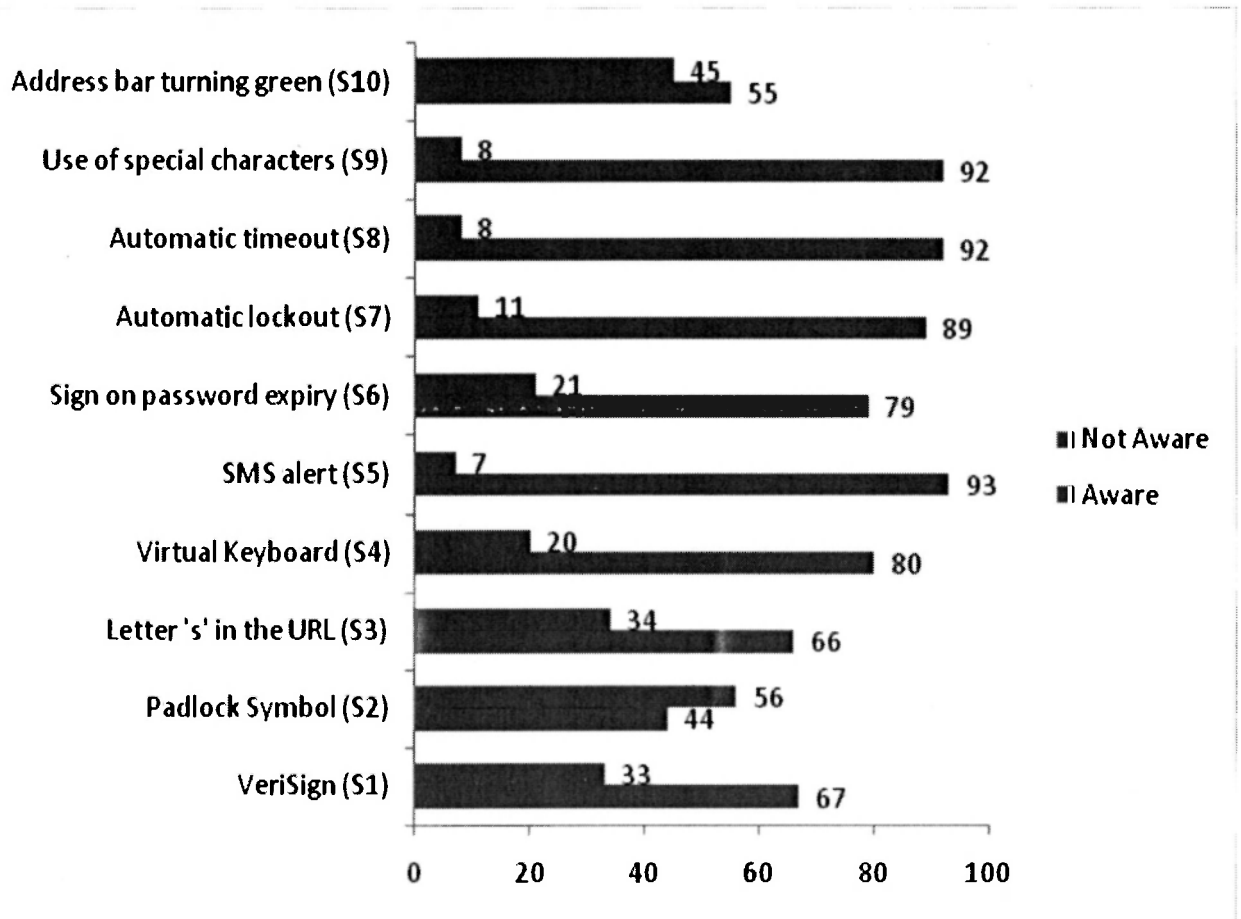
guessing any of the IB user's password and getting unauthorized access to IB account, the password should compulsorily contain a mix of alphabets, numbers and special characters such as !@#$%^&*(){}[]. This security feature prohibits IB users to use personal data as passwords such as name, address, telephone number etc. which are easily guessable by others.

The Address Bar Turning Green (S10) – If the address bar is turning green, it is an indication that it is safe and the site is legitimate. Higher version of web browsers like Microsoft Internet Explorer 7 and above, Firefox 3.03 and above, Opera 9.5 and future versions of these browsers will support Extended Validation Secure Socket Layer (EV-SSL) feature and trigger the green bar. EV-SSL certificates are special SSL certificates that clearly identify a web site's organizational identity. Hence IB users are advised to upgrade web browsers regularly.

DATA ANALYSIS AND HYPOTHESIS TESTING

Figure 1 portrays IB user's awareness of each of the 10 security features adopted by banks.

Figure 1
Customer Awareness of Security Features Adopted by Banks



Source: Primary data

The top three security features about which over 90 per cent of the respondents has awareness are S5 (SMS alert), S8 (Automatic time out) and S9 (Mandatory use of special characters) respectively. Eighty nine per cent know about S7 (Automatic lock out), 80 per cent know about S4 (Virtual keyboard), 79 per cent know about S6 (Sign on password expiry), 67 per cent know about S1 (VeriSign), 66 per cent know about S3 (The letter 's' in the URL), 55 per cent know about S10 (Address bar turning green). More than half of the respondents (56 per cent) have no awareness of S2 (Padlock symbol). Thus it can be concluded that majority of the respondents have awareness of all the security features except S2.

Certain element of knowledge of computers and internet is a pre-requisite for banking over internet particularly for understanding the security features. Therefore, Chi-square test was used to examine the association between awareness of security features and level of computer knowledge of IB users and the results are given in Table 1.

H_0: There is no significant association between awareness of security features and level of computer knowledge.

Table 1

Association between Awareness of Security Features and Level of Computer knowledge

Code	Awareness	Average Level	Advanced Level	Total	χ^2	Sig.
S1	Not aware	105 (46)	29 (16)	134 (33)	39.205*	0.000
	Aware	124 (54)	148 (84)	272 (67)		
	Total	229 (100)	177 (100)	406 (100)		
S2	Not aware	144 (63)	84 (48)	228 (56)	9.647*	0.002
	Aware	85 (37)	93 (52)	178 (44)		
	Total	229 (100)	177 (100)	406 (100)		
S3	Not aware	106 (46)	32 (18)	138 (34)	35.408*	0.000
	Aware	123 (54)	145 (82)	268 (66)		
	Total	229 (100)	177 (100)	406 (100)		
S4	Not aware	61 (27)	20 (11)	81 (20)	14.707*	0.000
	Aware	168 (73)	157 (89)	325 (80)		
	Total	229 (100)	177 (100)	406 (100)		
S5	Not aware	14 (6)	15 (9)	29 (7)	0.839	0.360
	Aware	215 (94)	162 (91)	377 (93)		
	Total	229 (100)	177 (100)	406 (100)		
S6	Not aware	53 (23)	32 (18)	85 (21)	1.547	0.214
	Aware	176 (77)	145 (82)	321 (79)		
	Total	229 (100)	177 (100)	406 (100)		

S7	Not aware	30 (13)	14 (8)	44 (11)	2.784	0.095
	Aware	199 (87)	163 (92)	362 (89)		
	Total	229 (100)	177 (100)	406 (100)		
S8	Not aware	25 (11)	7 (4)	32 (8)	6.665	0.010
	Aware	204 (89)	170 (96)	374 (92)		
	Total	229 (100)	177 (100)	406 (100)		
S9	Not aware	16 (7)	17 (10)	33 (8)	0.916	0.339
	Aware	213 (93)	160 (90)	373 (92)		
	Total	229 (100)	177 (100)	406 (100)		
S10	Not aware	111 (49)	71 (40)	182 (45)	2.820	0.093
	Aware	118 (51)	106 (60)	224 (55)		
	Total	229 (100)	177 (100)	406 (100)		

Source: Primary data *Significance at 5 per cent level
Note: Figures in parenthesis indicates percentage to total

The results of Chi-square test revealed that there is significant association between awareness of S1 (VeriSign), S2 (Padlock symbol), S3 (The letter 's' in the URL) and S4 (Virtual keyboard) and level of computer knowledge at 5 per cent significance level as the observed significance of Chi-square values are less than 0.05.

Hence the null hypothesis is rejected for all these features and the alternative hypothesis is accepted and concluded that there is significant association between awareness of S1, S2, S3 and S4 and level of computer knowledge. It means that the difference in the percentage of users with advanced and average level of computer knowledge regarding awareness of the above mentioned security features is statistically significant. It is clear from Table 1 that larger percentage of IB users with advanced level of computer knowledge has awareness of S1, S2, S3 and S4 security features as compared to those with average level of computer knowledge.

S5 (SMS alert), S6 (Sign on password expiry), S7 (Automatic lockout) S8 (Automatic timeout) S9 (Mandatory use of special characters) and S10 (Address bar turning green) security features are found to have no association with level of computer knowledge at 5 per cent significance level as the observed significance of Chi-square values are more than 0.05. It means that the difference in the percentage of users with advanced and average level of computer knowledge regarding awareness of the above mentioned security features is not statistically significant. Hence the null hypothesis is accepted and concluded that there is no significant association between awareness of S5, S6, S7, S8, S9 and S10 security features and level of computer knowledge.

CONCLUSIONS AND SCOPE FOR FURTHER RESEARCH

From the foregoing analysis, it appears that, though majority of the respondents have awareness of various security features, there are users who are not aware of security features

especially about 'Padlock symbol' and 'Address bar turning green'. Before entering the user id and password, it is absolutely essential to ensure that the customer is not interacting with a website which is a replica of bank's website. 'Padlock Symbol' and 'Address bar turning green' are security features which indicate that the website is safe and legitimate.

Those who have lack of awareness of the above two security features are more vulnerable to the risk of fraud associated with IB. Therefore it is the need of the hour to create awareness about these security features amongst IB users particularly with average level of computer knowledge. Larger percentage of IB users with average level of computer knowledge are not aware of VeriSign', 'Padlock symbol', 'The letter 's' in the URL', and 'Virtual keyboard' security features when compared to those with advanced level of computer knowledge. These are 'risk preventive' in built security features. The above findings have managerial implications for banks to take necessary steps to guard users against the risk associated with IB. It is essential that IB service providers should educate their customers not only about the significance of risk preventive security features but also about risks of online banking and the steps the banks are taking to help mitigate those risks. Non awareness of IB security features limits the amount of banking transactions conducted by IB adaptors. Periodic articles in bank newsletters and in email messages and on bank websites can help increase customer awareness on these important security features.

The study has limitations as most field surveys suffer from. The study considered the perceptions of only retail banking customers and the perceptions of wholesale banking customers who use IB were not considered. Future research may replicate this study with wholesale banking customers to evaluate the validity of the findings of this study. Wholesale banking customers may use IB more frequently and therefore to enquire whether their awareness are similar to those of retail banking customers would be of interest to future researchers. The validity of the survey findings would have been enriched if the researcher had used probabilistic sampling technique for collecting the sample for the study. Since the banks cited confidentiality for not providing their customer details, the researcher resorted to non-probabilistic sampling technique. The present study was a cross sectional study in which subjects are contacted at a fixed point in time and relevant information is obtained from them. Additional research efforts are needed to evaluate the validity of the findings by conducting a longitudinal study at some point in future.

REFERENCES

Ahmed Kaleem and Saima Ahmad (2008), Bankers perceptions of electronic banking in Pakistan, *Journal of internet banking and commerce*, 13(1): 1-16.

Black, N.J., Lockett, A. Winklhofer, H. and Ennew,C. (2001), The adoption of internet financial services: a qualitative study, *International Journal of Retail and Distribution Management*, 29(8): 390-398.

Denny Stephanie (2000), The Electronic Commerce Challenge, *Journal of internet banking and commerce*, 3(3): 1-6.

Egwali Annie Oghenerukeybe (2009), Customers perception of security indicators in online banking sites in Nigeria, *Journal of Internet Banking and Commerce*, 14(1):1-15.

Geetika, Tanuj Nandan and Ashwani Upadhyay (2008), Internet Banking in India: Issues and Prospects, *The Icfai Journal of Bank Management*, 7(2): 47-61.

Guangying Hua (2009), An Experimental Investigation of Online Banking Adoption in China, *Journal of Internet Banking and Commerce*, 14(1): 1-12.

Kapoor, S. and Dhingara, D. (2007), Application of Information Technolgy in Banking. In R.K Uppal and Rimi Jatana, *E-banking in India : Challenges and opportunities* (pp. 97-111), New century publications: New Delhi.

Karjaluoto, H., Mattila, M. & Pento, T. (2002), Electronic banking in Finland: Consumer beliefs and reactions to a new delivery channel, *Journal of Financial Services Marketing*, 6(4): 346-361.

Laukkanen, P., Sinkkonen, S. and Laukkanen, T. (2008), Consumer resistance to internet banking: Postponers, opponents and rejectors, *The international Journal of Bank Marketing*, 26(6): 440-455.

Lee, E.K., Kwon, K.N. and Schumann, D.W. (2005), Segmenting the non-adopter category inthe diffusion of internet banking, *International Journal of Bank Marketing*, 23(5): 414-437.

Manzasno-Aldas, J., Navarre-Lassala, C., Mafe-Ruiz, C. and Blas-Sanz, S. (2009), Key drivers of internet banking services use, *Online Information Review*, 33(4): 672-695.

Ming-Chi Lee (2009), Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit, *Electronic Commerce Research and Applications*, l(8) :130-141.

Ozdemir Sena and Trott Paul (2009), Exploring the adoption of a service innovation: A study of internet banking adopters and non-adoptors , *Journal of Financial Services Marketing*, 13(4): 284-299.

Peter, J.P. and Ryan, M.J. (1976), An investigation of perceived risk at the brand level, *Journal of market research*, 13 (1): 184-188.

Philip Gerrard, Barton Cunningham, J. and James F. Devlin (2006), Why consumers are not using internet banking: a qualitative study, *Journal of Services Marketing*, 20(3): 160-168.

Polatoglu, V. and Ekin, S. (2001), An empirical investigation of the Turkish consumer's acceptance of internet banking services, *International journal of Bank marketing*, 19(4): 156-165.

Prakash, A. and Malik, G. (2008), Empirical study of internet banking in India, *CURIE, BITS Pilani*, 1(3): 83-92.

Ramayah, T., Ismail, N., and Ling, K.P. (2002), An exploratory study of Internet banking in Malaysia, Proceedings from Hangzhou City, P.R. China : *Third International Conference on Management of Innovation and Technology (ICMIT'02 and ISMOT'02.*

Rejikumar, G. and D. Sudharani Ravindran, (2012), An empirical study on service quality perceptions and continuance intention in mobile banking context in India, *Journal of Internet Banking and Commerce*, 17(1): 1-22.

Singh, N.P. (2007), Online fraud in Banks with Phishing, *Journal of Internet banking and commerce*, 12(2): 1-27.

Srivastava Rajeshkumar (2007), Customer's perception on usage of internet banking, *Innovative Marketing*, 3(4): 67-73.

Sujana Adapa, (2008), Adoption of Internet shopping: cultural considerations in India and Australia, *Journal of Internet Banking and Commerce*, 13(2): 1-17.

Sylvie Laforet and Xiaoyan Li (2005), Consumers' attitudes towards online and mobile banking in China, *International Journal of Bank Marketing*, 23 (5): 362-380.

Winnie Chung and John Paynter (2002), An evaluation of Internet banking in New Zealand, *Proceedings of the 35th Hawaii International Conference on System Sciences*, download from IEEE Xplore from Indian Institute of Management, Calicut.

Yiu Shing Chi, Grant, K. and Edgar, D.(2007), Factors affecting the adoption of Internet banking in Hong Kong – implications for the banking sector, *International Journal of Information Management*, 336-351 retrieved from http:// www. Sciencedirect.com