IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X.Volume 8, Issue 5 (Mar. - Apr. 2013), PP 01-09
www.iosrjournals.org

Innovation in Indian Banking: Extent of Precautions Taken By the Customers While E-Banking

Shakira Irfana[1], Prof.A.Raghurama[2]
[1](Research Scholar, Department of Commerce/Mangalore University, India)
[2](Professor, Department of Commerce/Mangalore University, India)

Abstract: *Financial liberalization and technology revolution have allowed the developments of new and more efficient delivery and processing channels as well as more innovative products and services in banking industry. Banking institutions are facing competition not only from each other but also from non-bank financial intermediaries as well as from alternative sources of financing. As financial institutions increasingly offer online banking services to their customers, they must face issues of consumer confidence in the Internet. Consumers are concerned about identity theft and wonder if the Internet is safe for online banking. The answer is yes—if financial institutions, in cooperation with their customers, make it safe. Therefore, building the best controls to prevent fraud and protect customers is of critical importance.*

This paper investigates the extent of safety measures followed by customers while e-banking, analyses the awareness of the customers regarding the various online banking scams and suggests safety measures to be followed while e-banking. Primary data was collected from 118 respondents through a structured questionnaire. Secondary data was used to know about the various electronic e-banking products and services and various online scams. The findings are of great help to bankers to enable them to frame proper guidelines for their customers who use e-banking facility. It helps e-banking customers to bank safely using the safety measures.

Key words- *E-banking, innovation, internet, online scams, safety measures.*

I. Introduction

Indian banking is the lifeline of the nation and its people. Banking has helped in developing the vital sectors of the economy and usher in a new dawn of progress on the Indian horizon. The sector has translated the hopes and aspirations of millions of people into reality. But to do so it has to control miles and miles of difficult terrain, suffer the indignities of foreign rule and the pangs of partition. Today, Indian banks can confidently compete with modern banks of the world.

As the banking institutions expand and become increasingly complex under the impact of deregulation, innovation and technological up gradation, it is crucial to maintain balance between efficiency and stability. During the last 30 years since nationalization tremendous changes have taken in the financial markets as well as in the banking industry due to financial sector reforms. The banks have shed their traditional functions and have been innovating, improving and coming out with new types of services to cater to the emerging needs of their customers. Banks have been given greater freedom to frame their own policies. Rapid advancement of technology has contributed to significant reduction in transaction costs, facilitated greater diversification of portfolio and improvements in credit delivery of banks.

During the past one decade, one of the sectors which underwent visible sea-change through innovative strategies is undoubtedly the banking sector. The sector has been growing at a fast pace in India and is challenged with several aspects like new regulations from time to time, changing customer needs and perceptions, changing technology and changing operations. Technology has been playing a crucial role in the tremendous improvement of banking services and operations. Banks appear to be on the path of achieving sustainability and a long term survival because of innovation. Technological changes relating to telecommunications and data processing have spurred financial innovations that have altered bank products and services and production processes.

1.1 Statement of the problem

While the e-banking offers enormous advantages and opportunities, it also presents various security risks. With this in mind, banks take extensive steps to protect the information transmitted and processing when banking online. This includes for example, ensuring that confidential data sent over the internet cannot be accessed or modified by unauthorized third parties.

But the banks normally have no influence over the systems used by their customers. The choice is entirely up to them. Moreover, the system selected – a PC connected to the internet, for example – will usually be used for a number of other applications as well. The systems used by online banking customers are therefore

exposed to risks beyond the banks control. For this reason, the banks cannot assume liability for them. To ensure that the bank's security measures cannot be undermined by manipulation, it is essential that customers, too, follow safety measures. Hence, as it is necessary to analyse the extent of safety measures followed by customers while e-banking, this paper focuses on measuring the precautions taken by e-banking customers, their awareness about various e-banking scams and suggests measures for a secured e-banking.

1.2 Objectives of the Study

1. To study the various innovative types of banking, innovative products and services of banking and the types of electronic system in modern banking.
2. To study the various services available through online banking
3. To study the various types of online banking scams
4. To study the extent of precautions followed by customers while e-banking
5. To suggest safety measures while e-banking

1.3 Research Questions

1. What are the various types of banking products and services in e-banking?
2. What are the various online scams in e-banking?
3. What is the extent of precautions followed by customers while e-banking?

1.4 Significance of the Study

A high level of perceived risk is considered to be a barrier to propagation of new innovations in e-banking. Influenced by the imagination – capturing stories of hackers, customers fear that an unauthorized party will gain access to their online account and serious financial implications will follow. "Security" is the biggest single concern for customers when faced with the decision to use internet banking. Security has always been an issue, but its scope has changed from mere doubts about the privacy of personal information to worries of financial loss.

Hence, this study measures the extent of safety measures followed by e-banking customers, educates the e-banking customers regarding the various online scams and suggests the safety measures to be followed while e-banking. The study will help bankers to know the safety measures followed by their customers which will enable them to take steps to educate their customers on safety measures while e-banking. The suggestions provided will help the customers to bank safely.

1.5 Scope of the Study

This study is premised on the current safety measures followed by customers in e-banking residing in Mangalore city of Karnataka. Therefore, responses of selected respondents are sought in providing answers to the research questions. The focus of the research in terms of study groups includes businessmen, doctors, academicians, bank officials, housewives and engineers who used e-banking facility in Mangalore city of Karnataka. Responses from the study groups were analysed to measure the extent of safety measures followed by them and suggest them with the required safety measures while e-banking.

1.6 Research Design

Survey research design and secondary data was used in this study. This research strategy was considered necessary because of its ability to view comprehensively and in detail the major questions raised in the study.

1.7 Study Population

A population is the entire set of relevant units of analysis. Thus, businessmen, doctors, academicians, bank officials, housewives and engineers who used e-banking facility in Mangalore city of Karnataka represent the population of the study.

1.8 Sampling Frame And Sampling Technique

Sampling is the procedure for drawing units from a population. It results in the reduction of the amount of data to be collected, by considering only data from a sub-group rather than all possible elements. When data serving as the basis for generalization is comprised of a subset or sub-group of the population, that subset or subgroup is called sample. Because of the absence of an up-to-date list of customers using e-banking facility in Mangalore city of Karnataka, 118 respondents consisting of 14 businessmen, 11 doctors, 18 academicians, 38 bank officials, 14 housewives and 23 engineers who used e-banking facility were drawn randomly where the respondents were approached for participation in the study.

1.9 Data Type and Data Collection Instrument

Primary data and secondary data were collected for the study. The primary data was obtained from the targeted respondents through a carefully constructed questionnaire. The questionnaire was designed to capture the demographic data of the respondents and the extent of safety measures followed by the respondents while e-banking. The questionnaire was constructed using a three- point likert scale.

Secondary data was collected to study the various e-banking products and services, facilities offered in e-banking and various e-banking online scams.

Method of Data Analysis

The data collected were analyzed using percentages.

II. Types of Innovative Banking

2.1 E-Banking: E-Banking enables people to carry out most of their banking transaction using a safe website which is operated by their respective bank.

Advantages

2.1.1 Faster and more convenient transaction
2.1.2 No longer required to wait in long queues
2.1.3 Opening of account simple and easy
2.1.4 Can apply for bank loan
2.1.5 Cost effective for bankers
2.1.6 Fund transfer becomes faster and convenient
2.1.7 Stock trading, exchanging bonds and other investment

2.2 Core Banking

2.2.1. Depositing and lending of money
2.2.2. Core banking solution
2.2.3 Knowing customers needs

2.3 Corporate Banking

Financial services to large corporate and MNC's.

Services

2.3.1 Overdraft facility
2.3.2 Domestic and international payments
2.3.3 Funding
2.3.4 Channel financing
2.3.5 Letters of guarantee
2.3.6 Working capital facility for domestic and international trade

2.4 Investment banking

2.4.1 Creating funds and wealth of clients
2.4.2 Fund creating in two ways: corporate finance and mergers & acquisitions
2.4.3 Professional sales person providing advice on stock trading

2.5 Rural banking

It provides and regulates credit services for the promotion and development of rural sector mainly agriculture, SSI, cottage and village industries, handicraft and many more

2.6 NRI banking

This facility is designed for diverse banking requirements of the vast NRI population spread across the globe. Deals with NRE (Non Resident External Account), NRO (Non Resident Ordinary Account), FCNR (Foreign Currency Non Resident Account)

2.7 Retail banking

It refers to banking in which banks execute transaction directly with individual rather than corporate banks. It is also known as 'one stop shop'.

Services

2.7.1 Saving and checking accounts
2.7.2 Mortgage

2.7.3 Housing Finance
2.7.4 Auto finance
2.7.5 Consumer durable loans
2.7.6 Personal loans
2.7.7 Educational loans
2.7.8 Credit cards

III. Types of Products and Services

3.1Total Branch Automation which speeds up bank transactions and reduces error, more customer friendly and flexible and paperless transactions.

3.2Any Branch Banking: It is a facility for customers to operate their account from any of the same banks network branch. Facilities available are cash withdrawal and cash deposits, account statement, facility to issue multi-city cheques, fund transfer, balance enquiry, purchase of demand drafts, pay order and repayment of loan account.

3.3Demat services: It offers secure and convenient way to track your securities and investment over a period of time without the hassle of handling physical documents. It provides facility of online trading.

3.4Microfinance: Microfinance refers to a movement that envisions a world in which low income households have permanent access to a range of high quality financial services to finance their income producing activities, build assets, stabilize consumption and protect against risks.

3.4.1 Plastic money: Plastic money are an alternative to the cash or standard money which is convenient to carry and is a generic term for all types of bank cards, debit cards, credit cards, smart cards.

3.4.2 Mobile Banking: In mobile banking, the account can travel with you. One can bank from anywhere, at any time and in any condition or any how using mobile phones. Facilities are balance enquiry, fund transfer, cheque book request etc.

IV. Types of Electronic Systems

4.1 ATM: ATM stands for Automated Teller Machine. In simple words, it is 'simple to use self service solution'. It offers value added services like recharging the mobile, paying the utility bills, mutual fund transactions etc.

4.2 RTGS: RTGS stands for 'Real Time Gross Settlement System'. It is a fund transfer mechanism where transfer of money takes place from one bank to another on a real time or gross basis. This is the fastest possible money transfer system through the banking system. It is primarily for large volume transaction. The time taken for effecting funds transfer from one account to another is normally 2 hours.

4.3 Finacle: This system provides the holistic and integrated transformation approach, complete with solutions and services. Finacle solution addresses the requirements of retail, corporate and universal banking worldwide like core banking solution, E-banking solution, mobile banking solution, wealth management, CRM requirements etc.

V. Various types of online banking scams

With the range of payments becoming ever greater over the world, everyone needs to be aware of the coherent steps that should be taken to minimize the chances of being an online fraud victim. Being an victim of fraud can cause stress and worry, so taking measures to protect yourself is essential. Some common online banking scams are:

5.1Phishing: This is the name given to e-mails that claim to be from your bank or other organizations but are actually sent to you by fraudsters. These e-mails typically urge you to click on a link that takes you to a fake website identical to the one you would expect to see. You are then asked to verify or update your personal information but, by doing so, you are actually giving your information to the fraudster who has created the fake website. The fraudster then uses the details to access your online bank account and take your money. One easy way to spot phishing e- mails is that they are usually addressed to "Dear valued customer" instead of your name. This is because phishing e-mails are usually sent out at random as the fraudsters only have limited information such as e-mail address. In a similar scheme, called 'Vishing', a person calls you and pretends to be a bank representative seeking to verify account information.

5.2Pharming: Pharming is the installation of malicious code on your computer without any acknowledgement on your part. In one type of pharming attack, you open an e-mail, or an e-mail attachment that installs malicious code on your computer. Later, you go to a fake web site that closely resembles your bank or financial institution. Any information you provide during a visit to the fake site is made available to malicious users. Both phishing and pharming share the one characteristic, they are created using technology, but in order to be successful, they require your information. In phishing attacks you have to provide the information or visit

links whereas with pharming, you have to open an e-mail, or e-mail attachment, to become a victim. You then visit a fake website and, without your knowledge, provide information that comprises your financial identity.

5.3Malware: Malware (malicious software) is a computer virus that can be installed on your computer without your knowledge. It is capable of monitoring your PC activity, enabling fraudsters to capture your passwords and other personal information. To be a malware victim, you must be tricked into performing actions you would not normally do. You have to install the malware on your computer either by running a program or by visiting a website through e-mail or instant message link. Then, you are requested to send your bank login information. Your financial information will then be at risk only after you perform all these steps. To make sure you do not become a victim of malware, make sure you have up-to-date anti-virus and anti-spyware software installed.

5.4Money Mules: Money mules are people who accept fraudulently obtained money into their account, and then withdraw the money and transfer it overseas to a fraudster. Money mules are often innocent people who have been deceived into helping criminals transfer funds abroad. Criminals offer prospective mules the chance to earn some easy money – concealing the fact that the work is illegal by advertising the job as a "shipping manager" or "sales manager" for an overseas company. However, money mules are liable for presentation and anyone who thinks they may have been deceived by such a scam should contact the police immediately.

5.5Identity Fraud: This fraud involves criminals obtaining key pieces of personal information that they use to pretend to be you. Criminals use these personal details to obtain financial services products in your name such as credit cards, loans, state benefits and documents such as driving licenses and passports. Alternatively criminals can use your personal information to gain access to your existing accounts.

VI. Results of the Extent of Safety Measures Followed By Respondents While E-Banking

Although internet banking is a very common way of accessing your bank account, it is vital to be aware of the ways in which criminals can try to gain access to your account and to learn how to protect yourself and your money. Financial institutions that employ any form of internet banking should have effective and reliable methods of authenticating customers. An effective authentication system is necessary in order to comply with requirements to preserve customer information to prevent money laundering, reduce fraud, restrain identity theft and promote the legal enforceability of their electronic agreements and transactions.

The risks of doing business with unauthorized or incorrectly identified persons in an internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unforceable agreements.

Table 1- Age of the respondents

AGE	Number of respondents	Percentage
Less than 20 years	6	5%
20-30 years	14	12%
30-40 years	48	41%
40-50 years	38	32%
Above 50 years	12	10%
Total	118	100%

Table 2 – Gender of the respondents

Gender	Number of respondents	Percentage
Male	74	63%
Female	44	37%
Total	118	100%

Table 3 – Educational Qualification of the respondents

Qualification	Number of respondents	Percentage
PUC	12	10%
Graduate	52	44%
Post-Graduate	14	12%
Doctorate Degree	4	3%
Professional Degree	36	31%

Total	118	100%

Table 4 – Job Profiles of the respondents

Job Profile	Number of respondents	Percentage
Businessmen	14	12%
Doctors	11	9%
Academicians	18	15%
Bank Officials	38	32%
Home makers	14	12%
Engineers	23	20%
Total	118	100%

Table 5- Facilities used by respondents in E-banking

Facilities in E-banking	YES		NO	
	No. of respondents	Percentage	No. of respondents	Percentage
a.)Financial transaction such as account to account transfer, bill payment etc	64	54%	54	46%
b.)Electronic bill display and payments	34	29%	84	71%
c.) Funds transfer between customers	18	15%	100	85%
d.) Financial transactions for sales and purchases	102	86%	16	14%
e.) Loan repayment	4	3%	114	97%
f.)Update of savings account	118	100%	0	0%
g.)Online bank statement status	118	100%	0	0%

Table 6 – Extent of safety measures followed while E-banking

Safety measures in E-banking	Sometimes		Always		Never	
	No.	%	No.	%	No.	%
a.)Disabling file and printer sharing in your computer while E-banking	22	19%	12	105	84	71%
b.)Avoiding installation or running software application from unknown sources	18	15%	14	12%	86	73%
c.)Avoid disclosing or entering of personal data like Date of Boirth, CVV number of the credit card, card number to unfamiliar websites, e-mails	22	19%	82	69%	14	12%
d.)Avoid accessing online banking or performing financial transactions from public terminals or computers or devices which cannot be trusted	32	27%	8	7%	78	66%
e.)Avoid keeping the computer on without logging out while E-banking	36	31%	60	51%	22	19%
f.)Ensuring that the website you are transacting on starts with ‘https://’ and not ‘http://’ where s means secure	6	5%	8	7%	104	88%
g.)Looking out for an icon of a padlock at the bottom of the browser	4	3%	5	4%	109	93%
h.)Changing your PIN frequently in 2 months	11	9%	5	4%	102	87%
i.)Not to send credit card or account details via e-mail and phone to anybody	8	7%	3	2%	107	91%
j.) Regularly check the monthly credit card billing statements	6	5%	112	95%	0	0%
k.)Checking the website’s private policy and install the latest anti-virus software and firewalls	63	53%	29	25%	26	22%
l.)Signing on the backside of a new credit card and keeping an eye on it during the transaction	4	3%	114	97%	0	0%

m.)Destroying the carbons of the credit card receipts	58	49%	18	15%	42	36%
n.)Taking immediate action in case of loss and theft	0	0%	118	100%	0	0%
o.)Ensuring that the credit card is swiped in your presence and the billed amount has been double checked before signing the payment slip	14	12%	102	86%	2	2%
p.)Accessing the internet banking site directly by entering the official bank URL and not through any site or links in e-mail	13	11%	32	27%	73	62%
q.)Checking the last log-in-date in your net banking account	18	15%	8	7%	92	78%
r.)Using the virtual keyboard provided on bank's website for logging in	17	14%	15	13%	86	73%
s.)Checking your credit rating system from time to time to make sure that nobody has tried to take out a loan in your name	3	2%	3	3%	112	95%
t.)Using a secured broadband connection to prevent others from accessing your broadband connection	26	22%	74	63%	18	15%
u.)To activate a pop-up window blocker	4	3%	8	7%	106	90%
v.)Ensuring that the ATM card, credit card & PIN are not kept together	4	3%	112	95%	2	2%

Table 7 – Frauds aware of by the customers in E-banking

Various frauds in E-banking	YES		NO	
	No. of Respondents	Percentage	No. of Respondents	Percentage
a.)Phishing	48	41%	70	59%
b.)Pharming	36	31%	82	69%
c.)Money mules	26	22%	92	78%
d.)Malware	38	32%	80	68%
e.)Identity Fraud	32	27%	86	73%
f.)Brand Spoofing	28	24%	90	76%
g.)Cyber-Mugging	18	15%	100	85%
h.)Trojan horses	16	14%	102	86%
i.)Keystroke sniffer	8	7%	110	93%
j.)Salami Slicing	6	5%	112	95%
k.)Skimming	12	10%	106	90%

6.1Findings of the Study

6.1.1 Majority of the respondents who used e-banking facility was in the age group of 30-40 years

6.1.2 Majority of the respondents used e-banking facility for account transfer, bill payment, sales and purchases, update of savings account and online bank statement status.

6.1.3 Respondents followed basic safety measures while e-banking

6.1.4 Online safety measures are not followed by majority of the respondents as they are not aware of them.

6.1.5 Offline safety measures are followed by the respondents to some extent

6.1.6 Overall safety measures followed by the respondents while e-banking is very low

6.1.7 Majority of the respondents are not aware of the frauds in e-banking and the security available to control internet threats and challenges.

6.2 Suggestions for Respondents While E-Banking

To improve the security online, one must follow the following precautions:

General Safety Precautions

6.2.1Before banking online

- Make sure your computer has up-to-date anti-virus software and a firewall installed
- Install anti-spyware software on your machine
- Download the latest security updates, known as patches for your browser and your operating system. Set your computer to automatically download these updates if possible
- Ensure your browser is set at its highest level of security notification and monitoring. The safety options are no always activated by default
- Keep your passwords and PINs secret- do not write them down or tell anyone what they are.

6.2.2 Whilst banking online

- Be aware of unsolicited e-mails or phone calls asking you to disclose any personal details or passwords. Your bank or the police would never contact you o ask you to disclose your PIN or your online banking password
- Always access your internet banking site by typing the bank's address into web browser
- Never go to a website from a link in an e-mail and then enter personal details
- The login pages of bank websites are secured through an encryption process, so ensure that there is a locked padlock or unbroken key symbol in your browser window when accessing your bank site. The beginning of the bank's internet address will change from 'http' to 'https' when a secure connection is established.
- Never leave your computer unattended when logged in to your online account
- When making a payment, always double check that you have entered the correct account number and sort code – if you enter incorrect details the payment will go to a different recipient and it may prove difficult to get the money back.

6.2.3 When you have finished banking online

- Ensure you log off from your online bank account before you shut down, especially if you are accessing your online bank account from a public computer or at an internet café
- Check your bank statements regularly and thoroughly. If you notice anything irregular on your account, contact your bank as soon as possible.

6.2.4 Shopping online securely

To minimize the chances of becoming a victim of fraud while shopping online, one should:

- Be aware that your card details are as valuable as cash in the wrong hands so store your cards securely at all times and try not to let them out of your site
- Sign up to " Verify by visa" or "MasterCard Secure Code" whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up, your card will have an additional level of security that will help prevent you from being a victim of online fraud.
- Only shop on secure sites. Before submitting card details, ensure that the locked padlock or unbroken key symbol is showing in your browser. (The locked padlock symbol is usually found at the top of the screen if you use Internet Explorer 7 or Firefox 2). The beginning of the online retailer's internet address will change from 'http' or 'https' when a connection is secure. In some new browsers such as Internet Explorer 7 and Firefox 2, the address bar may also turn green to indicate that a site has an additional level of security.
- Never disclose your PIN to anyone and never send it over the Internet.
- Print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number). There may be additional charges such as local taxes and postage, particularly if you are purchasing from abroad. When buying from overseas remember that it may be difficult to roll back if problems arise, but having all the aforementioned information will help your card company take up your case if you subsequently have any difficulties.
- Ensure you are fully aware of any payment commitments you are entering into, including whether you are authorizing a single payment or a series of payments.
- Consider using a separate credit card specifically for online transactions.

VII. Conclusion

E-banking has become a must for people's daily life due to its ease of access and transaction processing in a timely manner. However, many individuals or organizations are not vigilant enough and do not take appropriate safety precautions whilst online. Consequently, this leads to fraudsters capturing their personal information and performing all sorts of fraudulent transactions on the internet. For this reason, users of e-banking should ensure that they follow secure principles when giving away or accessing sensitive information.

References

[1] Akinci, S., Aksoy, S. and Atılgan, E. (2004), Adoption of internet banking among sophisticated consumer segments in an advanced developing country, International Journal of Bank Marketing, Vol.22 (3), pp. 212-32.
[2] Aladwani, M. Adel (2001), Online banking: a field study of drivers, development challenges, and expectations, International Journal of Information Management, pp. 213-225.
[3] Amato-McCoy, D. (2005), Creating virtual value, Bank Systems and Technology, 1(22).
[4] Asher, J. (1999), Small business: Suddenly everyone wants a piece of it, American Bankers Association. ABA Journal, 91, (4).
[5] Barnes, J.G., Howlett, D. M. (1998), Predictors of equity in relationships between financial services providers and retail customers, International Journal of Bank Marketing, Vol.16,pp.15-23.

[6] Bauer, H.H., Hammerschmidt, M. and Falk, T. (2005), Measuring the quality of e-banking portals, International Journal of Bank Marketing, Vol. 23, No. 2, pp. 153-75.
[7] Black, N.J., Lockett, A., Winklhofer, H. and Ennew, C. (2001), The adoption of internet financial services: a qualitative study, International Journal of Retail & Distribution Management, Vol.29 (8), pp. 390-398.
[8] Calisir F. and Gumussoy, C. A., (2008), Internet banking versus other banking channels: Young consumers‟ view, International Journal of Information Management, Vol.28, pp.215-221.
[9] Centeno, C. (2004), Adoption of Internet services in the Acceding and Candidate Countries, lessons from the Internet banking case, Telematics and Informatics, Vol.21, pp. 293-315.
[10] Chou, D., & Chou, A.Y. (2000), A Guide to the Internet Revolution in Banking, Information Systems Management, Vol.17 (2), pp. 51-57.
[11] Chung, W. and Paynter, J. (2002), An Evaluation of Internet Banking in New Zealand, In Proceedings of 35th Hawaii Conference in System Sciences (HICSS 2002), IEEE Society Press.
[12] Daniel, E. (1999), Provision of electronic banking in the UK and Republic of Ireland, International Journal of Bank Marketing, Vol.17(2), pp. 72-82.
[13] Durkin, M., Jennings, D., Mulholland G. and Worthington, S. (2008), Key influencers and inhibitors on adoption of the Internet for banking, Journal of Retailing and Consumer Services, Vol.15, pp. 348-357.
[14] Eriksson, K., Kerem, K., & Nilsson, D. (2008), The adoption of commercial innovations in the former Central and Eastern European markets. The case of internet banking in Estonia", International Journal of Bank Marketing, Vol.26 (3), pp. 154-69.
[15] Gerrard, P. and Cunningham, J.B. (2003), The Diffusion of internet banking among Singapore consumers, The Journal of Bank Marketing, Vol.21 (1), pp. 16-28.
[16] Gerrard, P., Cunningham, J.B. and Devlin, J.F. (2006), why consumers are not using internet banking: a qualitative study, Journal of Services Marketing, Vol.20 (3), pp. 160-168.
[17] Grabner-Kräuter, S., & Faullant, R. (2008), Consumer acceptance of internet banking: the influence of internet trust, International Journal of bank marketing, Vol.26 (7), pp. 483-504.
[18] Guerrero, M. M., Egea, J. M. O. and Gonzalez, M. V. R. (2007), Application of the latent class regression methodology to the analysis of Internet use for banking transactions in the European Union, Journal of Business Research, Vol.60, pp. 137-145.
[19] Hamlet, C. (2000), Community banks go online, American Bankers Association. ABA Journal, Vol.92 (3).
[20] Howcroft, B., Hamilton, R. and Heder, P. (2002), Consumer attitude and the usage and adoption of home-based banking in the United Kingdom, International Journal of Bank Marketing, Vol.20 (3), pp. 111-121.
[21] Hughes, T. (2001), Market orientation and the response of UK financial services companies to changes in Market conditions as a result e-commerce, International Journal of Bank Marketing, Vol.19 No.6, pp. 222-231.
[22] Ibrahim, E.E., Joseph, M and Ibeh, K.I.N (2006), Customers‟ perception of electronic service delivery in the UK retail banking sector, International Journal of Bank Marketing, Vol. 24, No. 7, pp. 475-493.
[23] IMRB and IMAI (2006), Internet in India- 2006 (Summary Report of I-Cube, 2006), New Delhi: IMRB International (e-technology Group@IMRB).
[24] Kothari.(2007), Banks are now just a Click or SMS away, The Week, Vol.25, No.48, pp. 63-76.