International Journal of Commerce and Economics
www.commercejournal.in
Online ISSN: 2664-7540, Print ISSN: 2664-7532
Received: 22-07-2022, Accepted: 08-08-2022, Published: 24-08-2022
Volume 4, Issue 2, 2022, Page No. 16-22

A comparative study on security and privacy issues in internet banking

Fousiya M P, Sameeha Thayyil
Research Scholar, Department of Commerce and Management Studies, PSMO College, Tirurangadi, Kerala, India

Abstract
The former functions of banks were accepting deposits and lending loans through direct mode. By the introduction of information technology, the entire face of banking transaction has changed. Information Technology has brought drastic change in the day-to-day functioning of banking operations. It not only brings improvements in their internal functioning and daily routine work but also enable them to provide better customer service efficiently and effectively. Online banking, also known as internet banking, e-banking or virtual banking, is one of the revolution happened in the banking due to IT. Online banking is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. According to the recent data of RBI (August 2017) on online banking transaction volume (public banks only), the total online banking transaction has reached at the value of 83 crores. However, it was 143 crores in the month of January 2017. It shows a decreasing trend, even though we expected an increase in online transaction due to the implementation of Demonetization in our country. The main reluctance customers are having while entering into online transaction is the security and privacy issues. This study attends to find out the customer perception towards security maintained by banks in online banking transactions, satisfaction on the measures adopted by their respective banks to ensure their privacy and security. This study tries to make a comparison between the customer perception and satisfaction on securities and privacy measures in public and private sector banks.

Keywords: banking, online banking, security and privacy

Introduction

The introduction of technology has created revolution in the banking industry. Perhaps no other industry has been these much influenced by development in technology. Electronic funds Transfer, Electronic clearings System, Automated Teller Machine (ATM), Corporate banking terminal (CBT), Point of Scale Terminal (POST), Electronic Data Interchange (EDI), Mobile banking and Net banking are the results of revolution in technology. Among these, online banking has been becoming more popular in the last few years. Actually, the usage increased after the demonetization. People feel it's safe to keep their money in bank than in liquid form. Now most of the customers are having either mobile banking or internet banking. FinCen (2000) states that "E-banking is an umbrella term for the process by which customer may perform banking transactions electronically without visiting a brick-and-mortar institution". It is an online payment system that enables the customers to conduct online financial transactions on a website. The e-banking system addresses several emerging trends: customer's demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. This system allows consumers to access their banking accounts, review most recent transactions, request a current statement, view current product information, and reorder checks.

For any idea, there will be two sides, the merits and demerits. In the case of online banking the demerits are much highlighted than the merits. The Commercial Banks in India have been facing lot of problems due to Online Banking Crimes. Because they are dealing with the personal property like personal data and identity, passwords. Here arise the importance of security and privacy in internet banking. The major security issues in internet banking are;

- **Phishing:** Phishing is a kind of scam where the scammers masquerade as a trustworthy source in attempt to gain private data such as PINs, and credit card data, etc. through the internet.
- **Internet frauds:** These attacks are created to make the fraud with private assets of customer directly rather than personal data through false undertakings, assurance tricks and more.
- **Malware:** Malware, mainly spyware, is malicious software camouflaged as legitimate software planned to accumulate and transmit private data, such as PINs, without the customer's consent or knowledge. They are often spread through software, e-mail and files from unofficial places.
- **Identity theft:** Identity theft is a crime in which a fraudster obtains key pieces of personal data, such as bank information, date of birth or driver's license numbers, in order to impersonate somebody. The personal

data exposed is then used criminally to apply for credit, buying goods and services, or gain right of entry to bank accounts.

- **Keystroke capturing/logging:** Keystroke capturing or logging attacks are takes place with the help of software or hardware key logger. Anything that user type on system can be captured and stored in a storage. This actually create a log file of user activities and at a particular instance of a day mail is automatically forwarded to the attacker. This log file contains id and password of different users and attacker can use this for his own purpose. This attack mainly takes place at internet cafes.
- **Pharming:** In Pharming attack fraudster create false website, so that people will visit them by mistake. The main purpose of pharmer is to obtain victims personal information for further frauds.
- **Spyware:** Spyware can enter in any system as hidden components of free programs. They can monitor web usage, keystroke logging and virtual snooping on user's computer activity.
- **Trojan horse/Trojan:** Trojan horse are the most dangerous type of attack in which attacker can directly gain unauthorized access to victims' systems. This virus enters in victim system with the help of different legitimate software. An updated antivirus and firewall can protect any user from this kind of attacks.
- **Virus:** Virus is a computer program that designed to replicate itself from one computer to another. It can slow down user system or corrupt its memory and files. Email and file-sharing facilities are the main reason for spreading viruses.
- **Worm:** This is a malicious program that replicate or reproduce itself until all the storage space on a computer drive will be filled. It uses system time, speed, and space when duplicating. It can also interrupt internet usage.
- **Denial of Service Attacks:** Denial of service attacks are used to overload a server and render it useless. The server is asked repeatedly to perform tasks that require it to use a large number of resources until it can no longer function properly. The attacker will install virus or Trojan software onto an abundance of user PC's and instruct them to perform the attack on a specific server.

Present security system offered by banks

- **User id & Transaction Password:** Here a customer has to register himself with a unique id and password for user verification
- **OTP:** This is an authentication service that makes use of an OTP in addition to the conventional ID and password for personal identification. User can perform authentication by entering an OTP displayed by the mobile phone application in addition to their normal ID and Password. The one-time passwords are specific to each user, and a new password is generated every minute. Even if the password is obtained by a third party fraudulently, it cannot be used outside its lifetime.
- **QRP:** code - QRP that is Quick Response Protocol, is a secure authentication system that uses a two-factor authentication by combining a password and a camera equipped mobile phone, where mobile phone is acting as an authentication token.
- **Biometric:** Biometric is specifically used for secure ATM transaction. In such a transaction, the use of a biometric mechanism such as iris/retinal scan, hand geometry or fingerprint scan can greatly improve overall security.
- **Security Question:** Based on research for multifactor authentication (MFA) and fraud risk mitigation, the verification process was strengthened for Internet Banking users by reducing the number of opportunities to correctly answer security challenge questions. If the user was incapable to answer correctly, the customer was locked out of Internet Banking until customer service unlocked or reset the MFA setting for the user.
- **SMS banking:** Account balance Inquiry, Transaction Inquiry, Cheque status Inquiry, Password Change are the different services provided by SMS banking. To utilize this SMS banking facility user has to enroll himself in his specific branch of bank.

Statement of the problem

Online banking is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. According to the data of RBI (August 2017) on online banking transaction volume (public banks only), the total online banking transaction has reached at the value of 83 crores. However, it was 143 crores in the month of January 2017. It shows a decreasing trend, even though we expected an increase in online transaction due to the implementation of Demonetization in our country. The main reluctance customers are having while entering into online transaction is the security and privacy issues. This study attends to find out the customer perception towards security maintained by banks in online banking transactions, satisfaction on the measures adopted by their respective banks to ensure their privacy and security.

This study tries to make a comparison between the customer perception and satisfaction on securities and privacy measures in public and private sector banks.

Objectives

1. To identify major concerns the customers are having in connection with the security and privacy in internet banking.
2. To analyze the customer satisfaction on the measures adopted by their respective banks.
3. To compare the level of security adopted by private and public sector banks.

Research methodology

The study is Descriptive in nature. Data is collected from primary sources and it consists of 50 respondents in Malappuram district who have adopted Internet banking facility of public sector and private sector banks. For this purpose, Convenience Sampling, method is adopted. A questionnaire is designed consisting of 8 Variables for exploring the concerns or issues in internet banking and 12 variables for measuring the satisfaction on the measures adopted.

Hypotheses

H1: There is significant difference in the perception towards issues in online banking among public and private sector bank customers.

H2: There is significant difference in the customer satisfaction on various measures adopted for internet security facility among public and private sector bank customers.

Analysis and interpretation

Table 1: Analysis of sample demographics

Variables	category	Frequency	Percentage
Type of Bank	Public sector	34	68
	Private sector	16	32
Gender	Male	19	38
	female	31	62
Monthly income	Below 10000	8	16
	10001-20000	10	20
	20001-30000	6	12
	30001-40000	17	34
	40001-50000	2	4
	40001-50000	7	14
Education	Plus two	2	4
	diploma	2	4
	UG	27	54
	Professional degree	19	38
Frequency of using	Once in a month	7	14
	Once in a quarter	5	10
	Twice in a week	12	24
	Once in a week	6	12
	More than once in a week	20	40
Awareness password	Not at all	2	4
	Partially	11	22
	Fully	37	74
Awareness _OTP	Not at all	2	4
	Partially	6	12
	Fully	42	84
Awareness HTTPS	Not at all	9	18
	Partially	26	52
	Fully	15	30
Awareness virtual keyboard	Not at all	8	16
	Partially	16	32
	Fully	26	52
Password strength	Very weak	1	2
	Weak	1	2
	neutral	9	18
	strong	22	44
	Very strong	17	34

Frequency of using virtual keyboard	never	13	26
	Occasionally	13	26
	sometimes	17	34
	frequently	5	10
	every time	2	4

Source: primary data

Among the respondents, 68% includes customers of public sector bank and 32% includes customers of private sector banks. Majority of the respondents fall under 30000-40000 income category. 40 percentage of respondents use internet banking more than once in a weekend. Respondents are having full awareness about password, OTP and virtual keyboard where as partial awareness about HTTPS. Most of the respondents are having a strong password. The usage of virtual keyboard is less.

Table 2: Descriptive statistics for concerns in security and privacy in internet banking

Variables	Mean	Std. Deviation
Fear of stealing password	3.3800	1.12286
Fear of transferring money from my account to another fraudulently	3.2600	1.13946
providing internet banking password at fake websites by mistake	2.6200	1.21033
others can easily monitor transaction history	2.8200	1.22374
reluctance from bank to refund money, if online frauds happen	3.4200	1.19676
sharing of account related information with third party	2.4600	1.09190
Sharing of online behaviour with third party.	2.8200	1.15511
vulnerable to fraud	3.4200	1.1444

Source: primary data

The above table depicts the mean and std. Deviation of all the variables in security and privacy issues in internet banking. Customers are having a big concern about the reluctance from the part of the bank, when an online fraud occurs and vulnerable to fraud with a mean value 3.42. For almost all the statements, their agreement level is high. Customers are having a negative to neutral opinion regarding providing internet banking password at fake websites by mistake, others can easily monitor transaction history, sharing of account related information with third party and sharing of online behavior with third party.

Table 3: Descriptive statistics for satisfaction with internet banking

Variable	Mean	Std. Deviation
Safe to use internet banking of my bank.	4.0600	.73983
virtual keyboard to enter Password and User ID	3.9400	.79308
guidelines in bank's homepage regarding the security measures	4.0000	.94761
OTP(One Time Password) is required, if logging from different browsers/computers	4.0800	1.10361
OTP for Third Party payments	4.3200	.84370
OTP for adding beneficiary	4.0400	1.00934
pressing back will immediately results in logging out from the session	3.7800	.97499
When my account stays idle for long time, automatically log off.	4.1200	.96129
entering wrong password more than 3 times lead to logging off	3.9000	.99488
Bank insist to create strong password for internet banking	4.4600	.78792
Remind me to change password from time to time.	3.8800	1.08119
Overall, I am satisfied with my bank's security features	4.1000	.58029

Source: primary data

Customer satisfaction with the internet banking facility provided by the banks can be interpreted with the above table. They have strong agreement with bank's insistence on creating new password frequently. From the table it can be concluded that banks are providing strong security and privacy features since all the statements are having a men value above 3.5.

Checking assumptions
Normality

Table 4: Normality result-Shapiro wilk test

	Statistic	Sig.
Mean concern	.977	.418
Mean satisfaction	.962	.103
Mean awareness	.876	.000

Frequency of using internet banking	.833	.000
Frequency of using virtual keyboard	.889	.000
Password strength	.823	.000

H0: data is normal.
H1: data is not normal

Since the p value (.418, .103) is greater than level of significance (.05) for concern and satisfaction respectively, it can be concluded that the null hypothesis is accepted and the data is normal. Whereas in the case of awareness about internet banking key terms, frequency of using internet banking, Frequency of using virtual keyboard and Password strength, the data is not normal because the p value is <.05.

Homogeneity of variance

In order to perform one way ANOVA and Independent sample t test, the variances between groups must be homogeneous. So levene's test of variance has been performed. For groups lacking homogeneity, non-parametric test has been performed.

Table 5: Test result on privacy and security issues in internet banking

Hypotheses	Test	P Value	Accept/Reject
H0: there is no significant difference between public and private sector banks in the customer perception towards security and privacy issues	T test	0.027	Reject
H0: there is no is no significant difference between male and female customers in the customer perception towards security and privacy issues	T test	0.652	Accept
H0: There is no significant relationship between age and customer perception towards security issues	Kendall's correlation test	0.352	accept
H0: there is no is no significant difference between various income people in the perception towards security and privacy issues	One way ANOVA	0.245	Accept
H0: there is no is no significant difference between education level of people in the perception towards security and privacy issues	One way ANOVA	0.656	Accept
H0: There is no significant relationship between frequency of using internet banking and customer perception towards security issues	Kendall's correlation test	0.056	Accept
H0: There is no significant relationship between password strength and customer perception towards security issues	Kendall's correlation test	0.033	Reject
H0: There is no significant relationship between frequency of using virtual keyboard and customer perception towards security issues	Kendall's correlation test	0.047	Reject
H0: There is no significant relationship between awareness about key terms in internet banking and customer perception towards security issues	Kendall's correlation test	0.161	Accept

Source: primary data

The above table shows the test result on security and privacy issues in internet banking.
Two out of nine hypotheses have been rejected. Those show the difference.

- There is significant difference between public and private sector banks in the customer perception towards security and privacy issues. In order to know the difference, we need to check the mean value of both banks.
- Mean value public sector bank: 2.87
- Mean value private sector bank: 3.33
- From the mean value, it can be understood that customers of private sector bank are having big concern than customers in public sector banks.
- There is significant relationship between password strength and customer perception towards security issues. The correlation coefficient is -0.239121 which indicates that there is an inverse relationship between password strength and customer perception towards security issues.
- There is significant relationship between frequency of using virtual keyboard and customer perception towards security issues. since the correlation coefficient is -0.217171, it can be concluded that there is negative relation between frequency of using virtual keyboard and customer perception towards security issues

Table 6: Test result on satisfaction with internet banking

Hypotheses	test	P value	Accept/reject
H0: there is no significant difference between public and private sector bank customers in the satisfaction with internet banking of theirs	T test	0.396	Accept
H0: there is no is no significant difference between male and female customers in the satisfaction with internet banking of theirs	T test	.024	Reject
H0: There is no significant relationship between respondent's age and satisfaction with internet banking of theirs	Kendall's correlation test	0.152	Accept
H0: there is no is no significant difference between various income people customers in the satisfaction with internet banking of theirs	One way ANOVA	0.514	Accept
H0: there is no is no significant difference between education level of people in the satisfaction with internet banking of theirs	One way ANOVA	0.705	Accept
H0: There is no significant relationship between frequency of using virtual keyboard and customer satisfaction with internet banking	Kendall's correlation test	.085	Accept
H0: There is no significant relationship between awareness about key terms in internet banking and customer satisfaction with internet banking	Kendall's correlation test	.010	Reject
H0: There is no significant relationship between frequency of using internet banking and customer satisfaction with internet banking	Kendall's correlation test	.250	Accept

Source: primary data

Eight hypotheses have been accepted while two hypotheses have been rejected.

- There is significant difference between male and female customers in the satisfaction with internet banking of theirs.
- Mean value for male: 4.24
- Mean value for female: 3.94

According to the mean value, we can say that the female is having less satisfaction compared to male.

- There is significant relationship between awareness about key terms in internet banking and customer satisfaction with internet banking. The relation is positive as the correlation coefficient is 0.278663.

Findings

1. Majority of the Customers are fully aware about password, OTP and virtual keyboard whereas partially aware about HTTPS.
2. Most of the respondents are having a strong password.
3. More than once in a week, most of them uses internet banking
4. The usage of virtual keyboard is less.
5. Respondents are having big concern about bank's reluctance to refund money in case of any fraud. They are not sure whether, they will get it refunded or not.
6. Almost all the customers are satisfied in the security maintained by their respective bank.
7. The customers of private sector banks are having big concern than customers in public sector banks.
8. There is inverse relationship between password strength and customer perception towards security issues.
9. there is negative relation between frequency of using virtual keyboard and customer perception towards security issues
10. Female are having less satisfaction compared to male.
11. Relationship between awareness about key terms in internet banking and customer satisfaction with internet banking are positive.

Conclusion

Internet banking is actually a boon to the industry of banking, because electronic banking (e-banking) is offering its customers with a wide range of services. Customers are now able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions. Today electronic banking can be termed as a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard. Most research studies have indicated that the common problem affecting information security and privacy of customers is e-services provider's lack of security control, which allows damaging privacy losses.

This paper also says proves this statement. The major issue faced by them is the responsibility and accountability from the part of the banks. They agree that internet banking is vulnerable to frauds. However, they are afraid whether their bank will refund the money in case of any fraud.

This has to be changed. The banks must prove that they are with them for any help. The banks should ensure the safety of their money

Suggestions

1. Private banks must focus more on the security and privacy issues in internet banking.
2. Banks must encourage their customers to use virtual keyboard.
3. Banks should provide awareness about https in internet banking
4. Customers should ensure that they are using secure version of the site by looking at https.
5. Banks should create an atmosphere of faith in customers that bank is responsible for third party intervention. They should take quick action when such an issue is reported and try refund the amount as early as possible.

References

1. Reynolds OM. [Review of PRIVACY AND FREEDOM, by A. F. Westin]. Administrative Law Review,1969:22(1):101-106. http://www.jstor.org/stable/40708684
2. Albrechtsen E. A qualitative study of users' view on information security. Comput. Secur,2007:26:276-289.
3. Cheung CM, Lee M. Understanding consumer trust in Internet shopping: A multidisciplinary approach. J. Assoc. Inf. Sci. Technol,2006:57:479-492.
4. Debar H, Viinikka J. Security information management as an outsourced service. Computer Security,2006:14(5):416-434.
5. Dhillon G. Challenges in managing information security in the new millennium. In: G. Dhillon (ed.) Information Security Management: Global Challenges in the New Millennium. Hershey, PA: Idea Group Publishing, 2001, 1-8.
6. Dhillon G, Torkzadeh G. Values-focused assessment of information system security in organizations. Information Systems Journal,2006:16(3):293-314.
7. Belanger F, Hiller JS, Smith WJ. ("Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes" Journal of Strategic Information Systems,2002:11:245-270.
8. Leach J. Improving user security behavior. Computers and Security,2003:22(8):685-692.
9. Malhotra NK, Kim SS, Agarwal J, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model" Information Systems Research,2004:15(4):336-355.
10. Nolan J, Best practices for establishing an effective workplace policy for acceptable computer usage. Information Systems Control Journal,2005:6(2):32-35.