Online Banking Operating Pattern and Risk of Cyber Fraud - Findings from Empirical Research

Dr. Heena Thanki
Assistant Professor,
Shri Jairambhai Patel Institute of Business Management,Gandhinagar, Gujarat

Dr. Shankrrao Junare
Professor and Dean,
Faculty of Management, (IFS) and Director
(Training) Gujarat Forensic Sciences University
Gujarat - INDIA

Abstract

"Online-banking or Internet-banking is used for a new age banking system with the internet technology as a delivery channel to conduct banking activities." Singhal & Padhmanabhan, 2008. According to IBEF report on banking "Around 44% people are using Net banking, which remains the most favorite mode of payment among internet users in India[1],"According to an India Spend analysis of the data of Reserve Bank of India, reports that mobile banking transaction has increased by 175% and money transfer using mobile banking has grown by 369% by 2016.(if compare it with the October 2015 data[2].)

The increased penetration of internet and usage of mobile-smart phones and tablets for online banking and other financial transactions have increased risks and alarming situation for security issue in India.[3] In past 10 years (2005 to 2014), cyber crime (reported) has increased 19 times from 481 in 2005 to 9,622 in 2014.

In this present study an attempt has been made to understand the usage and operating pattern of the online banking services and security threat associated with it.

Key words: online banking, Security, CSA,CBA, Phishing

Introduction

"Online-banking or Internet-banking is used for a new age banking system with the internet technology as a delivery channel to conduct banking activities." Singhal & Padhmanabhan, 2008. Online banking, also referred as internet banking /e-banking /virtual banking, is an electronic payment arrangement that facilitate clients of a bank to conduct a variety of financial transactions through the financial institution's website. Online banking system enables the customer to manage their financial transaction like bill payment, account statement generation, fund transfer, upgrading and linking their personal information etc. from anywhere using their online banking facility. by adopting the online banking facility many tedious and time consuming banking task can be done by a touch of finger, online banking has revolutionaries the banking industries and the way people were performing their banking task.

Internet Users in India

Table 1: Internet Users in India

Year	Internet Users	Penetration (% of Pop)	Total Population	1Y User Change	1Y User Change	Population Change
2016*	**462,124,989**	34.80%	1,326,801,576	30.50%	108,010,242	1.20%
2015*	**354,114,747**	27%	1,311,050,527	51.90%	120,962,270	1.22%
2014	**233,152,478**	18%	1,295,291,543	20.70%	39,948,148	1.23%
2013	**193,204,330**	15.10%	1,279,498,874	21.50%	34,243,984	1.26%
2012	**158,960,346**	12.60%	1,263,589,639	26.50%	33,342,533	1.29%
2011	**125,617,813**	10.10%	1,247,446,011	36.10%	33,293,976	1.34%
2010	**92,323,838**	7.50%	1,230,984,504	48.50%	30,157,710	1.38%

Source: http://www.internetlivestats.com/internet-users/india/

From the above data we can see that there has been 400% increase in internet users in India since 2010, by the end of 2016 the penetration of internet in India is 34% of the total population. (here internet users, refers to the "individual who can access to the Internet at their home, via any device and connection"[4].) so the actual penetration and if we add up the data for people who have accessed to internet over their work place/school college etc..the percentage can even go higher. According to Telecom Ministry 730 million internet users are anticipated in the country by 2020[5]. Indian government mission of Digitization has led to massive growth rate in internet users in India.

According to IBEF report on banking "Around 44% people are using Net banking, which remains the most favorite mode of payment among internet users in India[6],"According to an India Spend analysis of the data of Reserve Bank of India, reports that mobile banking transaction has increased by 175% and money transfer using mobile banking has grown by 369% by 2016.(if compare it with the October 2015 data[7].) With the ongoing digital drive in India and after demonetization baking industry has face a revolutionary change in the way of its operation, According to the report of Facebook and BCG group, the number of users opting for online banking is anticipated to reach 150 million by 2020, from the current 45 million active urban online banking users in India[8].

The increased penetration of internet and usage of mobile-smartphones and tablets for online banking and other financial transactions have increased risks and alarming situation for security issue in India[9]. In past 10 years (2005 to 2014), cyber crime (reported) has increased 19 times from 481 in 2005 to 9,622 in 2014. India is now ranked third as a source of "malicious activity" on the Internet after the US and China, and second as a source of "malicious code"[10]. As indicated by the Indian Computer Emergency Response Team (CERT-In), 27,482 instances of cybercrime were accounted for from January to June 2017. These incorporate phishing, defacements, virus or malicious code, scanning or probing etc[11].

Online Banking Fraud is an extortion or robbery conferred utilizing on the online technology to illicitly expel cash from a financial balance as well as exchange cash to a record in an alternate bank.

The secrecy, protection and security of online banking transaction and individual data are the significant worries for both the banking industry and customers of that. Assaults on internet banking today depend on misleading the client to take login information. Phishing, Cross-website scripting, adware, malware, spyware, Trojans and viruses are currently the most familiar internet banking security threats and risks. Because of some lack of sensation or senseless slip-ups the confidential data can be stilled without much of a stretch.

Literature Review

According to Kalakota & Whinston (1997), "Security in e-commerce is defined as a threat that creates the 'circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, fraud, and abuse"

online banking crime or fraud is generally operated through any of the three modus operandi, credential stealing attack(CSA), man-in-the browser(man in the middle), or channel breaking attack(CBA)(Khrais,2015[12]).

Credential stealing attack (CSA)

CSA, where fraudsters endeavor to hoard users' credentials, either with the utilization of malicious software or through phishing[13]. (Khrais,2015).

Phishing, A person's personal credential information are acquired by criminals posing as bankers, who hang a site similar to that of the person's banking website. They request to provide all personal information such as account number, user id, and passwords on the excuse of database up gradation. The credential information about the id and password are then used to carry out communication on their behalf without their knowledge. Normally, a phishing email will ask an internet banking client to follow a link in order to catch individuals' personal and financial information. If the link is followed, the target downloads a program which catches his or her keeping money login subtle elements and sends them to an outsider. Phishing employs social engineering and subterfuge techniques to steal consumers' personal identity and financial account credentials (Anti-Phishing Working Group, 2007). It also refers to an act of an Internet swindler who uses e-mails to lure Internet users by asking for password and financial data.

Malicious software, According to Vinod, Laxmi, & Gaur (2009) "Malware is a term for any malicious software which enters system without user or system authorization". "It can also be defined as software that is harmful to other software and possibly and indirectly control other hardware by (affected) driver application" (Kramer & Bradfield, 2010).

Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, Trojans, spyware, adware and root kits, etc., The harm done can differ from something slight as changing the creator's name on an archive to full control of your machine without your capacity to effectively discover.

Man-in-the browser (man in the middle) attack

It happens in the application layer between the client and the browser. The opponent is approved with privileges to read, write, change and erase browser's information while the client is ignorant about it.(Khrais,2015[14]). In view of Callegati, Cerroni, & Ramilli, (2009) "Man-in-the-middle (MITM) attacks occur when an attacker acts as a gateway in the traffic stream and compromises the connection between clients and legitimate servers."

Channel breaking attack (CBA)

it includes blocking the correspondence between the customer side and banking server, by taking on the masquerading of the server to the customer and the other way around(Khrais,2015[15]).

Majority types of Online Attacks

- Trojan attacks/ Spyware attack:
- Malicious hackers:
- Phishing
- sniffers or network monitors
- Malicious software

The Security Models and Measures by banks

From the dangers above, it is evident that there is a dire need of effective and efficient security models by banks. online banking transactions are carried out in the verity of environment and always are in the target of the criminals. Hence bank should must secure the end clients online banking with a multi-faceted security arrangements that recognizes every movement of hacking and assembling every technology that can guarantee security of clients data and credentials. Online banking companies are continuously improving their security measures to protect the interest of their client. Few security measures taken by banks are

- One-time password (OTP) tokens
- Browser protection
- Device register
- CAPTCHA
- Short message service (SMS)
- Device identification
- Pass-phrase
- Positive identification

Research Objective

- To identify the reason for using online banking.
- To identify the usage and operating patterns of online banking
- To know whether the proper security protection are adopted by online banking users or not.

Research methodology

Present study follows cross sectional descriptive research design. Structured questionnaire was prepared containing demographic information of the respondents and various question to identify the usage pattern of online banking and related to security checks used by users to prohibit banking fraud. The questionnaire then was administered via personal contact and Google form method, 200 was the targeted sample size but, because of non response and incomplete data the final sample size was considered to be 158.

Analysis and Discussion

Table 2: Demographic characteristics of the sample

	Frequency	Percent
Gender		
Male	106	67
Female	52	33
Total	**158**	**100**
Marital Status		
Married	96	61
Single	62	39
Total	**158**	**100**
Age		
Up to 25	42	27
26-45	97	61
46-60	16	10
Above 60	3	2
Total	**158**	100
Education		
SSC or less than SSC	4	3
HSC	16	10
Graduate	76	48
Post- Graduate	62	39
Total	**158**	100
Occupation		
Govt. Employee	44	28
Employed with Pvt. sector	62	39
Self-Employed	16	10
House wife	3	2
Retired	5	3
Student	28	18
Total	**158**	100
Income		
Up to 15,000	41	26
15,001 – 30,000	60	38
30,001 – 50,000	32	20
50001 – 75,000	17	11
75001-100000	5	3
100000 and above	3	2
Total	**158**	100

The above table shows the Demographic characteristics of the selected sample, 67 percent of the sample is represented by male gender, 61 percent of selected sample was from the married group,61 percent of the selected sample was from age group 26-45, 48 percent of the selected sample holds degree up to graduation,39 percent of the sample represented by private sector employees. 38 percent sample belongs to the income category of the 15001 to 30000.

Reason for using online banking

To get an idea about what has forced customer to adopt online banking, they have asked to select the reason for using online banking,

Table 3 : Reason for using online banking

	Response	Percent
Avoid waiting in a queue	138	87
Reduce time spent commuting	108	68
Easy and prompt transaction using online banking	153	97
Availability of banking on Sunday and public holiday	103	65
No extra charges	56	35

97 percent of the selected samples agree that they use online banking because it is easy and prompt, while 87 percent are of the opinion that with the use of online banking they can save on time waiting in queue.

Most used online bank

To get a view about the mostly used bank for online banking facility they were asked to select the bank they were using for online banking, and asked to select more than one if they are using more than one bank. And the most used banks for online banking were following

Table 4 : Most used online bank

	Response	**Percent**
Bank of Baroda	37	23
State Bank of India	96	61
Axis Bank	39	25
HDFC Bank	24	15
ICICI Bank	20	13
Kotak Mahindra Bank	10	6

Frequency of using online banking facility

Table 5: Frequency of using online banking facility

	Frequency	Percent		Frequency	Percent
None or rarely	18	11	6-10 times	30	19
1 or 2 times	28	18	11-20 times	19	12
3-5 times	55	35	More than 20	8	5

From the above table it is clear that 35 % of the users uses online banking only 3-5 times a month and only 17 % of the People(12+5) uses online banking services more than 10 times a month.

Reason for choosing particular bank for their online banking services

Table 6: Reason for choosing particular bank for their online banking services

	Frequency	Percent
I have a traditional bank account with the same bank	62	39
The brand name of the bank	36	23
The excellent online banking service offered by this bank	30	19
The security protection offered by bank for online banking	30	19

From the above table it can be seen that 39 percent of the users have selected the bank because it was the bank in which they were having their traditional account. While only 19 percent says that they have selected particular bank because of the security protection offered by that bank.

Purpose for using online banking

Table 7: Purpose for using online banking

	Response	Percent
Balance Inquiry,	140	89
Account Statement	133	84
Fund Transfer	61	39
Bill Payment	103	65

From the above table it is clear that though there is much facility of instant payment and, NEFT, RTGS , online bill payment is available not all the users are availing that services, only 39 percent of the users are using facility of fund transfer where as 65 percent are using online banking for the bill payment.

Access point of online banking

Table 8: Access point of online banking

	Frequency	Percent
My house	17	11
My friend's house	3	2
My workplace	36	23
Public place	3	1
Mobile phone	85	54
Laptop	14	9

From the table it is clear that majority 54 percent of the users are using online banking facility via their mobile, where as 23 percent use online banking at their work places.

Security protection

To get a view about whether any kind of security protection instruments are used by online banking users they were asked some question like, use of antivirus software, firewall protection, popup blocker etc.

Table 9: Security protection

	Frequency of Yes	Percent
I have installed firewall application	55	35
I have installed licensed version anti-virus software	77	49
I have installed anti-spyware/ adware/ Trojan/backdoor	44	28
I have installed popup windows blocker	62	39
I update operating system is regularly for all securities update in my Computer/Mobile	47	30
I read the terms and condition s of the software / application for which type of permission they ask for before downloading and installing the app/ software	33	21

From the above table it is clear that only 35 percents of the users have installed firewall application. 49 percent of the users uses licensed version of the antivirus software. Only 28 percent of the users installed anti-spyware/ adware/ Trojan/backdoor. Only 21percent says that they read terms and condition before installing any software or application.

Security updation

Just using the security protection is not enough for protection against the online theft they need to be regularly updated to better protect your system and personal data.

Table 10: Security updation

	Frequency	Percent
Once a day	3	2
Once a week	7	4
Once a month	17	11
Whenever I get time	36	23
Auto update	60	38
I don't use security protection	35	22

From the table it can be seen that 22 percent of the users don't use any kind of security protection and only few percent of the people upgrade on daily to weekly basis.

Password protection

Table 11: Password Protection

	Frequency	Percent
Very frequently (after every few days or after few transaction)	10	6
Every month	16	10
Every 3 months	19	12
Every 6 months	9	6
Once a year	38	24
Whenever my password expires	66	42

It is advisable to frequently change the password of online banking for better protection but the above data revels that only 6 percent of the users frequently changes the password. Majority of the users (42 %) says that they changes the password when the old password expires.

Findings

From the analysis of the data following findings it can be drawn

- Easy and prompt services and availability of the banking facility on public holidays Sundays are the reason for adoption of the online banking
- Majority of the users uses the online banking facility only 3-5 times a month.
- Users have not selected or change the bank because of the security reasons, majority of the users are using the same banks' online banking where they were having their traditional banking account.
- Online banking facilities are not used to the fullest capacity as majority uses it for the balance checking and account statement purpose.
- Majority of the users operate online banking facility via mobile.
- The usage of security protection system to prevent the frauds is disappointing as Only 35% have installed the firewall protection in their system, 51% are using systems without virus protection, only 28% users

have installed Trojan and spyware blocker, and only 21% reads the term and condition before installing any software and application in their system.

Users shows lazy attitude for he password security also,42 percent conforms that they change password only when it is required by the system or password expires.

Conclusion

Use of online banking is advantageous in numerous manners, as it saves time waiting in queue, commuting time, and you can perform your transaction 24*7 and even on holidays also, accepting the online banking is a need of time and digitization era, and by accepting the online banking, the risk of online baking is also accepted. However banking companies are trying hard to offer the best security measure to protect their client information, but few step clients also can take which can reduced the risk of fraud.

From the above discussion and findings it can conclude that to better protect the online banking transaction and to keep the criminal at their bay following few steps can be adopted by the users of the online banking.

Keep your device protected by Install licensed anti-virus software, anti-spyware security software , firewalls etc.

Keep your operating system and internet browser up to date, and download the entire security patch[16].

Always get to Online Banking website just by writing the URL in the address bar of your program.

Never endeavor to get to Online Banking via an external link of unknown or suspicious origin appearing on other websites, search engines or e-mails.

Before logging in the website, check for the Bank's Security details (e.g. green address line and Lock, HTTPs) that verify that you are visiting the secure pages of Bank[17].

Ignore and erase instantly suspicious fake (phishing, parody, trick) messages that give off an impression of being from Bank, asking you to urgently click a connection to a false (spoof) site that tries to imitate the Bank's site and to draw you into giving out your identity, (PIN, record or card numbers, individual recognizable proof data et al.) bring in the notice of bank and complain for the same.

Avoid using Online Banking from public shared PCs (as in internet cafes, libraries, etc.) to avoid the risk of having your sensitive private information copied and abused.

Use Virtual Key board.

Use secured network only, do not use free Wi-Fi for online transaction.

Sign-on to Online Banking frequently and monitor your account transactions,

Maintain and check track of your last log-on date and time.

Contact your bank promptly in case of any emergencies, or you notice any phishing activity[18].

Reference

Anti-Phishing Working Group. (2007). Phishing Activity Trends Report for the Month of December, 2007. Retrieved from https://docs.apwg.org/reports /apwg_report _jan_2008.pdf

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to theHTTPS protocol. IEEE Security and Privacy, 7(1), 78-81.

http://indianexpress.com/article/technology/technology-others/cyber-crimes-in-india-likely-to-double-in-2015/

http://indianexpress.com/article/technology/technology-others/cyber-crimes-in-india-likely-to-double-in-2015/

http://indiatoday.intoday.in/story/digital-india-internet-users/1/913797.html

http://infosecawareness.in/secure-online-banking

http://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

http://www.business-standard.com/article/economy-policy/post-demonetisation-digital-payments-are-down-15-116122700098_1.html

http://www.business-standard.com/article/economy-policy/post-demonetisation-digital-payments-are-down-15-116122700098_1.html

http://www.financialexpress.com/industry/banking-finance/online-banking-users-in-india-to-reach-150-billion-by-2020-according-to-a-study/731048/

http://www.icommercecentral.com/open-access/highlighting-the-vulnerabilities-of-online-banking-system.php?aid=61518

http://www.internetlivestats.com/internet-users/india/

http://www.worldjute.com/ebank1.html(asses on 08/09/2017)

https://en.wikipedia.org/wiki/Online_banking

https://en.wikipedia.org/wiki/Online_banking https://in.norton.com/cybercrime-trojansspyware

https://www.ibef.org/download/Banking-February-2017.pdf

https://www.ibef.org/download/Banking-February-2017.pdf

https://www.techopedia.com/definition/4015/malicious-software-malware

https://www.youthkiawaaz.com/2016/06/cyber-crime-rate-in-india/

Kalakota, R., & Whinston, A. B. (1997). Electronic commerce: a manager's guide. Addison Wesley Professional.

Khrais LT (2015) Highlighting the Vulnerabilities of Online Banking System. J Internet Bank Commer 20:120 assessed from http://www.icommercecentral.com/open-access/highlighting-the-vulnerabilities-of-online-banking-system.php?aid=61518

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. Journal in Computer Virology, 6(2), 105-114.

Singhal, D., & Padhmanabhan, V. (2008). A Study on Customer Perception TowardsInternet Banking: Identifying Major Contributing Factors. Journal of Nepalese Business Studies, 5(1), 101-111.

Singhal, D., & Padhmanabhan, V. (2008). A Study on Customer Perception Towards Internet Banking: Identifying Major Contributing Factors. Journal of Nepalese Business Studies, 5(1), 101-111.

Utakrit, N. (2012). Security awareness by online banking users in Western Australian of phishing attacks. Retrieved from http://ro.ecu.edu.au/theses/503

Vinod, P., Laxmi, V., & Gaur, M. S. (2009). Survey on Malware Detection Methods.Proceedings of the Thrid Hackers' Workshop on Computer and Internet Security(pp.74-79). Kanpur, UP, India: Indian Institute of Technology (IIT).

Endnotes:

1. https://www.ibef.org/download/Banking-February-2017.pdf

2. http://www.business-standard.com/article/economy-policy/post-demonetisation-digital-payments-are-down-15-116122700098_1.html

3 . http://indianexpress.com/article/technology/technology-others/cyber-crimes-in-india-likely-to-double-in-2015/

4. http://www.internetlivestats.com/internet-users/india/

5. http://indiatoday.intoday.in/story/digital-india-internet-users/1/913797.html

6. https://www.ibef.org/download/Banking-February-2017.pdf

7. http://www.business-standard.com/article/economy-policy/post-demonetisation-digital-payments-are-down-15-116122700098_1.html

8. http://www.financialexpress.com/industry/banking-finance/online-banking-users-in-india-to-reach-150-billion-by-2020-according-to-a-study/731048/

9 . http://indianexpress.com/article/technology/technology-others/cyber-crimes-in-india-likely-to-double-in-2015/

10. https://www.youthkiawaaz.com/2016/06/cyber-crime-rate-in-india/

11. http://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

12. http://infosecawareness.in/secure-online-banking

13. http://infosecawareness.in/secure-online-banking

14. http://infosecawareness.in/secure-online-banking

15. http://infosecawareness.in/secure-online-banking

16. http://infosecawareness.in/secure-online-banking

17. http://infosecawareness.in/secure-online-banking

18. http://infosecawareness.in/secure-online-banking