Scholarly Research Journal for Humanity Science & English Language, Online ISSN 2348-3083, SJ IMPACT FACTOR 2021: 7.278,
http://www.srjis.com/issues_data?issueId=215
PEER REVIEWED & REFEREED JOURNAL, JUNE-JULY 2023, VOL-11/58
https://doi.org/10.5281/zenodo.8240925

CUSTOMERS' CONSCIOUSNESS ABOUT FINANCIAL CYBER FRAUDS IN ELECTRONIC BANKING: AN INDIAN PERSPECTIVE WITH SPECIAL REFERENCE TO MUMBAI CITY

Ameya Madhukar Rane, Ph.D.

Senior Lecturer, Regenesys Business School, South Africa, Email: ameyar@regenesys.net

Paper Received On 20 June 2023

Peer Reviewed On 22 July 2023

Published On: 1 August 2023

Abstract

The use of Machine Learning and Deep Learning techniques has become pervasive in areas of finance, such as trading, mobile banking, payments, and granting of credit to customers. Moreover, these methods are essential in dealing with financial offenses, fraud, and cyberattacks. Cybercrime is on the rise and cybercriminals are taking advantage of hacking and social engineering strategies to undermine the security systems of financial and corporate establishments. It is troublesome to recognize financial cybercrime activities. Banks and other financial organizations have to confront not just the challenge of distinguishing authentic illegal dealings, but also the need of transparency, fairness, and confidentiality from their customers and regulatory authorities, which necessitates applying artificial intelligence techniques to identify fraud-related activities in a specific way. Despite their popularity, there is still a lack of a complete comprehension of the financial cybercrime environment, associated methods, their flaws, and fresh open issues in this area. Through this investigation, the researcher intends to fill the void by examining the financial cybercrime system based on two levels: (a) the various deceitful practices utilized by criminals; and (b) customers' comprehension of various kinds of financial cyber frauds. This study will concentrate on the financial literacy and public understanding of cybercrime technique. The goal is not only to address cybercrime yet additionally to build up preventive measures by characterizing proper procedures which fraud is acted and devoted. It is estimated that the income generated from financial wrongdoings makes up 2-5% of the world's total GDP (approx. $2 trillion USD) (Forum, n.d.). The anti-money laundering rules in effect are not adequate enough to tackle a problem of this magnitude. Not only have the number of crimes, both identified and hidden, grown, but so has their cost. Cybercrime and malicious hacking have become more common. In the world of financial crime, regulators are continually changing the rules, with a view to counter illegal trafficking and money laundering, and governments are more actively utilizing economic sanctions, focusing on countries, organizations and even single people. Institutions are realising that their existing techniques for dealing with such criminal activities are not enough.

***Keywords**: Financial crime, E-Banking, Cybercrime, Security threats, Customer Awareness*

1. Introduction:

As per Juniper Research (2020), there are over two billion individuals using electronic banking services through their mobile phones, smartwatches, and tablets, and this number is growing exponentially due to the user-friendly interface of the applications, their time-saving aspect and cost-effectiveness. The COVID-19 pandemic has also had an influence on the growth of these services since customers are unable to visit their banks for financial activities.

With the development of modern computing technology and data networks, people no longer need to break into vaults to steal money as there is a much larger sum of money in the digital space. Banks are adapting to the current trend of doing business virtually and at the same time protecting themselves from cybercriminals. Cybercrime is a form of criminal activity that uses technology, such as a computer and a network, from anywhere in the world. It is increasing due to cyber-criminals taking advantage of the advancements in technology, which can be used to either commit the crime or be the target of an attack. Any person with access to a working computer and the internet can be at risk of being a victim of cybercrime. It can affect anyone, from offices, banks, business owners, government departments, schools, universities, and even individuals.

Cybercrime is a type of illegal activity that is done to gain monetary gain, particularly in the finance and banking sectors. Examples of this type of crime include identity theft, financial fraud, phishing emails, and internet fraud, as well as attempts to steal data from consumers, such as account information, internet banking, credit card details, and other bank accounts.

According to Gordon and Loeb (2003), the most common types of cybercrime related to finances involve denial-of-service virus attacks, unapproved access, hacking, and website vandalism. Cybercrime in the money-related domain denotes a criminal activity that is financially motivated and includes identity theft, ransomware assaults, email and online fraud, and attempts to steal information regarding bank accounts, credit cards, or other payment cards.

Generally, commercial banks are very keen to promote the utilisation of electronic banking in order to provide customers with rapid and efficient banking services. Such services are delivered via digital channels with a minimal physical presence. Nonetheless, cybercrime still remains a problem in the banking industry with cyber criminals taking full advantage of the new digital technology.

In order to comprehend the security problems and the necessity for remedial measures, one has to be aware of the methods and tactics employed by cyber-criminals to gain access without permission and utilize financial data for illegal purposes. Identity theft is a frequent approach used by computer hackers when dealing with web-based businesses, particularly with online banking, where the identity of another person or third party, for example, a bank card, name, date of birth, is stolen for illegitimate activities. Any information acquired by cyber-criminals through identity theft can be used for whatever objective, like obtaining loans, opening an account, or applying for credit cards.

2. Objectives of the study:

1. To understand the customer awareness towards potential threat to e-banking services provided by banks and financial institutions

2. To know the level of awareness related to precautionary measures to be taken to avoid financial frauds

3. The types of Financial cyber-attacks on e-banking:

It is critical that individuals who use online banking be aware of the cyber threats that exist so they can protect themselves. In the following parts of this study, cybercrimes are examined.

Malware is a shortened form of malicious software and includes viruses, ransomware and spyware. Developed by cybercriminals, malware is built to damage data and systems or access confidential information. The users of e-banking can be impacted by malware if they download untrustworthy applications or click on links that are not needed.

Social engineering entails criminals looking for private information. When individuals are the targets, the criminals are usually trying to deceive them into giving away their passwords or banking details, or getting access to their computer to surreptitiously install malicious software. This gives the criminals control of the computer and confidential data, as well as access to passwords and financial information.

Phishing is a form of social engineering attack in which the aggressor sends an email or text message with catchy content, containing links that can lead to the installation of malware, system freezing as part of a ransomware attack, or the exposure of confidential information (A. Naser, 2021).

Keylogger is recognized as one of the earliest forms of malware that is still prevalent and regularly utilized as part of bigger cyber-assaults. It can be simply defined as a type of monitoring software that is programmed to capture keystrokes a user inputs. These keystroke loggers collect the information typed into a website or application and send it to an unauthorized third party.

Man-in-the-middle is a type of threat that happens when a hacker meddles with the communication between a sender and receiver either to secretly listen in or alter the traffic that is travelling between them. Attackers may utilize MitM attacks to take login credentials or personal information.

Shoulder surfing is a form of social engineering threats used to obtain data such as (PINs), passwords and other sensitive information by looking over the victim's shoulder. The perpetrator can observe the keystrokes typed on a device or eavesdrop on private conversations.

A denial-of-service (DOS) attack is a method used to disrupt a service or network, thus making it inaccessible to the intended users. This is done by sending a huge amount of requests or data that will cause the system to crash.

Vishing is a type of social engineering attack that uses the telephone to coax victims into revealing sensitive information, such as passwords and PINs. The perpetrator usually uses psychological techniques, like fear, sympathy, and greed, to manipulate people into giving up what they want.

4. Related Literature

The article "Formulating specialized legislation to address the growing spectre of cybercrime: A comparative study" by Cassim F.(2019) examines cyber legislation designed to control cybercrime in USA, UK, Australia, India, Gulf states, and South Africa. The research demonstrates that existing laws are inadequate in managing the risks of cybercrimes, and thus, there should be specialized cyber laws to address the rapid changes in technology. Moreover, there is a need for continuous research and training of IT security personnel, financial service sector personnel, police officers, prosecutors, and the judiciary to help them stay up-to-date with the evolving technology.

A. Lakshmanan (2019) conducted an exploration which was solely based on cybercrime and concluded that cybercrime activities will continue to rise with no sign of stopping. Ms. Neeta and Dr. V.K. Baksh (2019) shared a research paper on Cybercrimes in Banking Sector, recommending that cyber-attacks should be prevented by following the law strictly. H. Singh Rao (2019) conducted a research to analyze Cyber Crimes in Banking Sector, which exposed that India is one of the top 20 countries that is vulnerable to cybercrime.

Vimla (2016) conducted a study to gain an insight into the customers' perceptions and comprehension of E-banking security, as well as the issues they encountered while utilizing e-banking services. The sample size included 50 customers from a single area. The results revealed that only 32% of the participants had knowledge regarding the safety issues in E-banking and 50% experienced cyber-attacks, such as hacking and phishing. The study additionally concentrated on the inadequacy of information among victims of cyber-crime and the responsibilities of the local government and banks to conduct Awareness campaigns to educate people about the cyber security risks.

5. Significance of the research:

The value of this research can be seen in the successful suggestions for improved security measures and heightened awareness among online banking customers. It is a useful resource for financial institutions looking to make people knowledgeable on the subject of cyber security and provide them with advice to cope with online risks. The originality of this research lies in the comprehensive strategy taken to comprehend the severity of threats to the online banking sector.

6. Research Methodology:

The study is based upon both primary and secondary data

6.1 Primary Data: A survey was done targeting inhabitants of Mumbai who make use of e-banking services. A random selection method was used for the survey. The questionnaire was then distributed to 260 e-banking users in Mumbai during the month of January 2023.

6.2 **Secondary data:** Additionally, secondary data was utilized for the research, which was sourced from articles, working papers, and websites of various banks.

6.3 Questionnaire design: The questionnaire consisted of 15 exhaustive questions and was given to customers to gauge their opinion on cyber-attacks. The data was collected from people aged 18 and above who use online banking services. A sample of 260 individuals was taken into consideration for the study.

6.4 Area of study: Until September 2022, the Mumbai Police's cybercrime wing has observed 3,668 scenarios, with 1,073 of them concerning internet or credit card fraud (PTI, 2023). As Mumbai is considered to be the financial capital of India, it is more likely to be targeted for economic crime. Therefore, this research will focus on measuring the level of knowledge among the e-banking customers in Mumbai.

6.5 Hypothesis of the study

H0: The e-banking customers are completely aware about the potential threat to such services provided by banks and financial institutions.

6.6 Limitations of the study

This research concentrates exclusively on cybercrimes associated with the Indian E-banking space. It does not assess the entire financial industry. The areas explored and the strategies implemented are limited to Mobile and Internet Banking customers. The inherent limitations of statistical tools applies to the study.

7. Results and Discussion:

7.1 Focus of the study: The study focuses on the following main questions that are addressed through the questionnaire.

1. Are e-banking customers of Mumbai city aware about financial cyber frauds?
2. Which type of financial fraud customers are aware about?
3. Are customers storing sensitive personal information on their device?
4. Do they trust on e-banking services?
5. Are they satisfied with the awareness programs being carried on by financial institutions?
6. Are they aware about the prevention techniques to avoid such attacks?

Table 1: Awareness about the financial cybercrimes?

	Responses	Percent
No	15	5.8
Somewhat	29	11.2
Yes	216	83.1
Total	260	100.0

(Source: Author's Computation)

Form the above data, 83.1% of the respondents are aware about the financial cyber frauds, whereas 11.2% are partially aware and 5.8% are not at all having knowledge about such crimes. Researcher has then focused to understand the level knowledge among the respondents who are have at least heard about financial cyber frauds (n=245)

In this section, researcher has highlighted the main finding of the questionnaire also the main characteristics of the result.

Table 2: Demographic distribution:

Age-wise Distribution		
	Number of respondents	Percent
18-29	29	11.8
30-39	100	40.8
40-49	92	37.6
50-59	24	9.8
Total	245	100.0
Education-wise distribution		
	Number of respondents	Percent

Graduation	30	12.2
Post-graduation	133	54.3
professional	82	33.5
Total	245	100.0
Occupation-wise distribution		
	Number of respondents	Percent
Business	5	2.0
Employment	162	66.1
Profession	54	22.0
Other	24	9.8
Total	245	100.0
Income-wise distribution		
	Number of respondents	Percent
up to 250000	35	14.3
Between 250000 and 500000	63	25.7
Between 500000 and 750000	66	26.9
Between 750000 and 1000000	18	7.3
Above 1000000	63	25.7
Total	245	100.0

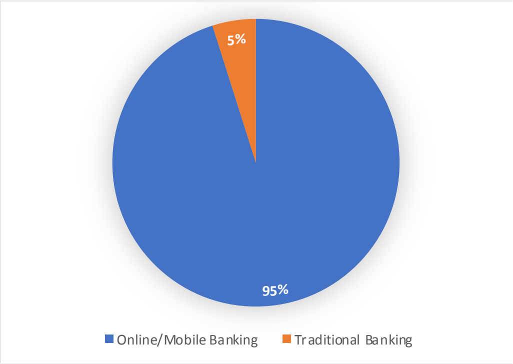
(Source: Author's Computation)

The above table shows the classification of respondents on the basis of their demography, which comprises of age, education, occupation and income of the respondents. The result shows the majority of the responses out of 245 are from the age group of 30-39 as 40.8% and 40-49 as 37.6%. The researcher also recorded the responses as per the education where 12.2% are graduates, 54.3% are post graduates and 33.5% are having professional qualification. The occupation of the respondents are categorised as employment, business, profession and other having responses as 66.1%, 2%, 22% and 9.8% respectively. In terms of income status, the respondents having salary of less than Rs 250000 are 14.3%, salary between Rs 250000 and Rs 500000 are 25.7%, salary between Rs 500000 and Rs 750000 are 26.9%, salary between Rs 750000 and Rs 1000000 are 7.3% and 25.7% for more than Rs 1000000.

7.2 Descriptive Analysis:

Descriptive statistics is an important tool for researchers as it helps them summarize data in an organized manner. The relationship between variables in a sample or population can be accurately described using this method. It provides more clarity to the research process and allows researchers to gain better insights into their data. Descriptive statistics can be used to identify correlations, trends, and patterns among variables in a sample or population, enabling researchers to make more informed decisions based on their findings.

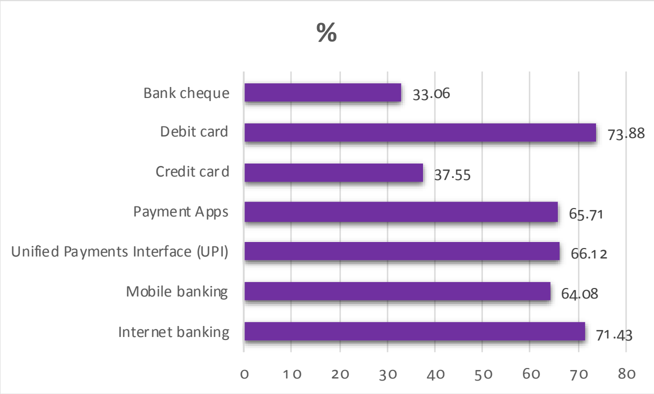
Figure 1: Preference towards mode of banking use



(Source: Author's Computation)

From 245 respondents, 233 (95%) prefer online banking over traditional banking which are 12 (5%)

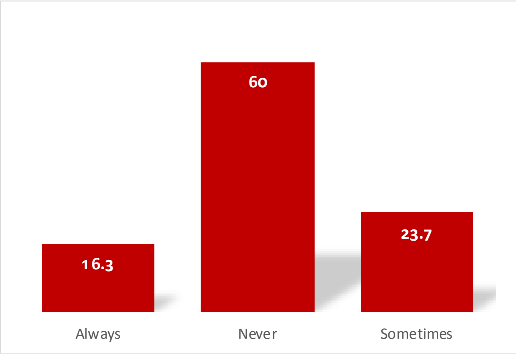
Figure 2: Customers' preference towards mode of payment



(Source: Author's Computation)

Above figure shows 73.88% of the respondents use debit card, 78.43% use internet banking, 66.12% use UPI, 65.71% use payment apps and 64.08% use mobile banking for making payment for various reasons. 37.55% of the respondents use credit card where as 33.06% use bank cheque for the payment.

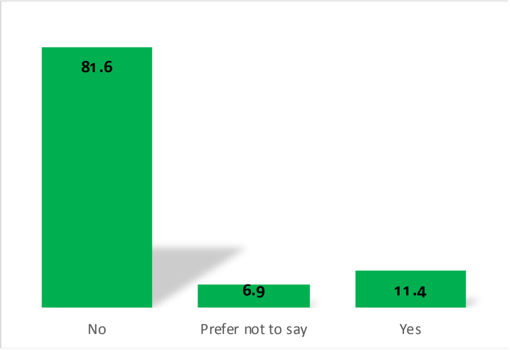
Figure 3: Storing bank related information in personal electronic devices.



(Source: Author's Computation)

As per the above figure, 40 respondents out of 245 i.e. 16.3% stores the banking related information on their smartphones and/or computer devices, whereas 58 respondents (23.7%) stores the information sometimes and 147 (60%) say they never stores the data on the electronic devices.

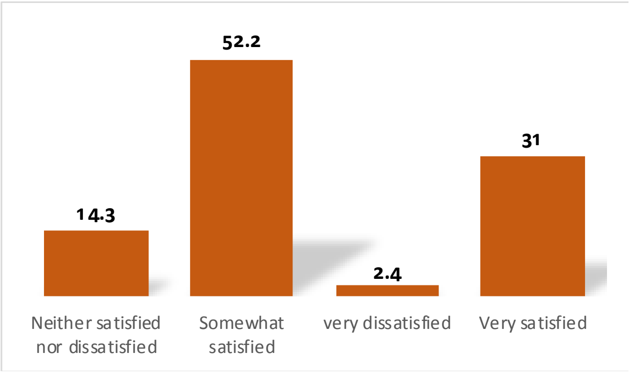
Figure 4: Loss of Money due to financial frauds



(Source: Author's Computation)

From the gathered data, 11.4% of the respondents (28 out of 245) have lost their money due to financial fraud and 81.6% i.e. (200 out of 245) have never encountered to such situation, whereas 6.9% respondents have denied to report for the same.

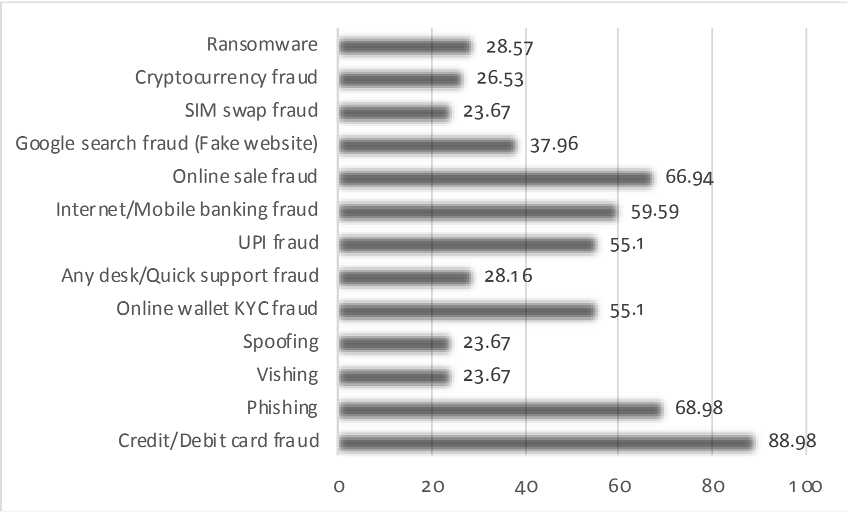
Figure 5: Efforts taken by bank in creating awareness about prevention of financial frauds



(Source: Author's Computation)

From the above figure, 31% of the respondents (76 out of 245) are extremely satisfied and 52.2% (128 out of 245) are moderately satisfied with the awareness programs of the banks for educating customers related to prevention techniques of financial crimes. 2.4% of the respondents are completely dissatisfied and 14.3% are neutral on this question.

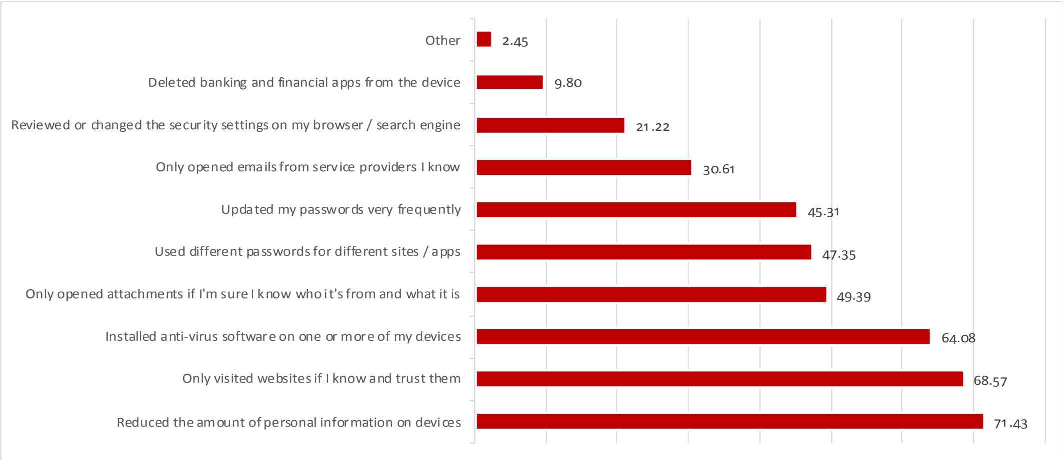
Figure 6: Awareness about various types of Financial crimes



(Source: Author's Computation)

Above figure shows 88.98% of the respondents know about credit/debit card fraud, 68.98% aware about phishing, 66.94% know online sale fraud, 59.59% aware about internet/ mobile banking fraud, 55.1% each know about UPI and online wallet KYC fraud. The respondents who also know about Ransomware, Cryptocurrency, SIM swap, Google search fraud, any desk/quick support fraud, spoofing and vishing are 28.57% 26.53% 23.67% 37.96% 28.16% 23.67% and 23.67% respectively.

Figure 7: Awareness about precautionary measures to be taken to safeguard from online financial fraud.



(Source: Author's Computation)

Above information is related to the precautionary measures taken by the respondents to avoid financial cyber frauds. 71.43% of the respondents reduce the amount of personal information on devices, 68.57% Only visit the known and trusted websites, 64.08% installed anti-virus software on one or more of the devices, 49.39% only open attachments if it is known who it's from and what it is, 47.35% use different passwords for different sites / apps, 45.31% update passwords very frequently, 30.61% only open emails from the known service providers, 21.22% review or change the security settings on the browser / search engine, 9.80% Delete banking and financial apps from the devices and 2.45% take other precautionary measures.

7.3 Hypothesis testing

Table 3.1: Descriptive analysis between age of the respondents and awareness of financial frauds

		I am aware about the information regarding threats, but not all type of threats	I am not aware about the threats involved in internet banking services	I know all types of threats associated with internet banking.	Total
Age	18-29	21	2	6	29
	30-39	69	2	29	100
	40-49	80	6	6	92
	50-59	17	1	6	24
Total		187	11	47	245

(Source: Author's Computation)

The above table shows 29 respondents (29%) from the age group 30-39 are completely aware about financial frauds. Similarly 6 (21%), 6 (7%) and 6 (25%) respondents are aware from the age group 18-29, 40-49 and 50-59 respectively. Rest of the respondents are either not aware or partially aware about such financial cyber frauds.

Table 3.2: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	17.994	6	.006
Likelihood Ratio	20.104	6	.003
N of Valid Cases	245		

(Source: Author's Computation)

The null hypothesis states that the e-banking customers are completely aware about the potential threat to e-banking services provided by banks and financial institutions. From the above table of chi-square test, the value of p is 0.003 which is less than the significant value of 0.05. Hence researcher failed to accept the null hypothesis. Therefore, the customers are still not completely aware about the potential threat to e-banking services provided by banks and financial institutions.

8. Conclusion:

This research was conducted with the responses of 245 people, which enabled us to come to a conclusion. It is essential to recognize and be cognizant of the security issues that may occur with online banking services. We need to measure the trust of the users of online banking. It is crucial that they are aware of the threats that could come from cyber criminals. These individuals often use techniques such as hacking, phishing, vishing, identity theft, denial of service, and social engineering to acquire financial data. Therefore, online banking customers should be conscious of the tactics used by these criminals.

This Study finds there are more than 60% users who give more preference to debit card, internet banking, payment apps, unified payment interface and mobile banking. Approximately 40% of the users save the banking related sensitive information on their personal electronic devices. Around 20% users might have lost their money due to financial cyber frauds. Nearly 70% of the customers are still not completely satisfied with the awareness programs carried on by the banking and Financial institutions to educate the customers. There are still more than 70% of the banking customers who are not aware about Ransomware, cryptocurrency fraud, SIM swap fraud, any desk or quick support fraud, spoofing and vishing. Looking at the precautionary measures to be taken by the customers, still there are more than 50% people who neither update their password frequently nor use different passwords for different sites nor open emails from known service providers, which eventually exposes them to search ill activities by the intruders. Hypothesis states there is a dire need of complete awareness of such financial fraud among the e-banking customers.

With the development of technology, banking has become more sophisticated. This can present both an opportunity and a challenge for bankers and clients. A banker's success is reliant on the amount of trust they gain from their customers. This trust is based on how they ensure the safety of the money. It is also the responsibility of the customers to secure themselves from cyber threats. This document explains the importance of customers being informed in the use of technology when it comes to banking. Merely updating the bank's systems is not enough to secure customers from cyber threats, but rather, educating customers about the use of technology is also essential.

References:

A. Adholiya and S. Adholiya, "A Study on Cyber Security Practices and Tips Awareness among E-Banking A Study on Cyber Security Practices and Tips Awareness among E- Banking Services Users of Udaipur , Rajasthan," Int. J. Sci. Res. Multidiscip. Study, vol. 5, no. 8, pp. 148–154, 2019.

A. Naser, M. Jazzar, D. Eleyan, and A. Eleyan, "Social Engineering Attacks : A Phishing Case Simulation," no. 03, 2021.

Forum, W. E. (n.d.). Global Coalition to fight Financial Crime. Retrieved January 2023, from weforum.org: https://www.weforum.org/projects/coalition-to-fight-financial-crime

Gordon, L.A. & Loeb, M.P. (2003). A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM, 46(3), 81-85. https://doi.org/10.1145/636772.636774

Gupta, S. (2012). Buffer overflow attack. IOSR Journal of Computer Engineering, 1(1), 10-23. https://doi.org/10.9790/0661-0111023

Lakshmanan A (2019) "Literature review on Cyber Crimes and its Prevention Mechanisms" UniversitiSains Malaysia, pp.01-05.

Neeta, Dr.V.K.Bakshi, (2019) "Cyber Crimes in Banking Sector"Aayushi International Interdisciplinary Research Journal (AIIRJ), Vol.VI, Issue V, pp.25-31.

Singh Rao(2019), "Cyber Crime in Banking Sector", International Journal of Research - Granthaalayah, 7(1), pp.148-161.

V. Vimala, "An Evaluative Study on Internet Banking Security among Selected Indian Bank Customers," Amity J. Manag. Res., vol. 1, no. 1, pp. 63–79, 2016.

World Economic Forum Annual Meeting, Davos-Klosters, Switzerland, January 23–26, 2018; LexisNexis risk solutions 2018 True Cost of Fraud study, LexisNexis, August 2018, risk.lexisnexis.com.

Cite Your Article As:
Dr. Ameya Madhukar Rane. (2023). CUSTOMERS' CONSCIOUSNESS ABOUT FINANCIAL CYBER FRAUDS IN ELECTRONIC BANKING: AN INDIAN PERSPECTIVE WITH SPECIAL REFERENCE TO MUMBAI CITY. Scholarly Research Journal for Humanity Science & English Language,, 11(58), 420–432. https://doi.org/10.5281/zenodo.8240925