

**A STUDY ON CUSTOMER PERCEPTION TOWARDS
ONLINE BANKING FRAUD**

Submitted in partial fulfilment of the requirements for the award of

MASTER OF BUSINESS ADMINISTRATION

by

VIGNESH.N

Register No.40410192



DEPARTMENT OF BUSINESS ADMINISTRATION

SCHOOL OF MANAGEMENT STUDIES

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL 2022



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with “A” grade by NAAC | 12B Status by UGC | Approved by AICTE

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **VIGNESH.N 40410192** who carried out the project entitled “**A Study on customer perception towards online banking fraud**” under my supervision from January 2022 to March 2022.

Dr. Princy. A.S

Internal guide

External Guide

Dr. BHUVANESWARI. G

Dean – School of Management Studies

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **VIGNESH.N (40410192)** hereby declare that the Project Report entitled “**A Study on customer perception towards online banking fraud**” done by me under the guidance of **Dr. Princy. A.S** is submitted in partial fulfilment of the requirements for the award of Master of Business Administration degree.

DATE:

PLACE: CHENNAI

SIGNATURE OF CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my sincere thanks to **Dr. G. Bhuvaneswari, Dean - School of Management Studies** and **Dr. A. Palani, Head - School of Management Studies** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. Princy. A.S, Assistant Professor** for her valuable guidance, suggestions, and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **School of Management Studies** who were helpful in many ways for the completion of the project.

VIGNESH.N

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	Abstract	(i)
	List of tables	(ii)
	List of charts	(iv)
1	Introduction	1
	1.1 . Online banking fraud	1
	1.2 . Industry profile	4
	1.3 Functions	4
2	Review of literature	5
3	Research methodology	10
	3.1 Need for study	
	3.2. Scope of the study	10
	3.3. Objectives of the study	10
	3.4. Research design	11
	3.5. Sources of data	11
	3.6. Structure of questionnaire	11
	3.7. Sampling technique	11
	3.8. Period of study	11
	3.9. Analytical tools	11
	3.10. Limitations of the study	12
4	Data analysis and interpretation	13
	4.1 Percentage analysis	13
	4.2. One sample t test	46
	4.3. Independent sample t test	57
	4.4 One-way Anova	65
5	Findings, suggestions and conclusion	69
	5.1. Findings	69
	5.2. Suggestions	74
	5.3. Conclusion	75
	References	76
	Annexure I – questionnaire	77
	Annexure II – Article	1

ABSTRACT

According to the RBI's annual report, bank frauds of ₹100,000 and above have more than doubled in value to ₹1.85 lakh crores in FY20 as compared to ₹71,500 crores in FY19. Also, the number of such cases has increased by 28% in the same period. According to a report by Hindustan Times, India has lost a total of ₹615.39 crores in more than 1.17 lakh cases of online banking frauds from April 2009 to September 2019. The occurrence of these frauds is spread over a decade. But the banking industry is witnessing a significant rise in the number of online banking frauds. Therefore, it is necessary to study on customer perception towards online banking frauds to create more awareness about online banking frauds.

LIST OF TABLES

TABLE NO.	PARTICULARS	PAGE NO.
4.1.1	Gender of the respondents	13
4.1.2	Age of the respondents	14
4.1.3	Highest Qualification of the respondents	15
4.1.4	Marital status of the respondents	16
4.1.5	Employment status of the respondents	17
4.1.6	How often respondents use online banking	17
4.1.7	How often respondent's access bank account using online banking	18
4.1.8	Respondent's importance towards online banking	19
4.1.9	Respondents know online banking fraud	20
4.1.10	How often respondent's follows bank's preventive rules	21
4.1.11	Respondents have been a victim of online fraud	22
4.1.12	Respondent's know someone who have been a victim of online banking fraud	22
4.1.13	How much money respondents have lost in online banking fraud	23
4.1.14	Respondents know national helpline to report cyber-crime	24
4.1.15	Respondent's thought's on helpline number	25
4.1.16	Respondent's awareness in online frauds	26
4.1.17	Respondent's level of agreement with statement	29
4.1.18	Respondent's degree of agreement with statement	31
4.1.19	Respondent's awareness in most common online banking fraud	33
4.1.20	Respondent's awareness in security instructions	37
4.1.21	Respondent's awareness in bank instructions	41
4.1.22	Respondent's rating in bank's mode of communication to increase awareness in online banking fraud	44

LIST OF CHARTS

CHART NO.	PARTICULARS	PAGE NO.
4.1.1	Gender of the respondents	13
4.1.2	Age of the respondents	14
4.1.3	Highest Qualification of the respondents	15
4.1.4	Marital status of the respondents	16
4.1.5	Employment status of the respondents	17
4.1.6	How often respondents use online banking	18
4.1.7	How often respondent's access bank account using online banking	19
4.1.8	Respondent's importance towards online banking	20
4.1.9	Respondents know online banking fraud	20
4.1.10	How often respondent's follows bank's preventive rules	21
4.1.11	Respondents have been a victim of online fraud	22
4.1.12	Respondent's know someone who have been a victim of online banking fraud	23
4.1.13	How much money respondents have lost in online banking fraud	24
4.1.14	Respondents know national helpline to report cyber-crime	25
4.1.15	Respondent's thought's on helpline number	26
4.1.16	Respondent's awareness in online frauds	27
4.1.17	Respondent's level of agreement with statement	29
4.1.18	Respondent's degree of agreement with statement	32
4.1.19	Respondent's awareness in most common online banking fraud	34
4.1.20	Respondent's awareness in security instructions	38
4.1.21	Respondent's awareness in bank instructions	42
4.1.22	Respondent's rating in bank's mode of communication to increase awareness in online banking fraud	44

CHAPTER 1

INTRODUCTION

1.1 ONLINE BANKING FRAUD

Online banking fraud or Internet banking fraud is fraud or theft that uses online technology to illegally withdraw funds from a bank account and/or transfer funds to an account from another bank. . Internet banking fraud is a form of identity theft and is often carried out through techniques such as phishing. Now, internet banking is widely used to check account details, make purchases, pay bills, transfer funds, print statements, and more. In general, user identity is the customer ID number and password provided to secure transactions. But due to ignorance or some stupid mistake, it is easy to fall into the trap of cyber criminals. Here are some simple tips to help you avoid falling into the trap of cybercriminals. Remember that a simple ignorance or negligence can dramatically reduce your hard-earned savings.

1.1.1 Securing your account: Avoid online banking on insecure Wi-Fi systems and work only on your home computer. Do not share your password with anyone. Don't write it down on paper in your diary. Just remember. It must be alphanumeric and change frequently. Never respond to online inquiries from banks regarding your account or personal information. Do not store your personal data on public computers or email.

1.1.2 Phishing: A person's personal data is obtained by scammers posing as bankers, who launch a website similar to that of the person's bank. They are required to provide all personal information regarding themselves and their account at the bank for the reason of updating the database. The numbers and passwords are then used to transact on their behalf without their knowledge. Phishing is the use of a form of spamming to fraudulently gain access to people's online banking details. In addition to targeting online banking customers, phishing emails can target online auction sites or other online payment methods. Typically, a phishing email will ask online banking customers to follow a link to update their personal bank account details. If the link is followed, the victim downloads a program that obtains their banking credentials and passes them on to a third party.

1.1.3 Spam: Spam is an electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.

1.1.4 Nigerian Scam: Nigerian or Frauds 409 or 419 are basically the lottery scam in which some overseas persons are involved in cheating innocent persons or organizations by promising to give a good amount of money at nominal charges. Their intention is to steal money in the form of fee for the lottery prize.

1.1.5 Spyware: Spyware like a Trojan is generally thought of as software that is secretly installed on a computer and takes everything from it without the user's permission or knowledge. Spyware can get personal information, business information, bandwidth; or the ability to process and secretly give it to someone else. The "Trojan Horse" scheme occurs when malicious software (malware) embeds itself on a consumer's computer without the consumer's knowledge. Trojans usually take the form of links or attachments from unknown email senders. Once installed, the software detects when someone visits online banking sites and records usernames and passwords to send to criminals. People using public computers, in places like Internet cafes, are often susceptible to Trojans like malware or spyware.

1.1.6 Check sites URL: Always check the URL of your bank's web site. Fraudsters can lure you to enter your user ID and password at a fake website that resembles your bank. If you see anything other than the bank's genuine URL, it has to be fake. Never enter your user ID or password or such sensitive information without ascertaining that you are on the right website. Always type the Web address of your bank into the browser address space. Never click on the link in the email.

1.1.7 Fool-proof password: Change your online banking password at regular intervals. Also, avoid easy-to-guess passwords, like first names, birthdays, children's or spouse's name and telephone numbers. Try to have an alphanumeric password, one that combines alphabets and numbers. If you have several bank accounts, never use the same online banking password for all.

Never select the option on a browser that stores or retains the user name and password. As it can easily be cracked by cyber criminals. Also, never paste your password, always type it in. This small amount of 'finger exercise' will go a long way in safety.

1.1.8 Always check 'last logged': Most banks have a 'last logged in' panel on their websites. If your bank has it, check the panel whenever you log in. If you notice irregularities (like you are logging in after two days, but the panel says you logged in that morning!), report the matter immediately to your bank and change your password right away. Always log out when you exit the online banking portal. Close the browser to ensure that your secure session is terminated. Never exit simply by closing the browser.

1.1.9 Keep your system up to date: Regularly check for security updates for your computer operating system. Most security updates are aimed at reducing risks to your computer, these may be data-related or otherwise. Make sure that your operating system and browser have the latest security patches installed. And, always install these only from trusted websites. Install a personal firewall to prevent hackers from gaining unauthorised access to your computer, especially if you connect to the Internet through a cable or a DSL modem.

1.1.10 Public access can be injurious: Don't leave the PC unattended after keying in information while transacting on the website. Avoid accessing your bank online at cyber cafes or on a share or public computer. Also, avoid locations that offer online connections through wireless networks (Wi-Fi), where privacy and security are minimal.

1.1.11 Follow Bank instructions: Banks say that appropriate upgrade is carried out from time to time by their IT departments for risk mitigation. They issue instructions to customers to manage their accounts through virtual keyboards by way of which the characters typed by them are not identified by hackers. SMS alerts are also an important tool, since any transaction carried out on account is reported to the account holder through an SMS.

1.1.12 Protection: Learn the ways to protect yourself from online banking fraud schemes. Detect Trojans that appear on your PC in the form of viruses, spyware or malware through Antivirus Software, anti-Spyware,

and Adware. Also, learn to keep your cards, documents and passwords safe, and monitor your accounts to safeguard yourself from bank fraud committed through identity theft.

1.2 INDUSTRY PROFILE

The banking industry includes systems of financial institutions called banks that help people store and use their money. Banks offer clients the opportunity to open accounts for different purposes, like saving or investing their money. The banking industry is also valuable to the economy, as it provides resources for individuals, families and organizations to use for transactions and investments. One way that the banking industry does this is by organizing and distributing loans for applicants that they can use for purposes like purchasing property, starting a business or financing a college education.

1.3 FUNCTIONS

Banks as financial intermediaries are involved in remittances from end savers to end users. Banks often help change the terms of a contractual agreement as funds go through the remittance process in a way that supports and encourages economic activity. Banks can provide flexibility in the circulation of exchanges that improve the efficiency of payment systems by issuing tradable claims (bank deposits) to themselves. These deposits can support personal lending to consumers (retail banking) or short-term lending to non-financial companies (commercial banks). In this case, the bank supports liquidity management and promotes personal consumption and trade. Banks, each with a larger denomination for a longer period of time, to those who want to fund their investment in large capital projects by facilitating financing from a large number of small savers in a short period of time. We encourage a pool of funds to lend. Investment loans can take the form of securities issuance (investment banking) or real estate loans (mortgage business). By focusing on risk assessment, banks can monitor borrower performance. By diversifying across investment projects, we encourage the allocation of funds to ventures with maximum financial potential while minimizing certain risks. Through the international expansion of trade credit (merchant banking), banks can promote international trade and commerce.

CHAPTER 2

REVIEW OF LITERATURE

In this Chapter, the researcher has tried to study and understand the concepts of study on customer perception towards online banking fraud. This attempt includes, understanding the basic concepts of study on customer perception towards online banking fraud, analysing research studies made by earlier researchers in respect of study on customer perception towards online banking fraud, for this, the researcher has used various books, research Journals and websites. The detailed list is further elaborated in the Bibliography. Through this Literature Survey researcher wants to find out which are the important parameters of customer perception in respect of **A Study on customer perception towards online banking fraud.**

Mr. Rupesh. D. Dubey and Dr. Anita Manna (2022) in their paper “**E-BANKING FRAUDS AND FRAUD RISK MANAGEMENT**” has mentioned that E-banking means any entity that permits the borderless banking facilities anytime, anywhere and anyhow banking. Internet Banking Fraud is a form of identity theft and is usually made possible through techniques such as phishing, lottery fraud scam etc. In simple meaning any user with a personal computer and a internet connection get connected to his bank website to perform any of I.T system, the banking services are delivered by way of a Computer-Controlled System. With the advances in information technology, most banks in India have migrated to core banking platforms and have moved transactions to payment cards and to electronic channels like Automated teller machine (ATM), Internet Banking and Mobile Banking, It leads to the creation of minds of frauds through online i.e. internet banking frauds Fraudsters have followed customers into this space. Internet banking fraud is targeted on dormant account.

Komal Saxena,Dr. Anurag Awasthi (2022) in their paper “**A Solutions Provided to Secured Your Online Banking Frauds**” has mentioned that Growth of credit card and debit card usage along with online internet banking has led to a tremendous spurt in the amount of banking frauds. Individuals are typically promised large sums of money if they make payment of minor fees. 1.2(b) Phishing is a common method employed by cyber criminals to lure unsuspecting people to reveal their credit card numbers, ID and password. The most common route is to send an

email that requests recipients to click on a link that takes them to a fake website where they are required to disclose their details. 1.2(c) Identity theft is damaging in that criminals can make fraudulent use of credit cards or steal identity details in order to open false accounts or even obtain loans. SMS may be used as a route to target the unwary and obtain vital credit or debit card details. 1.2(g) Wire Transfer fraud: - of more relevance of institutions and of great concern is the growing amount of wire transfer fraud and automated clearing house transaction fraud. 4.2 Other Ways to Prevent yourself from Online fraud :a) Update your software's and use current virus protection. b) Create strong passwords by using at least one special character c) Don't expect or received emails from unknown. (Restricted your email box) d) Use your pop-up blocker e) Download files only from well-known sites f) Sign up for email/text "transaction alerts" from your bank to keep track of your purchases g) Remove history whenever use your id's credit card, Smart Card etc. h) Remove Log list from the net. I) always log off from your internet managing an account session.

MARTIN DESCAZEUX, MATHIEU COUTURIER & YASMINE EL HIMDI (2022) in their paper **“THE NEW METHODS IN THE FIGHT AGAINST ONLINE BANK FRAUD”** has mentioned that it is clear that inadequate management of the risks of fraudulent activity can have extremely damaging consequences: financial impacts of undetected fraudulent transactions, impacts on image, customer confidence, and operations. At the end of 2016, British bank Tesco Bank was the victim of a cyber-attack which affected 40,000 of its customers' accounts. The protection of the customer journey, in order to ensure secure processing of sensitive financial operations through the putting in place of protective measures and the development of customer awareness; The traditional approach to the protection of the customer journey is based on multiple solutions such as authentication which provides a first layer of essential security. As the degree of protection is quite limited in many cases, businesses have started to invest in systems which are better able to detect and respond rapidly to fraud, while continuing to offer a satisfying customer experience. Several concepts are being discussed in the context of French data protection legislation (LIL) and the EU's General Data Protection Regulation (GDPR), to limit the use of personal data and artificial intelligence.

Dr. C.B. Pavithra, Dr. K. Geetha (2021) in their paper **“FACTORS AFFECTING CUSTOMERS' PERCEPTION TOWARDS DIGITAL BANKING SERVICES”** has

mentioned that Digital banking is a refers to accomplishment of financial transactions over the Internet through a bank's secured websites. Users feel that digital banking is convenient, ubiquitous, instant transfer of funds and they are satisfied with digital banking services. The users of digital banking transactions are influenced by the factors such as Transaction Speed, Compatibility, Connectivity, Security, Convenience and Benefits. The respondents feel that using digital banking services are very much beneficial for them in many ways.

M. Kannan (2019) in their paper “Digital Users Perception on Digital Banking Frauds - A Study with Special Reference to Selected Digital Banking Services”

has mentioned that Digital banking is the new avenue of innovative banking in present day banking industry. The new age banking customers look for convenient, costless and any place banking services at any time motivate the bankers irrespective of their institutional structure to employ human less intervention banking with the support of modern and emerging information communication technology front gadgets namely automate teller machines, internet banking, mobile banking, apps, telebanking for various banking services ranges from deposit, loan, money transfer, account verification, loan syndication and basic utility services for their customers. The outcome of the study shows that the digital frauds especially on security and privacy have significant impact on the trust of customers on digital banking it is recommended to the bankers to invest a reasonable amount on bringing new technology on creating security walls as well as customer privacy syndromes.

V Vimala (2016) in their paper “An Evaluative Study on Internet Banking Security among Selected Indian Bank Customers”

has mentioned that India has third largest internet population in the world after China and United States and presents unmatched developmental prospect for the internet segment in coming years. Internet banking system proves to be very versatile in completing transactions like balance inquiry, withdrawal, deposits, viewing the bank statement, and record of recent transaction. This study provides a guide to the current structure of the Internet banking security and highlights awareness level of customers for using Internet banking, and their perception and satisfaction towards Internet banking with new technologies and its functioning. A supreme and powerful security policy employed by the banks and legislation instituted by local or state

Governments should be in use and obligatory in order to improve security in Internet banking systems

Veena K.P, Suheel (2016) in their paper “**Customer perception towards E-Banking services: A study with reference to Vijaya bank, Mysuru city**” has mentioned about Majority 50.00 per cent and 60.00 per cent of the respondents strongly agreed and satisfied with account statement and funds transfer e-banking services provided by the bank. All the respondents i.e. 100.00 per cent strongly agreed that bank provides 24/7 hours access e- banking services this is one of the motivational factor of customer to adopt e-banking services. Around 50.00 per cent and 56.00 per cent of the respondents were strongly agreed with bank provide quick ATM services and wireless e-banking services to the customer. The success of the banking sector whether directly or indirectly depends on the customer as they have they are the backbone of the company with development of technology the customer expectations are raising relentlessly, competitive will survive who can respond to the customer needs faster and better than anyone, skilled staff square measure less with relation to electronic banking than manual banking and the decision creating is within the hands of prime management solely

Shewangu Dzomira (2016) in their paper “**Financial consumer protection: internet banking fraud awareness by the banking sector**” has mentioned that financial customers become more urbane, it becomes critical for the banks to consider the use of technology and awareness efforts to take action to their incessantly changing needs. This study concludes that internet banking fraud awareness disclosure is very low by many Southern African banks There is positive reception of the accessible information on internet banking fraud awareness on Southern Africa banks’ websites, this study proposes a call for increasing the awareness information and update financial consumers of internet banking fraud perpetrated by internet fraudsters. To minimize internet banking fraud allied with internet activities conducted within the Southern Africa region, banks should make ample disclosure and awareness of internet fraud information on their websites and take correct measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which the bank is providing internet banking services. This study proposes a policy by banking regulators or overseers in each of the Southern Africa jurisdictions for increasing the internet

fraud awareness information and update financial consumers of internet banking fraud perpetrated by internet-fraudsters.

S. SURIYAMURTHI, MAHALAKSHMI. V & R.KARTHIK (2012) in their paper “**A STUDY ON CUSTOMER PERCEPTION TOWARDS INTERNET BANKING**” has mentioned that The main objective of the Indian banking sector reforms of the 1990s was to promote a diversified, efficient and competitive financial system with the ultimate goal of improving the efficiency of resources through operational flexibility, improved financial viability and institutional strengthening, to bring it at par with global benchmarks. While investigating all the variables and responses given by the consumers, this study reveals that the perception of the consumers can be changed by conducting awareness program, friendly usage, less charges, proper security, and the best response to the services offered. As per our basic assumptions we consider only those consumers who know how to use Internet and have accessibility of Internet, This study considers only to those banks which provide Internet banking Facility. Even though these people are inclined towards the manual banking, these can be turned to potential customers, it is well proved. Results through this study will help to understand customer’s perception and some actions can be initiated to improve the usage of internet banking. If the above data is used, it will be helpful for the banks in reducing the cost of operation whereas manual banking is more costly compared to internet banking.

Divya Singhal and V. Padhmanabhan (2009) in their paper “**A Study on Customer Perception towards Internet Banking: Identifying Major Contributing Factors**” has mentioned that Internet banking is the term used for new age banking system. The present study aims to explore the major factors responsible for internet banking based on respondents’ perception on various internet applications. Factor Analysis was performed with 15 statements related with internet banking features. This study has successfully examined the major factors responsible for internet banking based on respondents’ perception on various internet applications; future research may include examining the factors importance. The analysis done with the help of statistical tools clearly indicate the factors responsible for internet banking.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 NEED FOR STUDY

Research methodology is mainly needed for the purpose of framing the research process and the designs and tools that are to be used for the project purpose. Research methodology helps to improve by creating more awareness about online banking fraud between people. This study will help to understand customer perception towards online banking fraud. This study helps to create an awareness on customer about online banking fraud. This study helps customer to prevent from online banking fraud. This research methodology is framed for the purpose of finding the level of **customer's awareness and perception about online fraud in Chennai**.

3.2 SCOPE OF THE STUDY

Online banking fraud is happening in India. This study is to identify whether the people are aware of online banking fraud. The study is conducted to reveal how much customer aware of online banking fraud and their perception towards online banking fraud. This study will help to find out whether customer aware of online fraud and follows preventive measures.

3.3 OBJECTIVES OF THE STUDY

This project is designed mainly to identify and to study the customer perception on online banking fraud.

3.3.1 Primary objective:

- To know how far customer aware about online banking fraud.
- To know how far customer aware about the bank's preventive measure in online banking fraud.

3.3.2 Secondary objectives:

- To understand the customers perception towards online banking fraud.
- To improve preventive measures in online banking fraud.

3.4 RESEARCH DESIGN

3.4.1 Descriptive Research Design

Descriptive research is a study designed to depict the participants in an accurate way. More simply put, descriptive research is all about describing people who take part in the study.

3.5 SOURCES OF DATA

Data collection is the term used to describe a process of preparing and collecting data.

- Primary Data – Questionnaire given to 150 respondents
- Secondary Data - Websites and online journals, Published reports & Review of literature from published articles

3.6 STRUCTURE OF QUESTIONNAIRE

Questionnaire was divided into two sections. First part was designed to know the general information about customers and the second part contained the **respondent's perception towards online banking fraud.**

3.7 SAMPLING TECHNIQUE

3.7.1 Convenience sampling method

A convenience sample is one of the main types of non-probability sampling methods. A convenience sample is made up of people who are easy to reach.

3.8 PERIOD OF STUDY

The duration of study is from December 2021 to March 2022 which is two months of study.

3.9 ANALYTICAL TOOLS

3.9.1. Percentage analysis

Research questions are always answered with a descriptive statistic: generally, either percentage or mean. Percentage is appropriate when it is important to know how many of the participants gave a particular answer. Generally, percentage is reported when the responses have discrete categories.

3.10 LIMITATIONS OF THE STUDY

- The study is confined to Chennai district only
- The study is based upon the customer perception towards online banking fraud.
- The data collected for the research is fully on primary data given by the respondents. There is chance for personal bias. So, the accuracy is not true
- Due to shortage of time and other constraints, the study has been limited 150 respondents only.

CHAPTER 4

DATA ANALYSIS AND INTERPRETATION

4.1 PERCENTAGE ANALYSIS

Table 4.1.1 Gender of the respondents

Gender	No of Respondents	Percentage
Male	93	62%
Female	57	38%

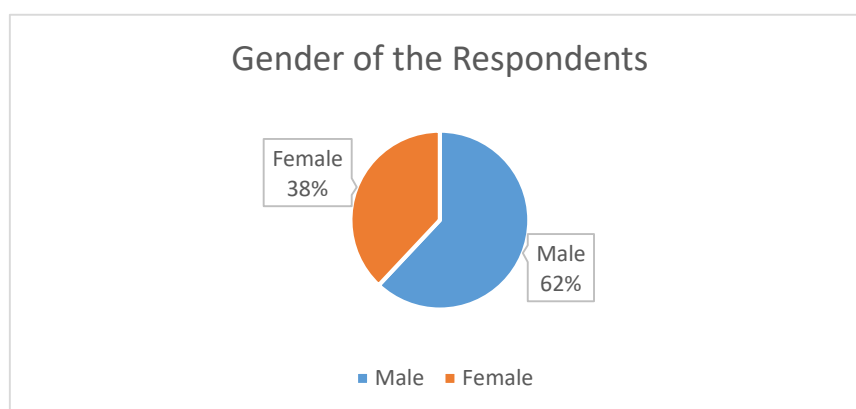


Chart 4.1.1 Gender of the respondents

INTERPRETATION:

From the above table total number of respondents is 150 and from above the table, it is interpreted that 62% of the respondents are male respondents and 38% of the respondents are female respondents.

INFERENCE:

Majority (62%) of respondents are male respondents.

Table 4.1.2 Age of the respondents

Age	No of Respondents	Percentage
18-20	8	5.33%
20-30	83	55.33%
30-40	14	9.33%
40-50	29	19.33%
Above 50	16	10.67%

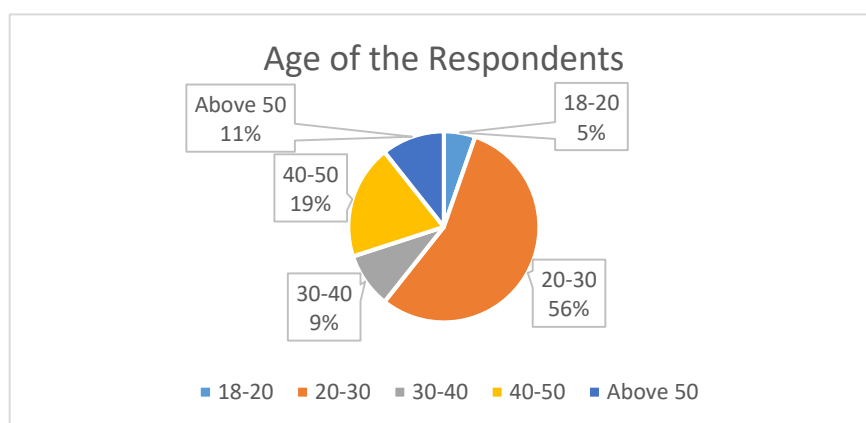


Chart 4.1.2 Age of the respondents

INTERPRETATION:

From the above table total number of respondents is 150 and from above table it is interpreted that 5.33% of respondents are 18-20 age respondent, 55.33% of respondents are 20-30 age respondent, 9.33% of respondents are 30-40 age respondent, 19.33% of respondents are 40-50 age respondent and 10.67% of respondents are Above 50 age respondent.

INFERENCE:

Majority (55.33%) of respondents are 20-30 age respondent.

Table 4.1.3 highest qualification of the Respondents

Highest Qualification	No of Respondents	Percentage
SSLC	0	0%
HSC	2	1.33%
UG	51	34%
PG	96	64%
DIPLOMA	1	0.67%

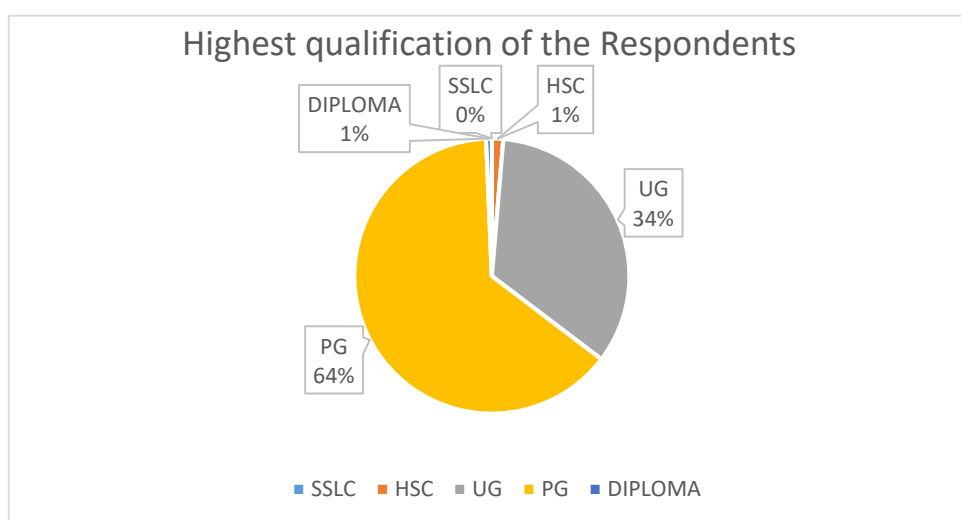


Chart 4.1.3 highest qualification Respondents

INTERPRETATION:

From the above table total number of respondent's is 150 and from above table, it is interpreted 0.00% of the respondent's completed SSLC, 1.33% of the respondent's completed HSC, 34% of the respondent's completed UG, 64% of the respondent's completed PG and 0.67% of the respondent's completed DIPLOMA.

INFERENCE: Majority (64%) of the respondent's completed PG.

Table 4.1.4 marital status of the Respondents

Marital Status	No of Respondents	Percentage
Married	60	40%
Single	90	60%

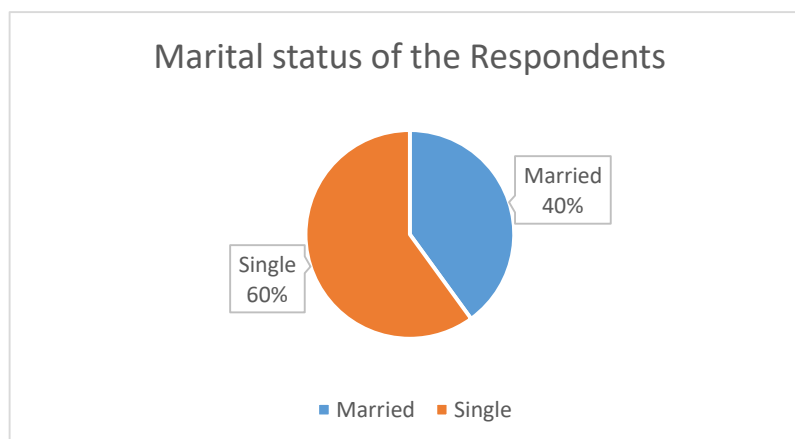


Chart 4.1.4 marital status of the Respondents

INTERPRETATION:

From the above table total number of respondents is 150 and from above table, it is interpreted that 40% of the respondents are married and 60% of the respondents are single.

INFERENCE: Majority (60%) of the respondents are single.

Table 4.1.5 employment status of the respondents

Are you Employed	No of Respondents	Percentage
Yes	90	60%
No	60	40%

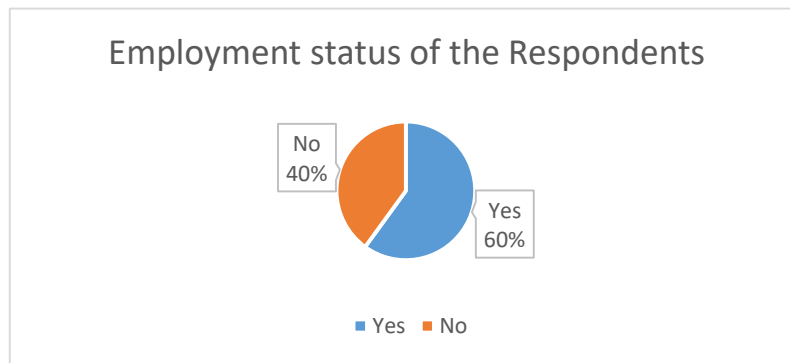


Chart 4.1.5 employment status of the respondents

INTERPRETATION:

From the above table total number of respondents is 150 and from above table, it is interpreted that 60% of the respondents are employed and 40% of the respondents are not employed.

INFERENCE: Majority (60%) of the respondents are employed.

Table 4.1.6 how often respondents use online banking

Online Banking Usage	No of Respondents	Percentage
Occasionally	54	36%
Frequently	73	48.67%
Never	11	7.33%
Very Often	12	8%

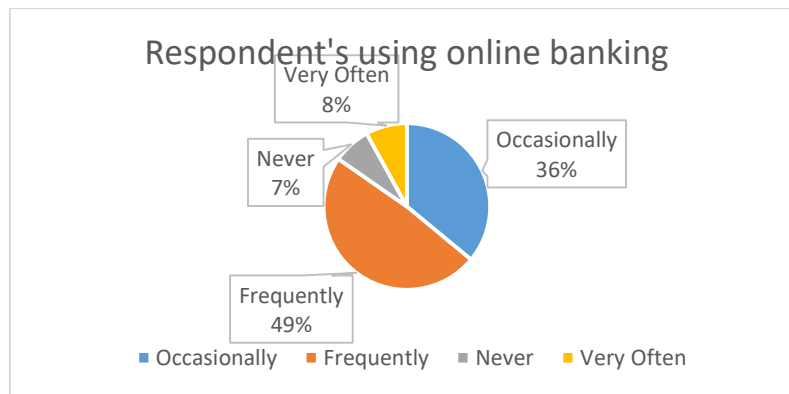


Chart 4.1.6 how often respondents use online banking

INTERPRETATION:

From the above table total number of respondents is 150 and from the above table, it is interpreted that 36% of respondents occasionally used online banking, 48.67% of respondents frequently used online banking, 7.33% of respondents never used online banking and 8% of respondents are used online banking very often.

INFERENCE:

Majority (48.67%) of respondents frequently used online banking.

Table 4.1.7 how often respondent's access bank account using online banking

Accessing bank account using online banking	No of Respondents	Percentage
Occasionally	60	40%
Frequently	63	42%
Never	13	8.67%
Very often	14	9.33%

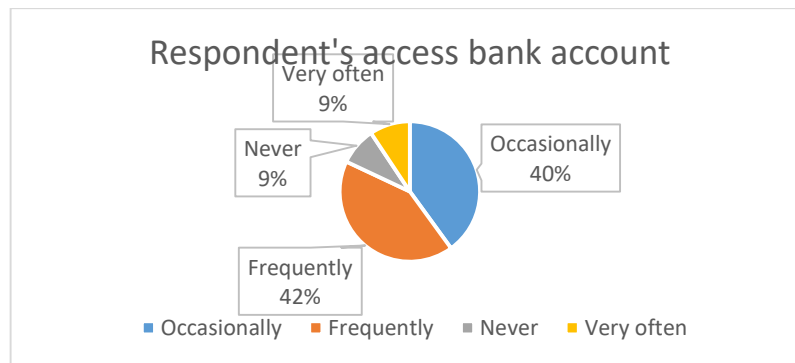


Chart 4.1.7 how often respondent's access bank account using online banking

INTERPRETATION:

From the above table total number of respondents is 150 and from the above table, it is interpreted that 40% of respondents occasionally used online banking to access bank account, 42% of respondents frequently used online banking to access bank account, 8.67% of respondents never used online banking to access bank account and 9.33% of respondents are used online banking very often to access bank account.

INFERENCE:

Majority (42%) of respondents frequently used online banking to access bank account.

Table 4.1.8 respondent's importance towards online banking

Online banking is Important to You	No of Respondents	Percentage
Important	88	59%
Moderate	56	37%
Not Important	6	4%

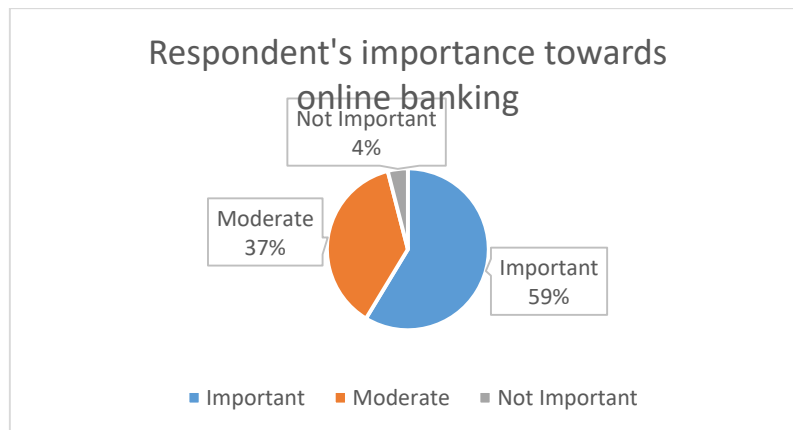


Chart 4.1.8 respondent's importance towards online banking

INTERPRETATION:

From the above table total number of respondents is 150 and from the table, it is interpreted that 59% of respondents think online banking is important, 37% of respondents think online banking is moderate and 4% of respondents thinks online banking is not important.

INFERENCE:

Majority (59%) of respondents think online banking is important.

Table 4.1.9 respondents know online banking fraud

Online banking Fraud	No of Respondents	Percentage
Yes	124	82.67%
No	26	17.33%

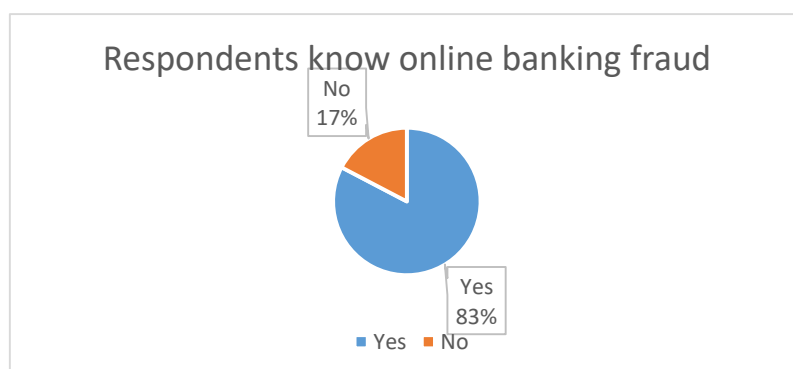


Chart 4.1.9 respondents know online banking fraud

INTERPRETATION:

From the above table total number of respondents is 150 and from the table, it is interpreted that 82.67% of respondents know about the online banking fraud and 17.33% of respondents didn't know about the online banking fraud.

INFERENCE:

Majority (82.67%) of respondents know about the online banking fraud.

Table 4.1.10 how often respondent's follows bank's preventive rules

Follows bank's preventive Rules	No of Respondents	Percentage
Occasionally	42	28%
Frequently	71	47.33%
Never	15	10%
Very Often	22	14.67%

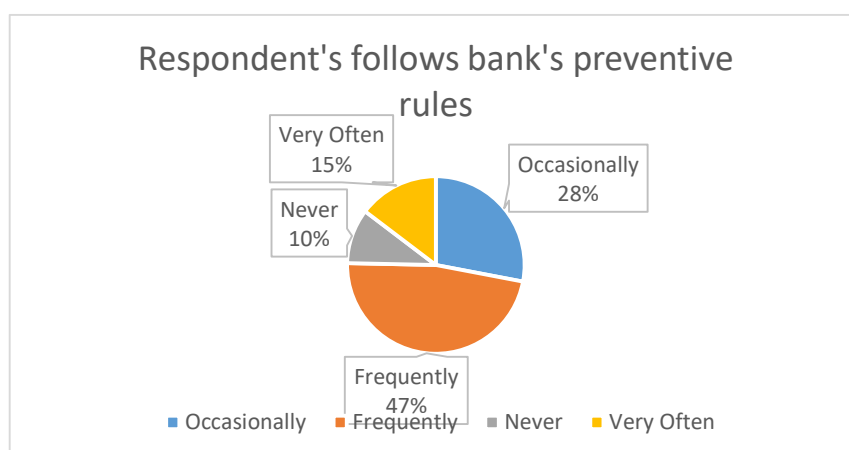


Chart 4.1.10 how often respondent's follows bank's preventive rules

INTERPRETATION:

From the above table total number of respondents is 150 and from the above table, it is interpreted that 28% of respondents occasionally follow's bank preventive rules, 47.33% of respondents frequently follow's bank preventive rules, 10% of respondents never follow's bank preventive rules and 14.67% of respondents follow's bank preventive rules very often.

INFERENCE:

Majority (47.33%) of respondents frequently follow's bank preventive rules.

Table 4.1.11 respondents have been a victim of online fraud

Have you been a Victim of Online Banking Fraud	No of Respondents	Percentage
Yes	28	18.67%
No	122	81.33%



Chart 4.1.11 respondents have been a victim of online banking fraud

INTERPRETATION:

From the above table total number of respondents is 150 and from the table, it is interpreted that 18.67% of respondents have been a victim of online banking fraud and 81.33% of respondents haven't been a victim of online banking fraud.

INFERENCE:

Majority (81.33%) of respondents haven't been a victim of online banking fraud.

Table 4.1.12 respondent's know someone who have been a victim of online banking fraud

Have you know someone who been a victim of online banking fraud	No of Respondents	Percentage
Yes	63	42%
No	87	58%



Chart 4.1.12 respondent's know someone who have been a victim of online banking fraud

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that 42% of respondents know someone have been a victim of online banking fraud and 58% of respondents didn't know someone have been a victim of online banking fraud.

INFERENCE:

Majority (58%) of respondents didn't know someone have been a victim of online banking fraud.

Table 4.1.13 how much money respondents have lost in online banking fraud

Money you have lost in online Banking Fraud	No of Respondents	Percentage
Less than 1000	13	8.67%
1000-5000	14	9.33%
5000-10000	3	2%
More than 10000	1	0.67%
Never	119	79.33%

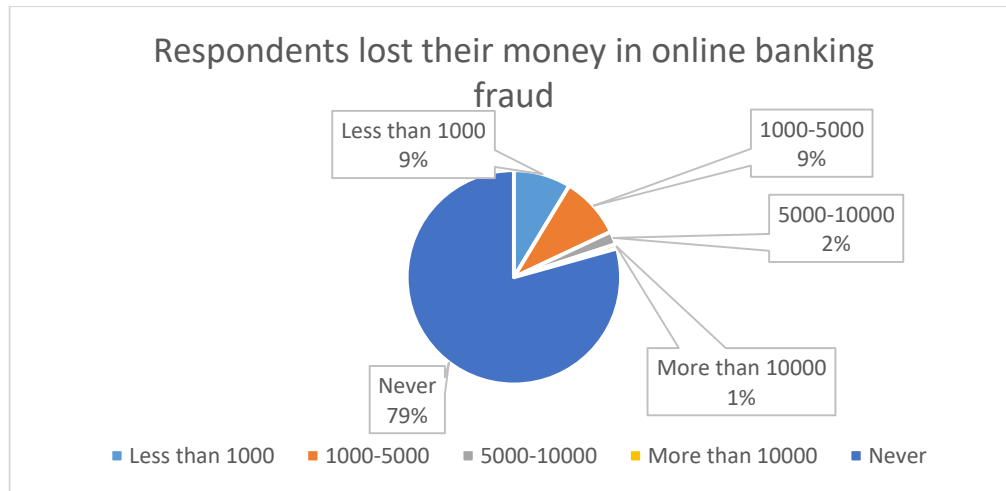


Chart 4.1.13 how much money respondents have lost in online banking fraud

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that 8.67% of respondents have lost their money worth less than Rs1000 in online banking fraud, 9.33% of respondents have lost their money worth in between Rs1000-5000 in online banking fraud, 2% of respondents have lost their money worth in between Rs5000-10000 in online banking fraud, 0.67% of respondents lost their money worth more than Rs10000 online banking fraud and 79.33% of respondents never lost their money in online banking fraud.

INFERENCE:

Majority (79.33%) respondents never lost their money in online banking fraud.

Table 4.1.14 respondents know national helpline to report cyber-crime

Government launches national helpline to report cyber-crime	No of Respondents	Percentage
Yes	64	42.67%
No	86	57.33%

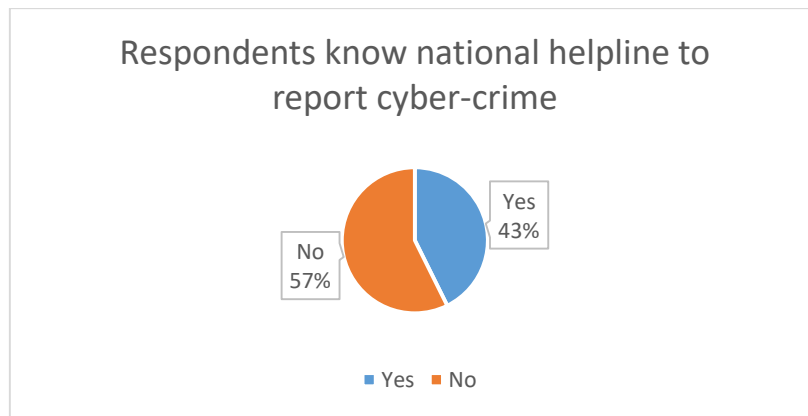


Chart 4.1.14 respondents know national helpline to report cyber-crime

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that 42.67% respondents know that the national helpline number to report cyber-crime and 57.33% respondents didn't know about the national helpline number to report cyber-crime.

INFERENCE:

Majority (57.33%) of respondents didn't know about the national helpline number to report cyber-crime.

Table 4.1.15 respondent's thought's on helpline number

Thought's on helpline number	No of Respondents	Percentage
Useful	128	85.33%
Not useful	22	14.67%

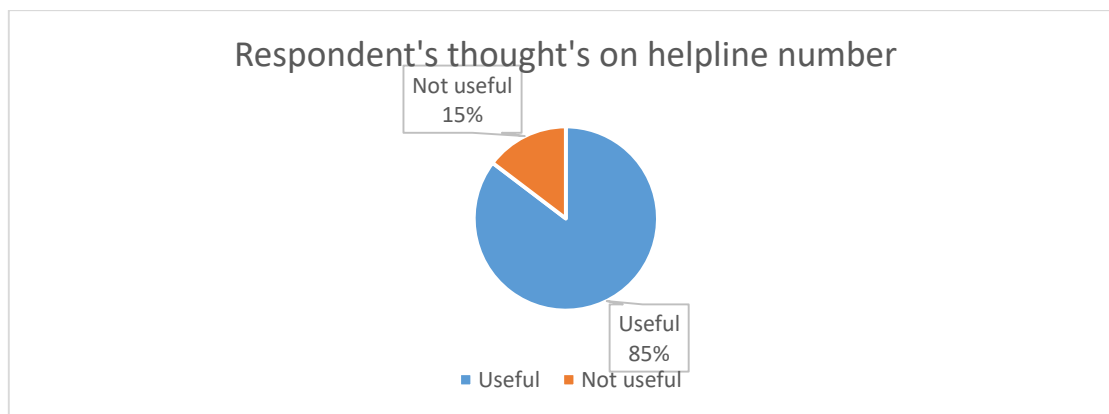


Chart 4.1.15 respondent's thought's on helpline number

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that 85.33% respondents think that national helpline number is useful and 14.67% respondents think that national helpline number is not useful.

INFERENCE:

Majority (85.33%) of respondents think that national helpline number is useful.

Table 4.1.16 respondent's awareness in online frauds

Aware of Online banking Fraud	Strongly Not aware	%	Not aware	%	Moderately aware	%	aware	%	Strongly aware	%
E-mail	18	12%	36	24%	34	22.67%	31	20.67%	31	20.67%
Text messages	9	6%	16	10.67%	37	24.67%	40	26.67%	48	32%
Website advertisements	15	10%	21	14%	48	32%	28	18.67%	38	25.33%
Telephone (Mobile phone)	11	7.33%	15	10%	38	25.33%	42	28%	44	29.33%
Redirect website page	14	9.33%	27	18%	37	24.67%	38	25.33%	34	22.67%
Downloaded software	9	6%	31	20.67%	42	28%	32	21.33%	36	24%

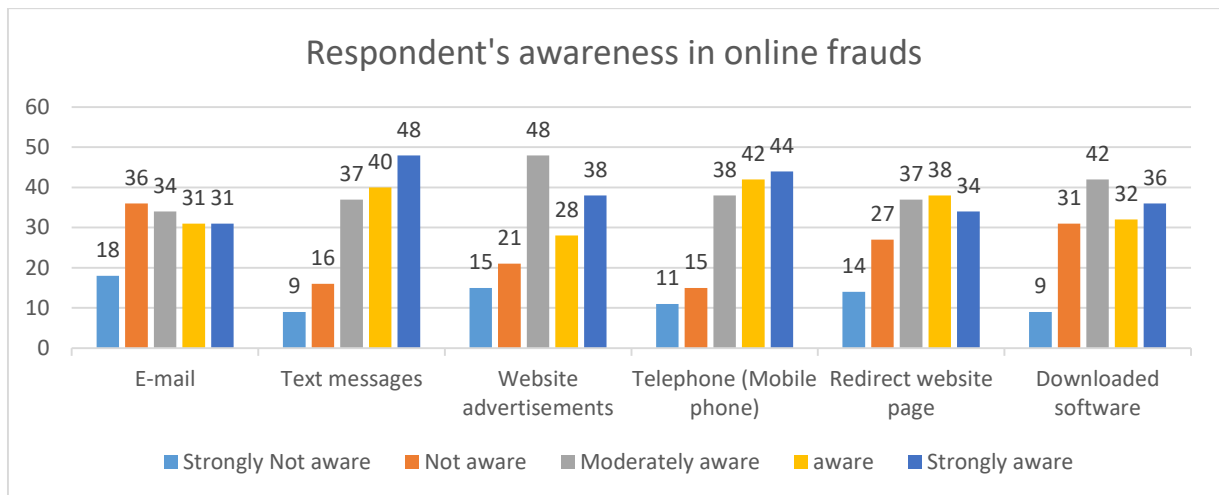


Chart 4.1.16 respondent's awareness in online frauds

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that

- 12% of respondents strongly Not aware of online fraud sent through E-mail, 24% of respondents Not aware of online fraud sent through E-mail, 22.67% of respondents Moderately aware of online fraud sent through E-mail, 20.67% of respondents aware of online fraud sent through E-mail and 20.67% of respondents strongly aware of online fraud sent through E-mail.
- 6% of respondents strongly Not aware of online fraud sent through Text messages, 10.67% of respondents Not aware of online fraud sent through Text messages, 24.67% of respondents Moderately aware of online fraud sent through Text messages, 26.67% of respondents aware of online fraud sent through Text messages and 32% of respondents strongly aware of online fraud sent through Text messages.
- 10% of respondents strongly Not aware of online fraud sent through website advertisements, 14% of respondents Not aware of online fraud sent through website advertisements, 32% of respondents Moderately aware of online fraud sent through website advertisements, 18.67% of respondents aware of online fraud sent through website advertisements and 25.33% of respondents strongly aware of online fraud sent through website advertisements.

- 7.33% of respondents strongly Not aware of online fraud sent through Telephone (Mobile phone), 10% of respondents Not aware of online fraud sent through Telephone (Mobile phone), 25.33% of respondents Moderately aware of online fraud sent through Telephone (Mobile phone), 28% of respondents aware of online fraud sent through Telephone (Mobile phone) and 29.33% of respondents strongly aware of online fraud sent through Telephone (Mobile phone).
- 9.33% of respondents strongly Not aware of online fraud sent through Redirect website page, 18% of respondents Not aware of online fraud sent through Redirect website page, 24.67% of respondents Moderately aware of online fraud sent through Redirect website page, 25.33% of respondents aware of online fraud sent through Redirect website page and 22.67% of respondents strongly aware of online fraud sent through Redirect website page.
- 6% of respondents strongly Not aware of online fraud sent through Downloaded software, 20.67% of respondents Not aware of online fraud sent through Downloaded software, 28% of respondents Moderately aware of online fraud sent through Downloaded software, 21.33% of respondents aware of online fraud sent through Downloaded software and 24% of respondents strongly aware of online fraud sent through Downloaded software.

INFERENCE:

- Majority 24% of respondents not aware of online fraud sent through E-mail.
- Majority 32% of respondents strongly aware of online fraud sent through Text messages.
- Majority 32% of respondents moderately aware of online fraud sent through website advertisements.
- Majority 29.33% of respondents strongly aware of online fraud sent through Telephone (Mobile phone).
- Majority 25.33% of respondents aware of online fraud sent through Redirect website page.
- Majority 28% of respondents moderately aware of online fraud sent through Downloaded software.

Table 4.1.17 respondent's level of agreement with statement

Level of Agreement with Statement	Strongly Disagree	%	Disagree	%	Moderate	%	Agree	%	Strongly agree	%
I am aware of the risks from online banking	12	8%	8	5.33%	30	20%	69	46%	31	20.67%
My bank provides free anti-virus for my online banking	16	10.67%	39	26%	51	34%	33	22%	11	7.33%
My bank provides adequate support against online fraud	7	4.67%	11	7.33%	72	48%	42	28%	18	12%

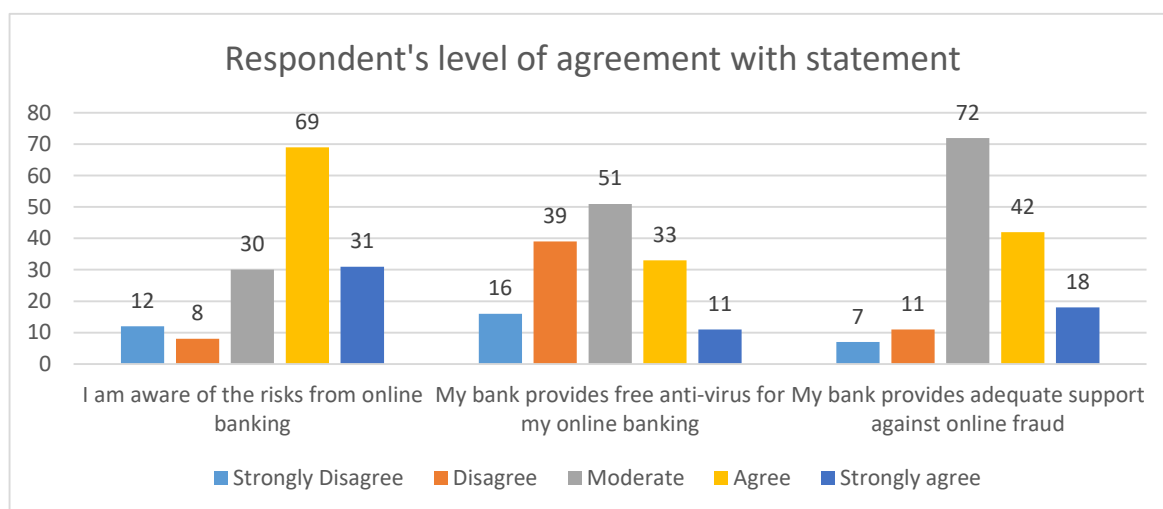


Chart 4.1.17 respondent's level of agreement with statement

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that

- 8% of respondents strongly disagree with the statement I am aware of the risks from online banking, 5.33% of respondents disagree with the statement I am aware of the risks from online banking, 20% of the respondents

moderate with the statement I am aware of the risks from online banking, 46% of respondents agree with the statement I am aware of the risks from online banking and 20.67% of respondents strongly agree with the statement I am aware of the risks from online banking.

- 10.67% of respondents are strongly disagree with the statement my bank provides free anti-virus for my online banking, 26% of respondents are disagree with the statement my bank provides free anti-virus for my online banking, 34% of respondents are moderate with the statement my bank provides free anti-virus for my online banking, 22% of respondents are agree with the statement my bank provides free anti-virus for my online banking and 7.33% of respondents are strongly agree with the statement my bank provides free anti-virus for my online banking.
- 4.67% of respondents are strongly disagree with the statement my bank provides adequate support against online fraud, 7.33% of respondents are disagree with the statement My bank provides adequate support against online fraud, 48% of respondents are moderate with the statement My bank provides adequate support against online fraud, 28% of respondents are agree with the statement my bank provides adequate support against online fraud and 12% of respondents are strongly agree with the statement my bank provides adequate support against online fraud.

INFERENCE:

- Majority 46% of respondents agree with the statement I am aware of the risks from online banking.
- Majority 34% of respondents are moderate with the statement my bank provides free anti-virus for my online banking.
- Majority 48% of respondents are moderate with the statement my bank provides adequate support against online fraud.

Table 4.1.18 respondent's degree of agreement with statement

Degree of Agreement with statement	Strongly Disagree	%	Disagree	%	Moderate	%	Agree	%	Strongly agree	%
Do you agree that the information provided by your bank about online fraud awareness is adequate	14	9.33 %	17	11.33 %	59	39.33 %	46	30.67 %	14	9.33 %
Do you need more awareness about online fraud risk	5	3.33 %	14	9.33 %	47	31.33 %	45	30%	39	26%

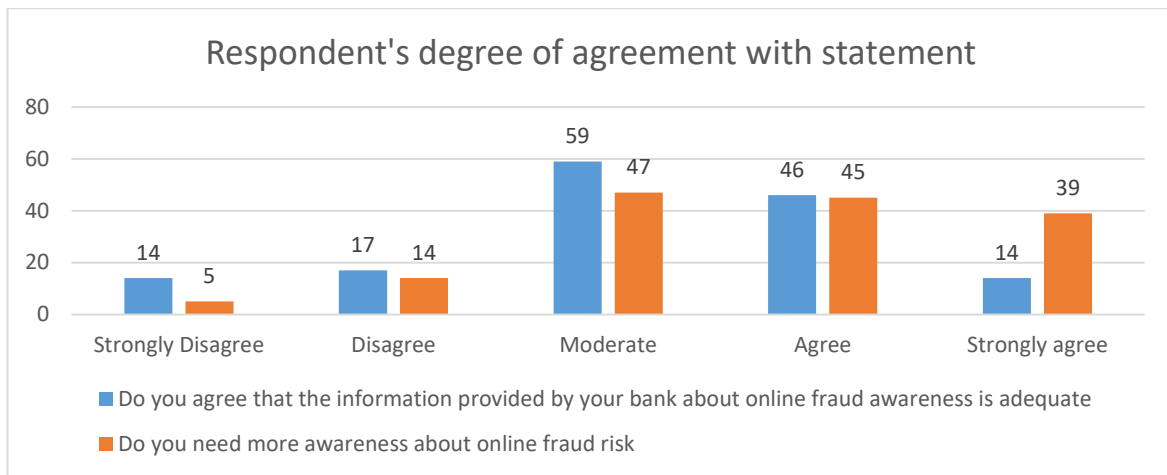


Chart 4.1.18 respondent's degree of agreement with statement

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that

- 9.33% of respondents strongly disagree with the statement Do you agree that the information provided by your bank about online fraud awareness is adequate, 11.33% of respondents disagree with the statement Do you agree that the information provided by your bank about online fraud awareness is adequate, 39.33% of the respondents moderate with the statement Do you agree that the information provided by your bank about online fraud awareness is adequate, 30.67% of respondents agree with the statement Do you agree that the information provided by your bank about online fraud awareness is adequate and 9.33% of respondents strongly agree with the statement Do you agree that the information provided by your bank about online fraud awareness is adequate.
- 3.33% of respondents are strongly disagree with the statement Do you need more awareness about online fraud risk, 9.33% of respondents are disagree with the statement Do you need more awareness about online fraud risk, 31.33% of respondents are moderate with the statement Do you need more awareness about online fraud risk, 30% of respondents are agree with the statement Do you need more awareness about online fraud risk and 26% of respondents are strongly agree with the statement Do you need more awareness about online fraud risk.

INFERENCE:

- Majority (39.33%) of the respondents are moderate with the statement Do you agree that the information provided by your bank about online fraud awareness is adequate.
- Majority (31.33%) of the respondents are moderate with the statement Do you need more awareness about online fraud risk.

Table 4.1.19 respondent's awareness in most common online banking fraud

Most common online Banking Fraud	Strongly Not aware	%	Not aware	%	Moderately aware	%	aware	%	Strongly aware	%
Scam	11	7.3 3%	17	11.3 3%	34	22.6 7%	54	36%	34	22.6 7%
Malware /Virus	7	4.6 7%	25	16.6 7%	40	26.6 7%	51	34%	27	18%
Spyware	12	8%	23	15.3 3%	50	33.3 3%	38	25.3 3%	25	16.6 7%
Phishing or fraudulently making customers give their own information	11	7.3 3%	15	10%	38	25.3 3%	43	28.6 7%	43	28.6 7%
Hacked accounts and mobile	11	7.3 3%	15	10%	50	33.3 3%	40	26.6 7%	34	22.6 7%

apps (like Phone pay, Gpay.,et c.)										
Spam	9	6%	15	10%	36	26%	55	36.6	7%	23.3
Cash send fraud	8	5.3	19	12.6	38	25.3	47	29.3	3%	25.3

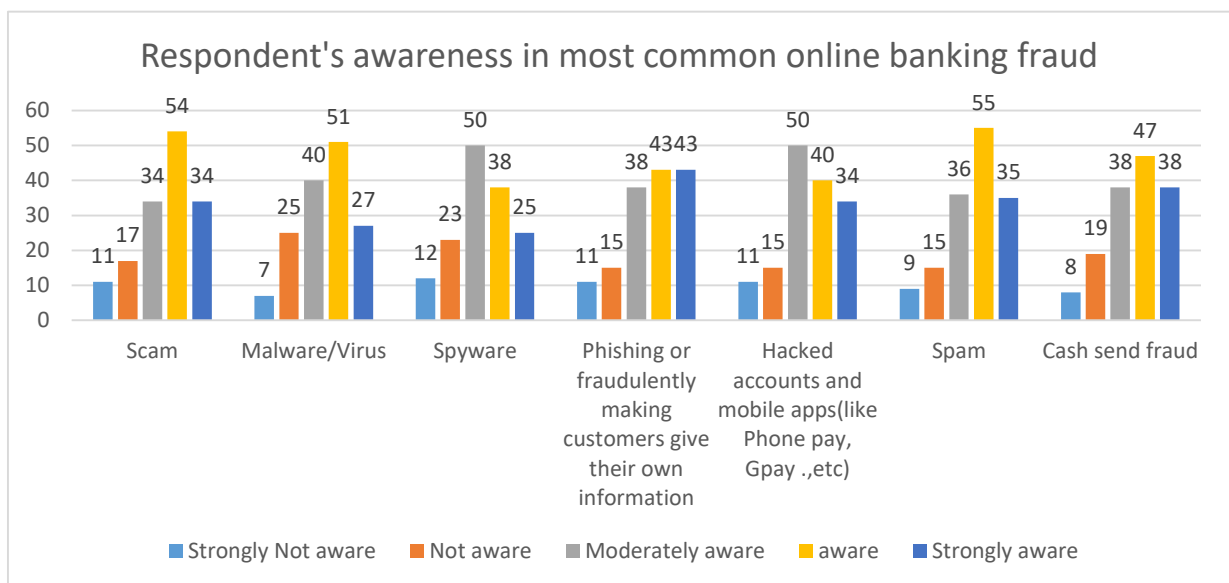


Chart 4.1.19 respondent's awareness in most common online banking fraud

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that

- 7.33% of respondents strongly not aware of most common online banking fraud scam, 11.33% of respondents not aware of most common online banking fraud scam, 22.67% of respondents moderately aware of most common online banking fraud scam, 36% of respondents aware of most

- common online banking fraud scam and 22.67% of respondents strongly aware of most common online banking fraud scam.
- 4.67% of respondents strongly Not aware of most common online banking fraud malware/virus, 16.67% of respondents Not aware of most common online banking fraud malware/virus, 26.67% of respondents Moderately aware of most common online banking fraud malware/virus, 34% of respondents aware of most common online banking fraud malware/virus and 18% of respondents strongly aware of most common online banking fraud malware/virus.
 - 8% of respondents strongly Not aware of most common online banking fraud spyware, 15.33% of respondents Not aware of most common online banking fraud spyware, 33.33% of respondents Moderately aware of most common online banking fraud spyware, 25.33% of respondents aware of most common online banking fraud spyware and 16.67% of respondents strongly aware of most common online banking fraud spyware.
 - 7.33% of respondents strongly Not aware of most common online banking fraud phishing or fraudulently making customers give their own information, 10% of respondents Not aware of most common online banking fraud phishing or fraudulently making customers give their own information, 25.33% of respondents Moderately aware of most common online banking fraud phishing or fraudulently making customers give their own information, 28.67% of respondents aware of most common online banking fraud phishing or fraudulently making customers give their own information and 28.67% of respondents strongly aware of most common online banking fraud phishing or fraudulently making customers give their own information.
 - 7.33% of respondents strongly Not aware of most common online banking fraud hacked accounts and mobile apps (like phone pay, G-pay., etc.), 10% of respondents Not aware of most common online banking fraud hacked accounts and mobile apps (like phone pay, G-pay., etc.), 33.33% of respondents Moderately aware of most common online banking fraud hacked accounts and mobile apps (like phone pay, G-pay., etc.), 26.67% of respondents aware of most common online banking fraud hacked accounts and mobile apps (like phone pay, G-pay., etc.) and 22.67% of respondents

strongly aware of most common online banking fraud hacked accounts and mobile apps (like phone pay, G-pay., etc.).

- 6% of respondents strongly Not aware of most common online banking fraud spam, 10% of respondents Not aware of most common online banking fraud spam, 26% of respondents Moderately aware of most common online banking fraud spam, 36.67% of respondents aware of most common online banking fraud spam and 23.33% of respondents strongly aware of most common online banking fraud spam.
- 5.33% of respondents strongly Not aware of most common online banking fraud cash send fraud, 12.67% of respondents Not aware of most common online banking fraud cash send fraud, 25.33% of respondents Moderately aware of most common online banking fraud cash send fraud, 29.33% of respondents aware of most common online banking fraud cash send fraud and 25.33% of respondents strongly aware of most common online banking fraud cash send fraud.

INFERENCE:

- Majority 36% of respondents aware of most common online banking fraud scam.
- Majority 34% of respondents aware of most common online banking fraud malware/virus.
- Majority 33.33% of respondents moderately aware of most common online banking fraud spyware.
- Majority 28.67% of respondents both aware and strongly aware of most common online banking fraud phishing or fraudulently making customers give their own information.
- Majority 33.33% of respondents moderately aware of most common online banking fraud hacked accounts and mobile apps (like phone pay, G-pay., etc.).
- Majority 36.67% of respondents aware of most common online banking fraud spam.
- Majority 29.33% of respondents aware of most common online banking fraud cash send fraud.

Table 4.1.20 respondent's awareness in security instructions

Aware of these security instructions	Strongly Not aware	%	Not aware	%	Moderately aware	%	aware	%	Strongly aware	%
Use smart verified app only	12	8%	16	10.67%	47	31.33%	46	30.67%	29	19.33%
Browse secure and authorized apps only	5	3.33%	21	14%	49	32.67%	43	28.67%	32	21.33%
Never share sensitive personal information	8	5.33%	11	7.33%	35	23.33%	33	22%	63	42%
Do not respond to unsolicited calls SMS or E-mails	8	5.33%	5	3.33%	36	26%	60	40%	41	27.33%
Be vigilant when	7	4.67%	8	5.33%	32	21.33%	60	40%	43	28.67%

using the card										
Keep your password secret	6	4%	6	4%	34	22.6 7%	38	25.3 3%	66	44%
keep financial data separate	8	5.3 3%	11	7.33 %	35	23.3 3%	55	36.6 7%	41	27.3 3%
keep your computer and mobile devices up to date	6	4%	7	4.67 %	47	31.3 3%	49	32.6 7%	41	27.3 3%

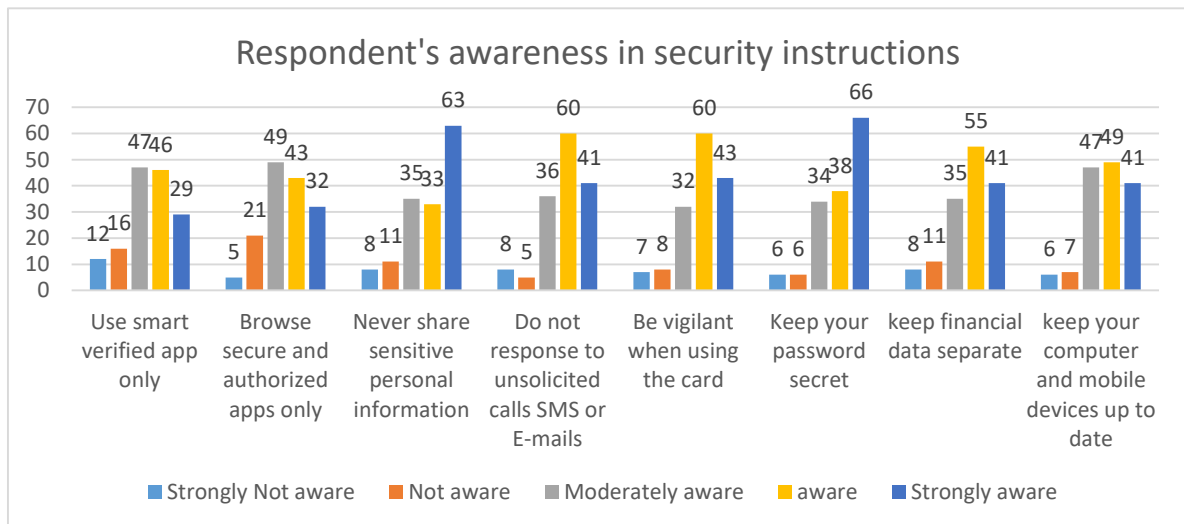


Chart 4.1.20 respondent's awareness in security instructions

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that

- 8% of respondents strongly Not aware of security instruction use smart verified app only, 10.67% of respondents Not aware of security instruction use smart verified app only, 31.33% of respondents Moderately aware of security instruction use smart verified app only, 30.67% of respondents aware of security instruction use smart verified app only and 19.33% of respondents strongly aware of security instruction use smart verified app only.
- 3.33% of respondents strongly Not aware of security instruction browse secure and authorized apps only, 14% of respondents Not aware of security instruction browse secure and authorized apps only, 32.67% of respondents Moderately aware of security instruction browse secure and authorized apps only, 28.67% of respondents aware of security instruction browse secure and authorized apps only and 21.33% of respondents strongly aware of security instruction browse secure and authorized apps only.
- 5.33% of respondents strongly Not aware of security instruction never share personal information, 7.33% of respondents Not aware of security instruction never share personal information, 23.33% of respondents Moderately aware of security instruction never share personal information, 22% of respondents aware of security instruction never share personal information and 42% of respondents strongly aware of security instruction never share personal information.
- 5.33% of respondents strongly Not aware of security instruction do not response to unsolicited calls SMS or E-mails, 3.33% of respondents Not aware of security instruction do not response to unsolicited calls SMS or E-mails, 26% of respondents Moderately aware of security instruction do not response to unsolicited calls SMS or E-mails, 40% of respondents aware of security instruction do not response to unsolicited calls SMS or E-mails and 27.33% of respondents strongly aware of security instruction do not response to unsolicited calls SMS or E-mails.
- 4.67% of respondents strongly Not aware of security instruction be vigilant when using the card, 5.33% of respondents Not aware of security instruction be vigilant when using the card, 21.33% of respondents Moderately aware of security instruction be vigilant when using the card, 40% of respondents

aware of security instruction be vigilant when using the card and 28.67% of respondents strongly aware of security instruction be vigilant when using the card.

- 4% of respondents strongly Not aware of security instruction keep your password secret, 4% of respondents Not aware of security instruction keep your password secret, 22.67% of respondents Moderately aware of security instruction keep your password secret, 25.33% of respondents aware of security instruction keep your password secret and 44% of respondents strongly aware of security instruction keep your password secret.
- 5.33% of respondents strongly Not aware of security instruction keep your financial data separate, 7.33% of respondents Not aware of security instruction keep your financial data separate, 23.33% of respondents Moderately aware of security instruction keep your financial data separate, 36.67% of respondents aware of security instruction keep your financial data separate and 27.33% of respondents strongly aware of security instruction keep your financial data separate.
- 4% of respondents strongly Not aware of security instrument keep your computer and mobile phone device up to date, 4.67% of respondents Not aware of security instrument keep your computer and mobile phone device up to date, 31.33% of respondents Moderately aware of security instrument keep your computer and mobile phone device up to date, 32.67% of respondents aware of security instrument keep your computer and mobile phone device up to date and 27.33% of respondents strongly aware of security instrument keep your computer and mobile phone device up to date.

INFERENCE:

- Majority 31.33% of respondents moderately aware of security instruction use smart verified app only.
- Majority 32.67% of respondents moderately aware of security instruction browse secure and authorized apps only.
- Majority 42% of respondents strongly aware of security instruction never share personal information.
- Majority 40% of respondents aware of security instruction do not response to unsolicited calls SMS or E-mails.

- Majority 40% of respondents aware of security instruction be vigilant when using the card.
- Majority 44% of respondents strongly aware of security instruction keep your password secret.
- Majority 36.67% of respondents aware of security instruction keep your financial data separate.
- Majority 32.67% of respondents aware of security instrument keep your computer and mobile phone device up to date.

Table 4.1.21 respondent's awareness in bank instructions

Aware of these bank instructions	Strongly Not aware	%	Not aware	%	Moderately aware	%	aware	%	Strongly aware	%
Do not share your ATM Pin number	14	9.33 %	4	2.67 %	19	12.6 7%	37	24.6 7%	76	50.6 7%
Do not share your CVV number	11	7.33 %	10	6.67 %	18	12% 35	35	23.3 3%	76	50.6 7%
Do not share your OTP number	10	6.67 %	5	3.33 %	22	14.6 7%	43	28.6 7%	70	46.6 7%
Do not share your personal information about your bank account to others	8	5.33 %	5	3.33 %	24	16% 34	34	22.6 7%	79	52.6 7%

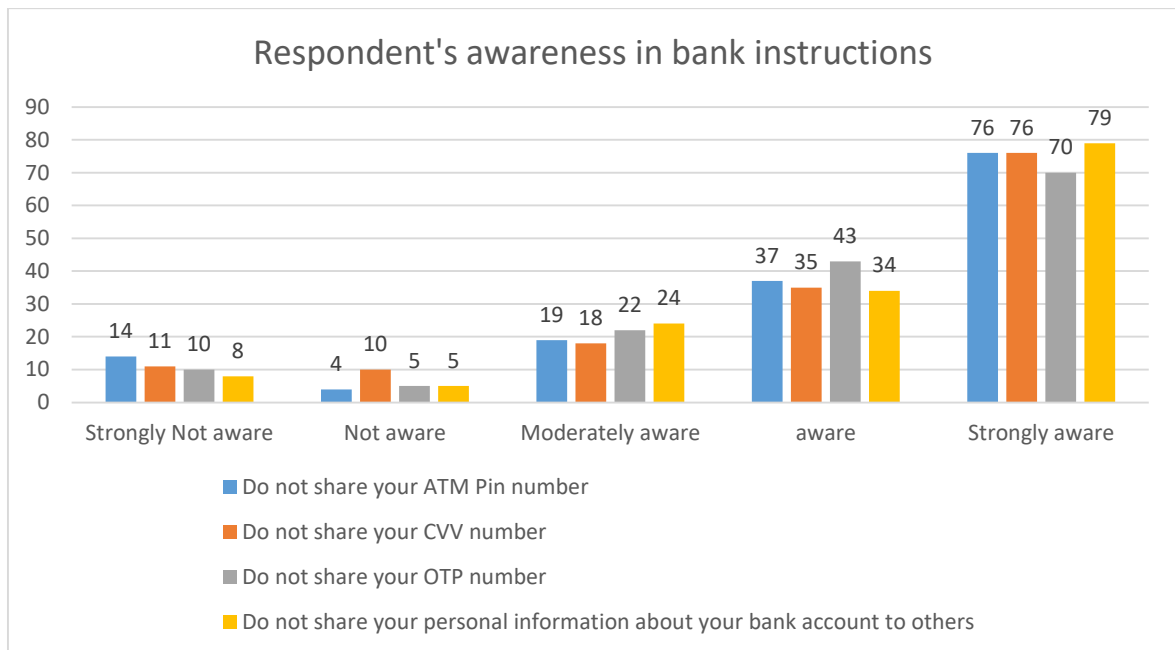


Chart 4.1.21 respondent's awareness in bank instructions

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that

- 9.33% of respondents strongly not aware of bank instruction do not share your ATM Pin number, 2.67% of respondents not aware of bank instruction Do not share your ATM Pin number, 12.67% of respondents moderately aware of bank instruction Do not share your ATM Pin number, 24.67% of respondents aware of bank instruction Do not share your ATM Pin number and 50.67% of respondents strongly aware of bank instruction Do not share your ATM Pin number.
- 7.33% of respondents strongly not aware of bank instruction Do not share your CVV number, 6.67% of respondents not aware of bank instruction Do not share your CVV number, 12% of respondents moderately aware of bank instruction Do not share your CVV number, 23.33% of respondents aware of bank instruction Do not share your CVV number and 50.67% of respondents strongly aware of bank instruction Do not share your CVV number.
- 6.67% of respondents strongly not aware of bank instruction Do not share your OTP number, 3.33% of respondents not aware of bank instruction Do not share your OTP number, 14.67% of respondents moderately aware of

bank instruction Do not share your OTP number, 28.67% of respondents aware of bank instruction Do not share your OTP number and 46.67% of respondents strongly aware of bank instruction Do not share your OTP number.

- 5.33% of respondents strongly not aware of bank instruction Do not share your personal information about your bank account to others, 3.33% of respondents not aware of bank instruction Do not share your personal information about your bank account to others, 16% of respondents moderately aware of bank instruction Do not share your personal information about your bank account to others, 22.67% of respondents aware of bank instruction Do not share your personal information about your bank account to others and 52.67% of respondents strongly aware of bank instruction Do not share your personal information about your bank account to others.

INFERENCE:

- Majority 50.67% of respondents strongly aware of bank instruction do not share your ATM Pin number.
- Majority 50.67% of respondents strongly aware of bank instruction do not share your CVV number.
- Majority 46.67% of respondents strongly aware of bank instruction do not share your OTP number.
- Majority 52.67% of respondents strongly aware of bank instruction do not share your personal information about your bank account to others.

Table 4.1.22 respondent's rating in bank's mode of communication to increase awareness in online banking fraud

Mode of communication	1	%	2	%	3	%	4	%	5	%
In the branch	27	18%	16	10.67%	36	26%	36	26%	35	23.33%
By E-mail	18	12%	22	14.67%	41	27.33%	32	21.33%	37	24.67%
By telephone	17	11.33%	15	10%	50	33.33%	30	20%	38	25.33%
On bank website	16	10.67%	9	6%	34	22.67%	49	32.67%	42	28%
By letter from the bank	23	15.33%	16	10.67%	31	20.67%	35	23.33%	45	30%

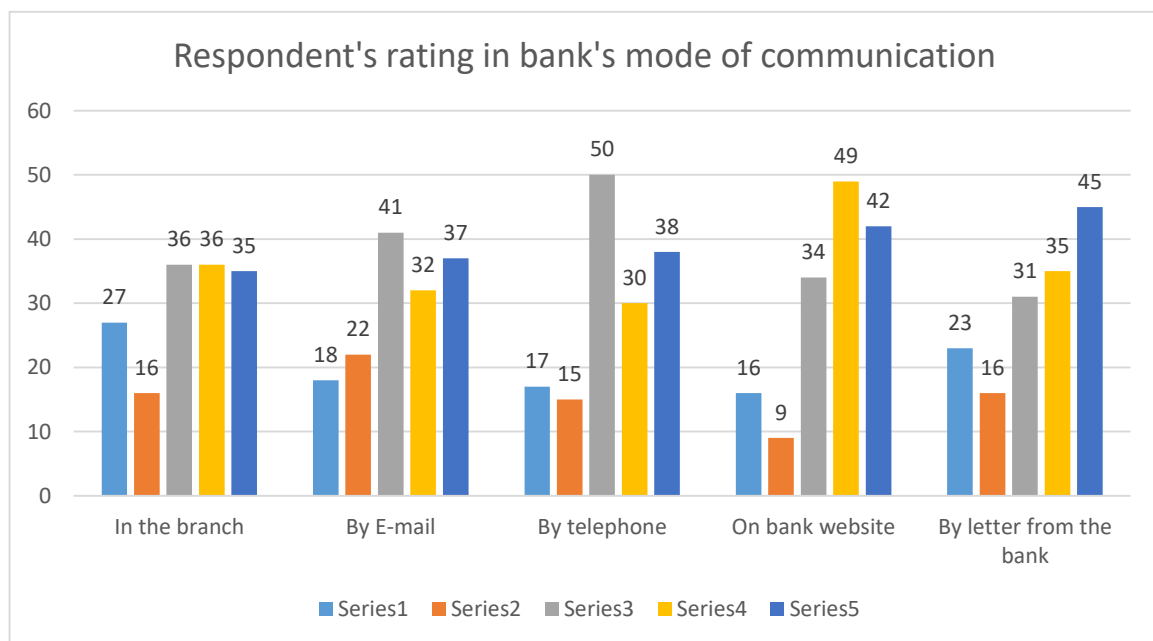


Chart 4.1.22 respondent's rating in bank's mode of communication to increase awareness in online banking fraud

INTERPRETATION:

From the above table total respondents is 150 and from the above table it is interpreted that

- For increase online fraud awareness bank communicate customer in the branch for that mode of communication 18% of the respondents rated 1, 10.67% of respondents rated 2, 26% of respondents rated 3, 26% of respondents rated 4, 23.33% of respondents rated 5.
- For increase online fraud awareness bank communicate customer by E-mail for that mode of communication 12% of the respondents rated 1-Not at all useful, 14.67% of respondents rated 2, 27.33% of respondents rated 3, 21.33% of respondents rated 4, 24.67% of respondents rated 5.
- For increase online fraud awareness bank communicate customer by telephone for that mode of communication 11.33% of the respondents rated 1, 10% of respondents rated 2, 33.33% of respondents rated 3, 20% of respondents rated 4, 25.33% of respondents rated 5.
- For increase online fraud awareness bank communicate customer on bank website for that mode of communication 10.67% of the respondents rated 1, 6% of respondents rated 2, 22.67% of respondents rated 3, 32.67% of respondents rated 4, 28% of respondents rated 5.
- For increase online fraud awareness bank communicate customer by letter from the bank for that mode of communication 15.33% of the respondents rated 1, 10.67% of respondents rated 2, 20.67% of respondents rated 3, 23.33% of respondents rated 4, 30% of respondents rated 5.

INFERENCE:

- Majority 26% of respondents rated both 3&4 for increase online fraud awareness bank communicate customer in the branch.
- Majority 27.33% of respondents rated 3 for increase online fraud awareness bank communicate customer by E-mail.
- Majority 33.33% of respondents rated 3 for increase online fraud awareness bank communicate customer by telephone.
- Majority 32.67% of respondents rated 4 for increase online fraud awareness bank communicate customer on bank website.
- Majority 30% of respondents rated 5 for increase online fraud awareness bank communicate customer by letter from the bank.

4.2 ONE SAMPLE T-TEST

4.2.1 Respondent's rating in awareness on online fraud vs test value 3

Null Hypothesis (H0): There is no significant difference between the mean Respondent's rating in awareness on online fraud are equal to average level.

Alternate Hypothesis (H1): There is significant difference between the mean Respondent's rating in awareness on online fraud are not equal to average level.

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
E-mail	150	3.14	1.321	.108
Text messages	150	3.68	1.200	.098
Website advertisements	150	3.35	1.275	.104
Telephone (Mobile phone)	150	3.62	1.213	.099
Redirect website page	150	3.34	1.268	.104
Downloaded software	150	3.37	1.223	.100

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
E-mail	1.298	149	.196	.140	-.07	.35
Text messages	6.939	149	.000	.680	.49	.87
Website advertisements	3.394	149	.001	.353	.15	.56
Telephone (Mobile phone)	6.259	149	.000	.620	.42	.82
Redirect website page	3.283	149	.001	.340	.14	.54
Downloaded software	3.672	149	.000	.367	.17	.56

INTERPRETATION:

Since P value is less than 0.05, the null hypothesis is rejected at 5% level of significance with regard to awareness on online fraud (text messages, website advertisements, telephone (mobile phone), redirect website page and downloaded

software). Hence the rating regard to awareness on online fraud is not equal to average level. Based on mean score, rating regard to awareness on online fraud (text messages, website advertisements, telephone (mobile phone), redirect website page and downloaded software) is above average level. Hence respondents aware of these online frauds.

Since P value is greater than 0.05, the null hypothesis is accepted at 5% level of significance with regard to awareness on online fraud (E-mail). Hence the rating regard to awareness on online fraud is equal to average level. Based on mean score, rating regard to awareness on online fraud (E-mail) is equal to average level. Hence respondents moderately aware of this online frauds

INFERENCE:

The respondent's mostly aware of online frauds like text messages, website advertisements, telephone (mobile phone), redirect website page and downloaded software. The respondent's mostly moderately aware of fraud send through E-mail.

4.2.2 Respondent's level of agreement with statements vs test value 3

Null Hypothesis (H0): There is no significant difference between the mean Respondent's rating in level of agreement with statements are equal to average level.

Alternate Hypothesis (H1): There is significant difference between the mean Respondent's rating in level of agreement with statements are not equal to average level.

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
I am aware of the risks from online banking	150	3.66	1.110	.091
My bank provides free anti-virus for my online banking	150	2.89	1.094	.089
My bank provides adequate support against online fraud	150	3.35	.949	.078

One-Sample Test

	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I am aware of the risks from online banking	7.281	149	.000	.660	.48	.84
My bank provides free anti-virus for my online banking	-1.194	149	.234	-.107	-.28	.07
My bank provides adequate support against online fraud	4.559	149	.000	.353	.20	.51

INTERPRETATION:

Since P value is less than 0.05, the null hypothesis is rejected at 5% level of significance with regard to level of agreement with statement (I am aware of the risks from online banking, my bank provides adequate support). Hence the rating regard to awareness on online fraud is not equal to average level. Based on mean score, rating regard to awareness on online fraud (I am aware of the risks from online banking, my bank provides adequate support) is above average level. Hence respondents agree with the statements.

Since P value is greater than 0.05, the null hypothesis is accepted at 5% level of significance with regard to awareness on online fraud (my bank provides free anti-virus for my online banking). Hence the rating regard to awareness on online fraud is equal to average level. Based on mean score, rating regard to awareness on online fraud (my bank provides free anti-virus for my online banking) is equal to average level. Hence respondents moderate with the statement.

INFERENCE:

The respondent's mostly agree with the statements I am aware of the risks from online banking, my bank provides adequate support. The respondent's mostly moderate with the statement my bank provides free anti-virus for my online banking.

4.2.3 Respondent's degree of agreement on statements vs test value 3

Null Hypothesis (H0): There is no significant difference between the mean Respondent's rating in degree of agreement with statements are equal to average level.

Alternate Hypothesis (H1): There is significant difference between the mean Respondent's rating in degree of agreement with statements are not equal to average level.

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
Do you agree that the information provided by your bank about online fraud awareness is adequate	150	3.19	1.066	.087
Do you need more awareness about online fraud risk	150	3.66	1.067	.087

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Do you agree that the information provided by your bank about online fraud awareness is adequate	2.221	149	.028	.193	.02	.37
Do you need more awareness about online fraud risk	7.575	149	.000	.660	.49	.83

INTERPRETATION:

Since P value is less than 0.05, the null hypothesis is rejected at 5% level of significance with regard to degree of agreement with statement (do you need more awareness about online fraud risk). Hence the rating regard to awareness on online

fraud is not equal to average level. Based on mean score, rating regard to awareness on online fraud (do you need more awareness about online fraud risk) is above average level. Hence respondents agree with the statements.

Since P value is greater than 0.05, the null hypothesis is accepted at 5% level of significance with regard to awareness on online fraud (do you agree that the information provided by your bank about online fraud awareness is adequate). Hence the rating regard to awareness on online fraud is equal to average level. Based on mean score, rating regard to awareness on online fraud (do you agree that the information provided by your bank about online fraud awareness is adequate) is equal to average level. Hence respondents moderate with the statement.

INFERENCE:

The respondent's mostly agree with the statements do you need more awareness about online fraud risk. The respondent's mostly moderate with the statement do you agree that the information provided by your bank about online fraud awareness is adequate.

4.2.4 Respondent's awareness rating on most common online banking fraud vs test value 3

Null Hypothesis (H0): There is no significant difference between the mean Respondent's awareness rating on most common online banking fraud are equal to average level.

Alternate Hypothesis (H1): There is significant difference between the mean Respondent's awareness rating on most common online banking fraud are not equal to average level.

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
Scam	150	3.55	1.173	.096
Malware/Virus	150	3.44	1.108	.090
Spyware	150	3.26	1.161	.095
Phishing or fraudulently making customers give their own information	150	3.61	1.208	.099

Hacked accounts and mobile apps(like Phone pay, Gpay .,etc)	150	3.47	1.163	.095
Spam	150	3.61	1.128	.092
Cash send fraud	150	3.59	1.154	.094

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Scam	5.777	149	.000	.553	.36	.74
Malware/Virus	4.863	149	.000	.440	.26	.62
Spyware	2.743	149	.007	.260	.07	.45
Phishing or fraudulently making customers give their own information	6.216	149	.000	.613	.42	.81
Hacked accounts and mobile apps(like Phone pay, G-pay .,etc.)	4.986	149	.000	.473	.29	.66
Spam	6.660	149	.000	.613	.43	.80
Cash send fraud	6.227	149	.000	.587	.40	.77

INTERPRETATION:

Since P value is less than 0.05, the null hypothesis is rejected at 5% level of significance with regard to awareness on most common online banking fraud (scam, malware/virus, spyware, phishing or fraudulently making customers give their own information, hacked accounts and mobile apps (like phone pay, G-pay., etc.), spam, cash send fraud). Hence the rating regard to awareness on most common online banking fraud is not equal to average level. Based on mean score, rating regard to awareness on online fraud (scam, malware/virus, spyware, phishing or fraudulently making customers give their own information, hacked accounts and mobile apps (like phone pay, G-pay., etc.), spam, cash send fraud) is above average level. Hence respondents aware of these most common online banking fraud.

INFERENCE:

The respondent's mostly aware of most common online banking fraud like scam, malware/virus, spyware, phishing or fraudulently making customers give their own information, hacked accounts and mobile apps (like phone pay, G-pay., etc.), spam, cash send fraud.

4.2.5 Respondent's awareness ratings on security instruction tips vs test value 3

Null Hypothesis (H0): There is no significant difference between the mean Respondent's awareness ratings on security instruction tips are equal to average level.

Alternate Hypothesis (H1): There is significant difference between the mean Respondent's awareness ratings on security instruction tips are not equal to average level.

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
Use smart verified app only	150	3.43	1.155	.094
Browse secure and authorized apps only	150	3.51	1.079	.088
Never share sensitive personal information	150	3.88	1.192	.097
Do not response to unsolicited calls SMS or E-mails	150	3.81	1.047	.086
Be vigilant when using the card	150	3.83	1.054	.086
Keep your password secret	150	4.01	1.093	.089
keep financial data separate	150	3.73	1.103	.090
keep your computer and mobile devices up to date	150	3.75	1.037	.085

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Use smart verified app only	4.525	149	.000	.427	.24	.61

Browse secure and authorized apps only	5.751	149	.000	.507	.33	.68
Never share sensitive personal information	9.039	149	.000	.880	.69	1.07
Do not response to unsolicited calls SMS or E-mails	9.434	149	.000	.807	.64	.98
Be vigilant when using the card	9.607	149	.000	.827	.66	1.00
Keep your password secret	11.356	149	.000	1.013	.84	1.19
keep financial data separate	8.141	149	.000	.733	.56	.91
keep your computer and mobile devices up to date	8.815	149	.000	.747	.58	.91

INTERPRETATION:

Since P value is less than 0.05, the null hypothesis is rejected at 5% level of significance with regard to security instruction tips like (use smart verified app only, browse secure and authorized apps only, never share sensitive personal information, do not response to unsolicited calls SMS or E-mails, be vigilant when using the card, keep your password secret, keep financial data separate, keep your computer and mobile devices up to date). Hence the rating regard to awareness on online fraud is not equal to average level. Based on mean score, rating regard to security instruction tips like (use smart verified app only, browse secure and authorized apps only, never share sensitive personal information, do not response to unsolicited calls SMS or E-mails, be vigilant when using the card, keep your password secret, keep financial data separate, keep your computer and mobile devices up to date) is above average level. Hence respondents aware of these security instruction tips.

INFERENCE:

The respondent's mostly aware of security instructions like text messages, website advertisements, telephone (mobile phone), redirect website page and downloaded software. use smart verified app only, browse secure and authorized apps only, never share sensitive personal information, do not response to unsolicited calls SMS

or E-mails, be vigilant when using the card, keep your password secret, keep financial data separate, keep your computer and mobile devices up to date.

4.2.6 Respondent's awareness ratings on bank instructions vs test value 3

Null Hypothesis (H0): There is no significant difference between the mean Respondent's awareness ratings on bank instructions are equal to average level.

Alternate Hypothesis (H1): There is significant difference between the mean Respondent's awareness ratings on bank instructions are not equal to average level.

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
Do not share your ATM Pin number	150	4.05	1.260	.103
Do not share your CVV number	150	4.03	1.250	.102
Do not share your OTP number	150	4.05	1.163	.095
Do not share your personal information about your bank account to others	150	4.14	1.135	.093

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Do not share your ATM Pin number	10.171	149	.000	1.047	.84	1.25
Do not share your CVV number	10.124	149	.000	1.033	.83	1.24
Do not share your OTP number	11.091	149	.000	1.053	.87	1.24
Do not share your personal information about your bank account to others	12.298	149	.000	1.140	.96	1.32

INTERPRETATION:

Since P value is less than 0.05, the null hypothesis is rejected at 5% level of significance with regard to bank instructions like (Do not share your ATM pin number, do not share your CVV number, do not share your OTP number, do not share your personal information about your bank account to others). Hence the rating regard to bank instructions like is not equal to average level. Based on mean score, rating regard to bank instructions like (Do not share your ATM pin number, do not share your CVV number, do not share your OTP number, and do not share your personal information about your bank account to others) is above average level. Hence respondents aware of these bank instructions.

INFERENCE:

The respondent's mostly aware of bank instructions like do not share your ATM pin number, do not share your CVV number, do not share your OTP number, and do not share your personal information about your bank account to others.

4.1.7 Respondent's ratings on mode of communication from bank to them to increase their level of awareness in online fraud vs test value 3

Null Hypothesis (H0): There is no significant difference between the mean Respondent's ratings on mode of communication from bank to them to increase their level of awareness in online fraud are equal to average level.

Alternate Hypothesis (H1): There is significant difference between the mean Respondent's ratings on mode of communication from bank to them to increase their level of awareness in online fraud are not equal to average level.

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
In the branch	150	3.24	1.398	.114
By E-mail	150	3.32	1.318	.108
By telephone	150	3.38	1.278	.104
On bank website	150	3.61	1.252	.102
By letter from the bank	150	3.42	1.411	.115

One-Sample Test	
	Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In the branch	2.102	149	.037	.240	.01	.47
By E-mail	2.975	149	.003	.320	.11	.53
By telephone	3.642	149	.000	.380	.17	.59
On bank website	6.000	149	.000	.613	.41	.82
By letter from the bank	3.646	149	.000	.420	.19	.65

INTERPRETATION:

Since P value is less than 0.05, the null hypothesis is rejected at 5% level of significance with regard to mode of communication from bank to them to increase their level of awareness in online fraud (By E-mail, by telephone, on bank website, by letter from the bank). Hence the rating regard to mode of communication from bank to them to increase their level of awareness in online fraud (By E-mail, by telephone, on bank website, by letter from the bank) is above average level. Hence respondents rated more than 3 for the mode of communication through bank to increase awareness of online fraud to them.

Since P value is greater than 0.05, the null hypothesis is accepted at 5% level of significance with regard to mode of communication from bank to them to increase their level of awareness in online fraud (In the branch). Hence the rating mode of communication from bank to them to increase their level of awareness in online fraud is equal to average level. Based on mean score, rating regard to awareness on online fraud (In the branch) is equal to average level. Hence respondents rated 3 for the mode of communication through bank to increase awareness of online fraud to them

INFERENCE:

The respondent's mostly rated more than 3 for the mode of communication from bank through E-mail, telephone, bank website and letter from the bank to increase

awareness of online fraud to them. The respondent's mostly rated 3 for the mode of communication from bank through branch to increase awareness of online fraud to them.

4.3 INDEPENDENT SAMPLE T-TEST

4.3.1 Respondent's rating in how much them aware on online frauds vs gender of the respondents

Null Hypothesis (H0): There is no significant difference between Male and Female with respect to the rating in how much them aware on online frauds by the respondents.

Alternate Hypothesis (H1): There is significant difference between Male and Female with respect to the rating in how much them aware on online frauds by the respondents.

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Respondent's rating in how much them aware on online frauds	Male	93	20.2581	6.53237	.67737
	Female	57	20.8947	6.40224	.84800

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	Df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Respondent's rating in how much them aware on online frauds	Equal variances assumed	.000	.998	-.584	148	.560	-.63667	1.09062	-2.79186	1.51852
	Equal variances not assumed			-.587	120.421	.559	-.63667	1.08533	-2.78547	1.51213

INTERPRETATION:

Since p value is greater than 0.05, the null hypothesis is accepted at the significant level with respect to the rating in how much they are aware of online frauds. Hence, there is no significant difference between male and female with respect to the rating in how much they are aware of online frauds by the respondents.

INFERENCE:

There are no differences between male and female respondents' perception towards how much they are aware of online frauds.

4.3.2 Respondent's level of agreement with statements vs gender of the respondents

Null Hypothesis (H0): There is no significant difference between Male and Female with respect to the rating on the level of agreement with statements by the respondents.

Alternate Hypothesis (H1): There is significant difference between Male and Female with respect to the rating on the level of agreement with statements by the respondents.

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Respondent's level of agreement with statements	Male	93	9.7312	2.70322	.28031
	Female	57	10.1930	2.29470	.30394

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	Df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Respondent's level of agreement	Equal variances assumed	.223	.637	-1.074	148	.285	-.46180	.43002	-1.31156	.38796

with statements	Equal variances not assumed			-1.117	133.144	.266	-.46180	.41347	-1.27961	.35601
-----------------	-----------------------------	--	--	--------	---------	------	---------	--------	----------	--------

INTERPRETATION:

Since p value is greater than 0.05, the null hypothesis is accepted at the significant level with respect to the rating on the level of agreement with statements. Hence, there is no significant difference between male and female with respect to the rating on the level of agreement with statements by the respondents.

INFERENCE:

There is no differences between male and female respondent's perception towards level of agreement with statements.

4.3.3 Respondent's degree of agreement on statements vs gender of the respondents

Null Hypothesis (H0): There is no significant difference between Male and Female with respect to the rating on the degree of agreement on statements by the respondents.

Alternate Hypothesis (H1): There is significant difference between Male and Female with respect to the rating on the degree of agreement on statements by the respondents.

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Respondent's degree of agreement on statements	Male	93	6.8495	1.97785	.20509
	Female	57	6.8596	1.66303	.22027

Independent Samples Test									
		Levene's Test for Equality of Variances		t-test for Equality of Means					
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference Lower Upper

Respondent's degree of agreement on statements	Equal variances assumed	2.254	.135	-.032	148	.974	-.01019	.31372	-.63014	.60976
	Equal variances not assumed			-.034	133.919	.973	-.01019	.30097	-.60546	.58508

INTERPRETATION:

Since p value is greater than 0.05, the null hypothesis is accepted at the significant level with respect to the rating on the degree of agreement on statements. Hence, there is no significant difference between male and female with respect to the rating on the degree of agreement on statements by the respondents.

INFERENCE:

There is no differences between male and female respondent's perception towards degree of agreement on statements.

4.3.4 Respondent's awareness rating on most common online banking frauds vs gender of the respondents

Null Hypothesis (H0): There is no significant difference between Male and Female with respect to the awareness rating on most common online banking frauds by the respondents.

Alternate Hypothesis (H1): There is significant difference between Male and Female with respect to the awareness rating on most common online banking frauds by the respondents.

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Respondent's awareness rating on most common online banking frauds	Male	93	25.0430	7.38964	.76627
	Female	57	23.7193	6.64604	.88029

Independent Samples Test		
	Levene's Test for Equality of Variances	t-test for Equality of Means

		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Respondent's awareness rating on most common online banking frauds	Equal variances assumed	.265	.607	1.106	148	.271	1.32371	1.19726	-1.04222	3.68965
	Equal variances not assumed			1.134	128.211	.259	1.32371	1.16708	-.98552	3.63295

INTERPRETATION:

Since p value is greater than 0.05, the null hypothesis is accepted at the significant level with respect to awareness rating on most common online banking frauds. Hence, there is no significant difference between male and female with respect to the awareness rating on most common online banking frauds by the respondents.

INFERENCE:

There is no differences between male and female respondent's perception towards most common online banking frauds.

4.3.5 Respondent's awareness rating on security instruction tips vs gender of the respondents

Null Hypothesis (H0): There is no significant difference between Male and Female with respect to the awareness rating on security instruction tips by the respondents.

Alternate Hypothesis (H1): There is significant difference between Male and Female with respect to the awareness rating on security instruction tips by the respondents.

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Respondent's awareness rating on security instruction tips	Male	93	29.5806	8.41107	.87219
	Female	57	30.5263	6.33332	.83887

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Respondent's awareness rating on security instruction tips	Equal variances assumed	3.495	.064	-.731	148	.466	-.94567	1.29378	-3.50234	1.61100
	Equal variances not assumed			-.781	141.712	.436	-.94567	1.21013	-3.33791	1.44657

INTERPRETATION:

Since p value is greater than 0.05, the null hypothesis is accepted at the significant level with respect to the awareness rating on security instruction tips. Hence, there is no significant difference between Male and Female with respect to the awareness rating on security instruction tips by the respondents.

INFERENCE:

There is no differences between male and female respondent's perception towards security instruction tips.

4.3.6 Respondent's awareness rating on bank instructions vs gender of the respondents

Null Hypothesis (H0): There is no significant difference between Male and Female with respect to the awareness rating on bank instructions by the respondents.

Alternate Hypothesis (H1): There is significant difference between Male and Female with respect to the awareness rating on bank instructions by the respondents.

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Respondent's awareness rating on bank instructions	Male	93	16.1075	4.72151	.48960
	Female	57	16.5439	4.59064	.60804

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Respondent's awareness rating on bank instructions	Equal variances assumed	.477	.491	-.555	148	.580	-.43633	.78597	-1.98952	1.11685
	Equal variances not assumed			-.559	121.155	.577	-.43633	.78066	-1.98183	1.10916

INTERPRETATION:

Since p value is greater than 0.05, the null hypothesis is accepted at the significant level with respect to the awareness rating on bank instructions. Hence, there is no significant difference between Male and Female with respect to the awareness rating on bank instructions by the respondents.

INFERENCE:

There is no differences between male and female respondent's perception towards bank instructions.

4.3.7 Respondents rating on mode of communication from bank to them to increase their level of awareness in online fraud vs gender of the respondents

Null Hypothesis (H0): There is no significant difference between Male and Female with respect to the rating on mode of communication from bank to them to increase their level of awareness in online fraud by the respondents.

Alternate Hypothesis (H1): There is significant difference between Male and Female with respect to the rating on mode of communication from bank to them to increase their level of awareness in online fraud by the respondents.

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
	Male	93	17.6237	5.25215	.54462

Respondents rating on mode of communication from bank to them to increase their level of awareness in online fraud	Female	57	15.9123	5.88364	.77931
--	--------	----	---------	---------	--------

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Respondents rating on mode of communication from bank to them to increase their level of awareness in online fraud	Equal variances assumed	.842	.360	1.850	148	.066	1.71138	.92512	-.11678	3.53953
	Equal variances not assumed			1.800	108.330	.075	1.71138	.95075	-.17312	3.59587

INTERPRETATION:

Since p value is greater than 0.05, the null hypothesis is accepted at the significant level with respect to the rating on mode of communication from bank to them to increase their level of awareness in online fraud. Hence, there is no significant difference between Male and Female with respect to the rating on mode of communication from bank to them to increase their level of awareness in online fraud by the respondents.

INFERENCE:

There is no differences between male and female respondent's perception towards mode of communication from bank to them to increase their level of awareness in online fraud.

4.4 ONE-WAY ANOVA

4.4.1 Respondent's awareness rating on most common online banking frauds vs Age of the respondents

Null Hypothesis (H₀): There is no significant difference among age groups with respect to the awareness rating on most common online banking frauds by the respondents.

Alternate Hypothesis (H₁): There is significant difference among age groups with respect to the awareness rating on most common online banking frauds by the respondents.

Descriptives								
Respondent's awareness rating on most common online banking frauds								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
18-20	8	24.2500	8.03119	2.83945	17.5358	30.9642	7.00	34.00
20-30	83	26.5663	6.17073	.67733	25.2188	27.9137	7.00	35.00
30-40	14	21.0714	6.46249	1.72717	17.3401	24.8028	12.00	34.00
40-50	29	20.6552	6.99120	1.29823	17.9959	23.3145	7.00	34.00
Above 50	16	24.2500	8.66025	2.16506	19.6353	28.8647	7.00	35.00
Total	150	24.5400	7.12273	.58157	23.3908	25.6892	7.00	35.00

ANOVA					
Respondent's awareness rating on most common online banking frauds					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	948.894	4	237.224	5.204	.001
Within Groups	6610.366	145	45.589		
Total	7559.260	149			

Respondent's awareness rating on most common online banking frauds			
Duncan ^{a,b}			
		Subset for alpha = 0.05	
Age	N	1	2

40-50	29	20.6552	
30-40	14	21.0714	
18-20	8	24.2500	24.2500
Above 50	16	24.2500	24.2500
20-30	83		26.5663
Sig.		.169	.360
Means for groups in homogeneous subsets are displayed.			
a. Uses Harmonic Mean Sample Size = 16.369.			
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.			

INTERPRETATION:

Since p value (0.001) is less than 0.05, the null hypothesis is rejected at the significant level with respect to the awareness rating on most common online banking frauds by the respondents. Hence, there is no significant difference between male and female with respect to the awareness rating on most common online banking frauds by the respondents.

INFERENCE:

There is significant difference among age groups with respect to the awareness rating on most common online banking frauds by the respondents.

4.4.2 Respondent's awareness rating on security instruction tips vs Age of the respondents

Null Hypothesis (H0): There is no significant difference among age group with respect to the awareness rating on security instruction tips by the respondents.

Alternate Hypothesis (H1): There is significant difference among age group with respect to the awareness rating on security instruction tips by the respondents.

Descriptives							
Respondent's awareness rating on security instruction tips							
					95% Confidence Interval for Mean		
	N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum
							Maximum

18-20	8	29.6250	10.18314	3.60029	21.1117	38.1383	8.00	40.00
20-30	83	31.0964	6.74377	.74022	29.6238	32.5689	8.00	40.00
30-40	14	26.6429	9.09444	2.43059	21.3919	31.8938	8.00	40.00
40-50	29	28.1379	8.16668	1.51651	25.0315	31.2444	8.00	40.00
Above 50	16	30.2500	8.28251	2.07063	25.8366	34.6634	16.00	40.00
Total	150	29.9400	7.67916	.62700	28.7010	31.1790	8.00	40.00

ANOVA					
Respondent's awareness rating on security instruction tips					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	359.694	4	89.923	1.547	.192
Within Groups	8426.766	145	58.116		
Total	8786.460	149			

Respondent's awareness rating on security instruction tips		
Duncan ^{a,b}		
Age	N	Subset for alpha = 0.05
30-40	14	26.6429
40-50	29	28.1379
18-20	8	29.6250
Above 50	16	30.2500
20-30	83	31.0964
Sig.		.141
Means for groups in homogeneous subsets are displayed.		
a. Uses Harmonic Mean Sample Size = 16.369.		
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.		

INTERPRETATION:

Since p value (0.192) is greater than 0.05, the null hypothesis is accepted at the significant level with respect to the awareness rating on security instruction tips by

the respondents. Hence, there is no significant difference between Male and Female with respect to the awareness rating on security instruction tips by the respondents.

INFERENCE:

There is no significant difference among age group with respect to the awareness rating on security instruction tips by the respondents.

CHAPTER 5

FINDINGS, SUGGESTION AND CONCLUSION

5.1 FINDINGS

- Majority (62%) of respondents are male respondents.
- Majority 55.33% of respondents are 20-30 age respondent.
- Majority (64%) of the respondent's completed PG.
- Majority (60%) of the respondents are single.
- Majority (60%) of the respondents are employed.
- Majority (48.67%) of respondents frequently used online banking.
- Majority (42%) of respondents frequently used online banking to access bank account.
- Majority (59%) of respondents think online banking is important.
- Majority (82.67%) of respondents know about the online banking fraud.
- Majority (47.33%) of respondents frequently follow's bank preventive rules.
- Majority (81.33%) of respondents haven't been a victim of online banking fraud.
- Majority (58%) of respondents didn't know someone have been a victim of online banking fraud.
- Majority (79.33%) respondents never lost their money in online banking fraud.
- Majority (57.33%) of respondents didn't know about the national helpline number to report cyber-crime.
- Majority (85.33%) of respondents think that national helpline number is useful.
- Majority 24% of respondents not aware of online fraud sent through E-mail.
- Majority 32% of respondents strongly aware of online fraud sent through Text messages.
- Majority 32% of respondents moderately aware of online fraud sent through website advertisements.
- Majority 29.33% of respondents strongly aware of online fraud sent through Telephone (Mobile phone).

- Majority 25.33% of respondents aware of online fraud sent through Redirect website page.
- Majority 28% of respondents moderately aware of online fraud sent through Downloaded software.
- Majority 46% of respondents agree with the statement I am aware of the risks from online banking.
- Majority 34% of respondents are moderate with the statement my bank provides free anti-virus for my online banking.
- Majority 48% of respondents are moderate with the statement my bank provides adequate support against online fraud.
- Majority (39.33%) of the respondents are moderate with the statement Do you agree that the information provided by your bank about online fraud awareness is adequate.
- Majority (31.33%) of the respondents are moderate with the statement Do you need more awareness about online fraud risk.
- Majority 36% of respondents aware of most common online banking fraud scam.
- Majority 34% of respondents aware of most common online banking fraud malware/virus.
- Majority 33.33% of respondents moderately aware of most common online banking fraud spyware.
- Majority 28.67% of respondents both aware and strongly aware of most common online banking fraud phishing or fraudulently making customers give their own information.
- Majority 33.33% of respondents moderately aware of most common online banking fraud hacked accounts and mobile apps (like phone pay, G-pay., etc.).
- Majority 36.67% of respondents aware of most common online banking fraud spam.
- Majority 29.33% of respondents aware of most common online banking fraud cash send fraud.
- Majority 31.33% of respondents moderately aware of security instruction use smart verified app only.

- Majority 32.67% of respondents moderately aware of security instruction browse secure and authorized apps only.
- Majority 42% of respondents strongly aware of security instruction never share personal information.
- Majority 40% of respondents aware of security instruction do not response to unsolicited calls SMS or E-mails.
- Majority 40% of respondents aware of security instruction be vigilant when using the card.
- Majority 44% of respondents strongly aware of security instruction keep your password secret.
- Majority 36.67% of respondents aware of security instruction keep your financial data separate.
- Majority 32.67% of respondents aware of security instrument keep your computer and mobile phone device up to date.
- Majority 50.67% of respondents strongly aware of bank instruction do not share your ATM Pin number.
- Majority 50.67% of respondents strongly aware of bank instruction do not share your CVV number.
- Majority 46.67% of respondents strongly aware of bank instruction do not share your OTP number.
- Majority 52.67% of respondents strongly aware of bank instruction do not share your personal information about your bank account to others.
- Majority 26% of respondents rated both 3&4 for increase online fraud awareness bank communicate customer in the branch.
- Majority 27.33% of respondents rated 3 for increase online fraud awareness bank communicate customer by E-mail.
- Majority 33.33% of respondents rated 3 for increase online fraud awareness bank communicate customer by telephone.
- Majority 32.67% of respondents rated 4 for increase online fraud awareness bank communicate customer on bank website
- Majority 30% of respondents rated 5 for increase online fraud awareness bank communicate customer by letter from the bank

- The respondent's mostly aware of online frauds like text messages, website advertisements, telephone (mobile phone), redirect website page and downloaded software. The respondent's mostly moderately aware of fraud send through E-mail.
- The respondent's mostly agree with the statements I am aware of the risks from online banking, my bank provides adequate support. The respondent's mostly moderate with the statement my bank provides free anti-virus for my online banking.
- The respondent's mostly agree with the statements do you need more awareness about online fraud risk. The respondent's mostly moderate with the statement do you agree that the information provided by your bank about online fraud awareness is adequate.
- The respondent's mostly aware of most common online banking fraud like scam, malware/virus, spyware, phishing or fraudulently making customers give their own information, hacked accounts and mobile apps (like phone pay, G-pay., etc.), spam, cash send fraud.
- The respondent's mostly aware of security instructions like text messages, website advertisements, telephone (mobile phone), redirect website page and downloaded software. use smart verified app only, browse secure and authorized apps only, never share sensitive personal information, do not response to unsolicited calls SMS or E-mails, be vigilant when using the card, keep your password secret, keep financial data separate, keep your computer and mobile devices up to date.
- The respondent's mostly aware of bank instructions like do not share your ATM pin number, do not share your CVV number, do not share your OTP number, and do not share your personal information about your bank account to others.
- The respondent's mostly rated more than 3 for the mode of communication from bank through E-mail, telephone, bank website and letter from the bank to increase awareness of online fraud to them. The respondent's mostly rated 3 for the mode of communication from bank through branch to increase awareness of online fraud to them.

- There is no differences between male and female respondent's perception towards how much them aware on online frauds.
- There is no differences between male and female respondent's perception towards level of agreement with statements.
- There is no differences between male and female respondent's perception towards degree of agreement on statements.
- There is no differences between male and female respondent's perception towards most common online banking frauds.
- There is no differences between male and female respondent's perception towards security instruction tips.
- There is no differences between male and female respondent's perception towards bank instructions.
- There is no differences between male and female respondent's perception towards mode of communication from bank to them to increase their level of awareness in online fraud.
- There is significant difference among age groups with respect to the awareness rating on most common online banking frauds by the respondents.
- There is no significant difference among age group with respect to the awareness rating on security instruction tips by the respondents.

5.2 SUGGESTION

- Banks should upgrade their software with strong firewall and keep updating them
- Two step authentication for old people, via their guardian. Like one OTP to their kid and the other to them to authenticate bigger transactions.
- Consultant with the official regarding the message or other activity is true by their knowledge before checking the message
- Any transaction that are more than 10k can be hold on for few minutes and can be released post confirmation from customer by reaching them through calls.
- Transactions should be validated with the User's location info and the place where transactions happens.
- Amount should be immediately hold on after the complaint has been raised.
- Banks should be able to recover the amount from deposited account stating it's a fraudulent transaction.
- Banks should be more transparent and supportive to customer on these scenarios.

5.3 CONCLUSION

Online banking fraud is a fraud which happen all over India. This research paper shows customer awareness towards online banking fraud. Even though they are aware of online banking fraud, they want bank to create more awareness on online banking fraud because some village people and some older people still don't have that much knowledge about the online banking fraud. So its bank's responsibility to create more awareness on online banking fraud so as to reduce more number of online banking fraud.

REFERENCES

- ✓ Divya singhal and v. Padhmanabhan (2009) in their paper “a study on customer perception towards internet banking: identifying major contributing factors”.
- ✓ S. Suriyamurthi, mahalakshmi. V & r.karthik (2012) in their paper “a study on customer perception towards internet banking”.
- ✓ V vimala (2016) in their paper “an evaluative study on internet banking security among selected indian bank customers”.
- ✓ Veena k.p, suheel (2016) in their paper “customer perception towards e-banking services: a study with reference to vijaya bank, mysuru city”.
- ✓ Shewangu dzomira (2016) in their paper “financial consumer protection: internet banking fraud awareness by the banking sector”.
- ✓ M. Kannan (2019) in their paper “digital user’s perception on digital banking frauds - a study with special reference to selected digital banking services”.
- ✓ Divya singhal and v. Padhmanabhan (2009) in their paper “a study on customer perception towards internet banking: identifying major contributing factors”.
- ✓ Dr. C.b.pavithra, dr. K.geetha (2021) in their paper “factors affecting customers’ perception towards digital banking services”.
- ✓ Mr. Rupesh. D. Dubey and dr. Anita manna (2022) in their paper “e-banking frauds and fraud risk management”.
- ✓ Komal saxena,dr. Anurag awasthi (2022) in their paper “a solutions provided to secured your online banking frauds”.
- ✓ Martin descazeaux, mathieu couture & yasmine el himdi (2022) in their paper “the new methods in the fight against online bank fraud”.

ANNEXURE I - QUESTIONNAIRE

1. Name
2. Gender
 - a) Male
 - b) Female
3. Age
 - a) 18-20
 - b) 20-30
 - c) 30-40
 - d) 40-50
 - e) Above 50
4. Highest qualification
 - a) SSLC
 - b) HSC
 - c) UG
 - d) PG
 - e) DIPLOMA
5. Marital status
 - a) Married
 - b) Single
6. Are you employed?
 - a) Yes
 - b) No
7. How often do you use online banking?
 - a) Occasionally
 - b) Frequently
 - c) Never
 - d) Very often
8. How often do you use online banking to access your bank account?
 - a) Occasionally
 - b) Frequently
 - c) Never
 - d) Very often

9. To what extend does online banking is important to you?
- a) Important
 - b) Moderate
 - c) Not important
10. Do you know what is online banking fraud?
- a) Yes
 - b) No
11. How often do you follow bank's preventive rules for online banking fraud?
- a) Occasionally
 - b) Frequently
 - c) Never
 - d) Very often
12. Have you been a victim of online banking fraud?
- 1) Yes
 - 2) No
13. Do you know someone who been a victim of online banking fraud?
- a) Yes
 - b) No
14. How much money have you lost in online banking fraud?
- a) Less Rs1000
 - b) Rs1000-Rs5000
 - c) Rs5000-Rs10000
 - d) More than Rs10000
 - e) Never
15. Do you know that Government launches national helpline Number to report cybercrime (helpline number 155260)?
- a) Yes
 - b) No
16. What is your thoughts on helpline number to report cybercrime whether it's useful or not?
- a) Useful
 - b) Not useful
17. To what extend are you aware of online fraud (scams) sent using:

Aware of Online banking Fraud	Strongly Not aware	Not aware	Moderately aware	aware	Strongly aware
E-mail					
Text messages					
Website advertisements					
Telephone (Mobile phone)					
Redirect website page					
Downloaded software					

18. What is your level of agreement with statements?

Level of Agreement with Statement	Strongly Disagree	Disagree	Moderate	Agree	Strongly agree
I am aware of the risks from online banking					
My bank provides free anti-virus for my online banking					
My bank provides adequate support against online fraud					

19. What is your degree of agreement on statement below *

Degree of Agreement with statement	Strongly Disagree	Disagree	Moderate	Agree	Strongly agree
Do you agree that the information provided by your bank about online fraud awareness is adequate					
Do you need more awareness about online fraud risk					

20. Are you aware of these most common online banking fraud which is given below? *

Most common online Banking Fraud	Strongly Not aware	Not aware	Moderately aware	aware	Strongly aware
Scam					
Malware/Virus					
Spyware					
Phishing or fraudulently making customers give their own information					
Hacked accounts and mobile apps (like Phone pay, Gpay, etc)					
Spam					
Cash send fraud					

21. Are you aware of these security instruction tips like *

Aware of these security instruction	Strongly Not aware	Not aware	Moderately aware	aware	Strongly aware
Use smart verified app only					
Browse secure and authorized apps only					
Never share sensitive personal information					
Do not response to unsolicited calls SMS or E-mails					
Be vigilant when using the card					

Keep your password secret					
keep financial data separate					
keep your computer and mobile devices up to date					

22. Are you aware of these bank instructions like

Aware of these bank instructions	Strongly Not aware	Not aware	Moderately aware	aware	Strongly aware
Do not share your ATM Pin number					
Do not share your CVV number					
Do not share your OTP number					
Do not share your personal information about your bank account to others					

23. What forms of communication would you prefer bank to use to increase your level of risk awareness on online fraud?

Mode of communication to increase awareness online banking fraud	1	2	3	4	5
In the branch					
By E-mail					
By telephone					
On bank website					
By letter from the bank					

24. Give any suggestion to create awareness on online banking fraud?
25. Give any suggestion to prevent online banking fraud?