

**A STUDY ON
THE LEVEL OF AWARENESS OF ONLINE BANKING FRAUDS
AMONG THE MIDDLE-AGED CATEGORY WITH SPECIAL
REFERENCE TO KUMBALANGI PANCHAYATH.**

Project Report

Submitted by

M SANJANA: (SB21BCOM043)

ANGEL SAJAN: (SB21BCOM022)

DIYA ANNA FRANCIS: (SB21BCOM035)

Under the guidance of

Smt. LIYA XAVIER

In partial fulfillment of the requirement for the Degree of

BACHELOR OF COMMERCE



ST. TERESA'S COLLEGE ESTD 1925

ST. TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

COLLEGE WITH POTENTIAL FOR EXCELLENCE

Nationally Re-Accredited with A++ Grade

Affiliated to

Mahatma Gandhi University

Kottayam-686560

April-2024

ST. TERESA'S COLLEGE, ERNAKULAM (AUTONOMOUS)

COLLEGE WITH POTENTIAL FOR EXCELLENCE

Nationally Re-Accredited with A++ Grade



CERTIFICATE

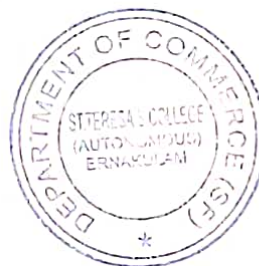
This is to certify that the project titled **"A STUDY ON THE LEVEL OF AWARENESS OF ONLINE BANKING FRAUDS AMONG THE MIDDLE-AGED CATEGORY WITH SPECIAL REFERENCE TO KUMBALANGI PANCHAYATH."** submitted to Mahatma Gandhi University in partial fulfilment of the requirement for the award of Degree of Bachelor in Commerce is a record of the original work done by **Ms. M Sanjana, Ms. Angel Sajan, Ms. Diya Anna Francis,** under my supervision and guidance during the academic year 2023-24.

Project Guide

Smt. Liya Xavier

Assistant Professor

Department of Commerce (SF)



Smt. Jini Justin D'Costa

(Head of the Department)

Department of Commerce (SF)

Viva Voce Examination held on.... 24/04/2024

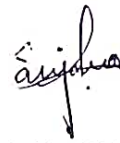
External Examiner(s)

DECLARATION

We Ms. M Sanjana, Ms. Angel Sajan and Ms. Diya Anna Francis, final year B.Com students, Department of Commerce (SF), St. Teresa's College (Autonomous) do hereby declare that the project report titled "A STUDY ON THE LEVEL OF AWARENESS OF ONLINE BANKING FRAUDS AMONG THE MIDDLE-AGED CATEGORY WITH SPECIAL REFERENCE TO KUMBALANGI PANCHAYATH." submitted to Mahatma Gandhi University is a bonafide record of the work done under the supervision and guidance of Smt. Liya Xavier, Assistant Professor of Department of Commerce (SF), St. Teresa's College (Autonomous) and this work has not previously formed the basis for the award of any academic qualification, fellowship, or other similar title of any other university or board.

PLACE: ERNAKULAM

DATE: 24/04/2024



M SANJANA

ANGEL SAJAN

DIYA ANNA FRANCIS

ACKNOWLEDGEMENT

First of all, we are grateful to God Almighty for his blessings showered upon us for the successful completion of our project.

It is our privilege to place a word of gratitude to all persons who have helped us in the successful completion of the project.

We are grateful to our guide **Smt. Liya Xavier**, Department of Commerce (SF) of St. Teresa's College (Autonomous), Ernakulam for her valuable guidance and encouragement for completing this work.

We would like to acknowledge **Dr. Alphonsa Vijaya Joseph**, Principal of St. Teresa's College (Autonomous), Ernakulam for providing necessary encouragement and infrastructure facilities needed for us.

We would like to thank **Smt. Jini Justin D'Costa**, Head of the Department, for her assistance and support throughout the course of this study for the completion of the project.

We will remain always indebted to our family and friends who helped us in the completion of this project.

Last but not the least; we would like to thank the respondents of our questionnaire who gave their precious time from work to answer our questions.

M Sanjana

Angel Sajan

Diya Anna Francis

CONTENTS

Chapters	Content	Page Number
Chapter 1	Introduction	1-3
Chapter 2	Review of Literature	4-8
Chapter 3	Theoretical Framework	9-26
Chapter 4	Data Analysis and Interpretation	27-48
Chapter 5	Findings, Suggestions and Conclusion	49-51
	Bibliography	
	Annexure	

LIST OF TABLES

Sl.No.	Contents	Page No.
1	Table 4.1 showing the classification of age group of people	23
2	Table 4.2 showing the classification of educational qualification of people	24
3	Table 4.3 showing the classification of occupation of people	25
4	Table 4.4 showing the number of online banking users	26
5	Table 4.5 showing that how often do you use online banking services	27
6	Table 4.6 Table showing the number of peoples who's banking details saved in your mobile phone	28
7	Table 4.7 Table showing that how many monthly bills are paid using online banking	29
8	Table 4.8 Table showing the best banking service medium according to the opinion of the target market	30
9	Table 4.9 showing the different online banking platforms used by the people	31
10	Table 4.10 showing the usage of various banking software application provided by the banks by the people	32
11	Table 4.11 showing satisfaction of people in using online banking services provided by their bank	33
12	Table 4.12 showing the number of people who fear using online banking services	35
13	Table 4.13 showing the number of people who have experienced banking frauds	36

14	Table 4.14 showing the number of people who are aware about any of the existing types of online banking frauds	37
15	Table 4.15 showing the source how people know about online banking frauds	38
16	Table 4.16 showing the number of persons who have been the victims of online banking frauds.	39
17	Table 4.17 showing different ways to prevent banking frauds	40
18	Table 4.18 showing how banks help peoples to overcome the frauds experience	41
19	Table 4.19 showing awareness about the impact of online frauds faced by the online banking users	42
20	Table 4.20 showing the level of awareness given by financial banks and other institutions about online banking frauds prevailing in India.	43
21	Table 4.21 satisfaction of people on redressal awareness given by banks	44
22	Table 4.22 showing different form of communication that preferred by the banks in order to increase the level of risk and awareness on online frauds	45

LIST OF FIGURES

Sl.No.	Contents	Page No.
1	Figure 4.1 showing the classification of age group of people	23
2	Figure 4.2 showing the classification of educational qualification	24
3	Figure 4.3 showing the classification of occupation of people	25
4	Figure 4.4 showing the number of online banking users	26
5	Figure 4.5 showing that how often do you use online banking services	27
6	Figure 4.6 showing the number of people who's banking details saved in mobile phone	28
7	Figure 4.7 Figure showing that how many people using monthly bills are paid using online banking	29
8	Figure 4.8 Figure showing the opinion of the target market on the best banking service medium	30
9	Figure 4.9 Figure showing the number of people using various online banking platforms	31
10	Figure 4.10 showing the usage of various banking software application provided by the banks by the people	32
11	Figure 4.11 showing satisfaction of people in using online banking services provided by their bank	33
12	Figure 4.12 showing the number of people who fear using online banking services	35
13	Figure 4.13 showing the number of people who have experienced banking frauds	36

14	Figure 4.14 showing the number of people who are aware about any of the existing types of online banking frauds	37
15	Figure 4.15 Figure showing the source how people know about online banking frauds	38
16	Figure 4.16 showing the number of people who have been victims of online banking frauds.	39
17	Figure 4.17 showing different ways to prevents banking frauds	40
18	Figure 4.18 showing how banks help peoples to overcome the frauds experience	41
19	Figure 4.19 showing the level of awareness about the impact of online frauds faced by online banking users	42
20	Figure 4.20 showing the level of awareness given by financial banks and other institutions about online banking frauds prevailing in India.	43
21	Figure 4.21 showing satisfaction of people on redressal awareness given by banks	44
22	Figure 4.22 showing different form of communication that preferred by the banks in order to increase the level of risk and awareness on online frauds	45

CHAPTER - 1
INTRODUCTION

1.1 INTRODUCTION

In the present scenario, where everything has been digitalized, all the tasks have become easier than before. When we look deep into this, we get to know that the level of increase in easiness is equal to the level of increase in cybercrimes. The more people get into this digital world, the more crimes are being reported. When it comes to banking, frauds and mishaps happen a lot. This is where we should be prepared and careful.

Online banking fraud refers to any illicit activity completed on the financial institution's web application or native mobile apps for money management, bank transfers, instant payments, and money lending. Fraud in online banking profoundly affects how banks and financial institutions provide their services and do their business. There's a pressing need to find a balance between innovating and ensuring safety for both retail and corporate customers.

1.2 STATEMENT OF THE PROBLEM

In this digital era, we can see that the number of cases with respect to online banking frauds has been drastically increasing day by day due to several factors like Inexperienced staffs, lack of understanding on part of customers, Lack of knowledge among the customers regarding how to use digital platforms, Lack of secrecy with regards to bank details, passwords, etc. and Non - compliance with the KYC rules, due to high workloads in the banks.

As we go deep into it, middle-aged adults are the most affected by online banking frauds. It is necessary to mark and improve this section of people so that we can educate a certain percentage of people about digital banking and thus make them more comfortable with the platform. And hereby we can maintain a reduced level of online banking frauds cases.

1.3 SIGNIFICANCE OF THE STUDY

One must be aware of some of the most common online banking frauds and its types. Internet banking frauds are constantly evolving, and it's crucial to be vigilant and take necessary precautions to protect oneself and their finances.

By being aware of the common types of e-banking frauds and following best practices for online security, one can easily reduce the risk of falling victim to these fraudulent activities.

Bank has put multiple security measures in place to ensure that their customers' accounts are safe. As everything is moving online, so are the core banking services, it is the obligation of the bank to ensure that its customers feel safe while conducting their transactions online.

1.4 OBJECTIVES OF THE STUDY

1. To identify the level of awareness on E- Banking frauds among adults in Kumbalangi Panchayath.
2. To find out the different forms of banking frauds and their effect on banking customers.
3. To examine the satisfaction level on the banking redressal mechanism.

1.5 SCOPE OF THE STUDY

The study focuses on spreading awareness on online banking fraud in Kumbalangi grama panchayath, Kerala. This study focuses on the level of awareness about online banking frauds among middle-aged adults. The data collection was randomly done to 50 respondents. The main source of data collection was the questionnaire.

1.6 RESEARCH METHODOLOGY

1.6.1 RESEARCH DESIGN

The study is descriptive, quantitative and analytical in nature. It is descriptive in the sense that it tries to identify various characteristics of research problems. It is quantitative because it involves numerical expression and it is analytical since it examines analyses since it examines, analyses and interprets collected data in order to arrive at conclusion.

RESEARCH INSTRUMENT

A questionnaire is a research instrument consisting of a series of questions and other prompts for the purpose of gathering information from respondents.

1.6.2 COLLECTION OF DATA

PRIMARY DATA:

The data which is collected from primary sources that is an origin from where the data is generated, they are collected for the first time by an investigation or an agency for any statistical analysis. For collecting primary data, we use the method of questionnaire. The questionnaire is a major technique for collecting primary data. The structured questionnaire was distributed to samples for gathering primary data.

SECONDARY DATA:

Secondary data on the other hand is one which has already been collected by someone else and has been passed through the statistical process. Information from secondary sources like journals, newspapers, books, magazines, reports, websites etc. has contributed to the study.

1.6.3 SAMPLE DESIGN

Sampling is a process used in statistical analysis in which a predetermined number of observations are taken from a large group. Random sampling was used to select the samples from the population.

POPULATION:

The population of the study was middle aged group of Kumbalangi Panchayath.

SAMPLE SIZE:

Out of the whole middle-aged group of respondents in Kumbalangi panchayath, a sample size of 50 was selected for the survey.

1.6.4 TOOLS FOR ANALYSIS

The collected data were used with the help of statistical tools like percentages. In the questionnaire a four-point scale was used. Tabular and graphical presentation were used for presentation of data. Graphical presentation includes bar diagram and pie chart.

1.7 LIMITATION OF THE STUDY

- Limited time is available in the study.
- Limited sample size to a particular panchayath.
- Biased response from the respondents.

CHAPTER -2
REVIEW OF LITERATURE

Dr. Gurmeet Singh, Dr. Simanpreet Kaur (2023) They conducted research on Bank Frauds Reported in India: A Case Study. The present study is founded on the sensible concern that, despite several rules, industry is suffering significant losses as a result of unethical behavior by individuals when public funds are involved.

Aravind T Sajeev, Archana R Nair, Dr. Prasanth A P (2023) The journal titled a study on awareness of e-banking frauds with reference to banking customers in Kerala. The objective of the study is to create an awareness about various factors of banking frauds. The customers are suggested to use only authenticate, safe, secure and trusted websites of banks to eliminate online banking frauds and avoid use of public or open Wi-Fi network for online banking transactions.

Aysha Shabbir, Maryam Shabir, Abdul Rehman Javed, Chinmay Chakraborty and Muhammad Rizwan (2021) This article titled Suspicious Transaction Detection in Banking Cyber–Physical Systems deals with the identification of transactions in banking sector and detection of frauds from it. Accordingly, in this paper, the authors provide the fastest, reliable, and efficient fraud detection approach. They use cognitive computing and quantum computing-based suspicious entity detection in the BCPS [Banking Cyber–Physical System] for the post-quantum era.

Dr. C P Gupta and Abhilasha Sharma (2021) In the journal Banking Frauds in India: Trends and Legal Challenges analyzed on various traditional and modern technological frauds prevailing within the industry and the relevancy and adequacy of Indian law on banking frauds. They evaluated the trends of banking frauds and the preventive measures of banking frauds.

Dr. Wojciech Wodo and Dr. Przemysław Blaskiewicz (2021) This features titled Evaluating the Security of Electronic and Mobile Banking sets the ultimate goal of this article as to address security issues faced in the digital platforms. In this article, the authors respond to the needs arising from threats that appear in cyber-space, in particular in the digital banking services market. They present an approach that takes into account the needs of individual users of banking services, among whom they have noticed an extremely low level of awareness of threats and possible protection measures, as well as a lack of emotional understanding of the consequences of an attack.

Ilker Kara (2021) In the journal titled Electronic Banking (e-Banking) Fraud with Phishing Attack Methods. In this study, a forensic analysis of a Phishing attack case sample prepared using electronic banking (e-banking) fake website is performed. It is evaluated that the approach and results used in the study will contribute to both the fight against this crime and future studies.

Priyanka Datta, Sarvesh Tanwar, Surya Narayan Panda, Ajay Rana (2020) They conducted research on Security and Issues of M-Banking: A Technical Report. In this paper, a thorough review has been done on various types of scams that are taking place frequently on mobile or online banking. This paper mainly focuses on the increasing number of online fraud cases related to the banking industry. Hence, awareness programs are required among bank customers to prevent or avoid different types of online fraud.

Dr. Eneji, Samuel Eneji; Angib, Maurice Udie; Ibe, Walter Eyong; Ekwegh, Kelechukwu Chimdike (2019) In the journal titled A Study of Electronic Banking Fraud, Fraud Detection and Control. This paper critically examines electronic banking frauds, detection of electronic banking frauds, control of electronic banking frauds, and challenges associated with the detection and control of electronic banking frauds.

Dr. D Mahila Vasanthi Thangam and Bhavin P P (2019) The research titled Banking Frauds in India; A Case Analysis examined the different types of bank frauds in India and also analyzed the depth of frauds in public private and cooperative banks. This paper tries to identify the involvement of bank officials in the banking industry and analyzed the legal consequences of these frauds within the framework of Indian penal codes.

Mostafa A Ali, Nazimah Hussin, Ibtihal A. Abed (2019) This article titled E-Banking Fraud Detection: A Short Review, a review of the security challenges associated with e-banking has been presented. Equally, the challenges and characteristics of e-banking fraud have been mirrored. This paper also reviewed different types of fraud and attacks detection systems, as well as some preventive measures in place to secure e-banking services.

Dr. Seema Thakur (2018) The journal titled Electronic Banking Frauds in India: Effects and controls examined the core banking activities and the fact that the security

problem may have seemed to be a crucial issue in the practice of E-banking in India but that could not imply that the operational efficiency of E-Banking is impaired.

Rachel Baker (2018) In the journal titled Awareness Creation on E-banking Fraud Prevention focuses on Knowledge in Management Perspective for E-Security and Customer Relationship Building researched on the prevention of fraudulent E-banking transactions to ensure trust and loyalty of the institution to enhance customer relationship. It concluded that the financial institution should enhance customer relationships to ensure a positive reputation of the banks.

Mr. Rupesh D Dubey and Dr. Anita Manna (2017) The journal titled E-Banking Frauds and Fraud Risk Management concluded as electronic payment volumes grow and more banking activity extends to the web and mobile devices, the ability to detect and prevent financial crime has become critical. The burden of financial institutions to protect their customers and themselves from the losses due to online banking frauds has increased over the period of time.

Ms. Sarika Digamberrao Gudup (2016) In the journal titled The Study of Frauds and Safety In E-banking studied about the various E-banking users and the risk and safety factors in E-Banking services. She also conducted research on the E-Banking frauds prevailed at that period and the level of awareness amongst the users about the frauds. She also studied the role of RBI towards the prevention of E- Banking frauds.

Charan Singh, Divyesh Satishkumar Dixit, Kiran Antony, Mohit Agarwala, Ravi Kant, Siddharth Nayak, S Mukunda, Deepanshu Pattanayak, Ravi Kant, Suryaansh Makked, Tamanna Singh, Vipul Mathur (2016) This study report is titled Frauds in The Indian Banking Industry. This study endeavors to cover issues such as banking frauds and mounting credit card debt, with a detailed analysis using secondary data (literature review and case approach) as well as an interview-based approach, spanning across all players involved in reporting financial misconduct. The report touches upon the case of rising NPAs in the past few years across various scheduled commercial banks, especially public sector banks. The study finally proposes some recommendations to reduce future occurrence of frauds in Indian banking sector.

Dr. Sukhamaya Swain and Dr. Lalatha K Pani (2016) They conducted research on Frauds in Indian Banking: Aspects, Reasons, Trend Analysis and Suggestive

Measures. This paper discusses the various aspects of frauds in Indian banking system. It evaluates the statistics involved with fraud basis secondary data available from reliable sources and also analyses the same. Each of the types of namely KYC related, loan related, and technological aspects are discussed in detail along with the reasons. At the end, some suggestions are placed for banks to practice.

Amit Donald Menezes and Dr. Prakash Pinto (2016) The research titled Banking Frauds and Ways to Prevent Them concluded with the advent of technology there have been positive as well as negative impacts to the banking industry. The positive thing is that it has brought lots of savings and money to bankers as well as the customers. Negative is that online banking frauds have increased over the years.

Rute Abreu, Fatima David & Liliane Segura (2016) They conducted research on E-banking services: Why fraud is Important? - The purpose of this paper is to answer the importance of fraud that arises from the use of e-banking services more ethical behavior applied to everyday moral problems. The results of the paper mitigate risks, such as showing several threats, vulnerabilities, incidents, impacts and responses that face e-banking services.

Hoffmann & Birnbrich (2012) The impact of fraud prevention on bank-customer relationships- An empirical investigation in retail banking: The purpose of this paper was to establish a conceptual as well as an empirical link between retail banks activities to protect their customers from third-party fraud, the quality of customer relationships, and customer loyalty. A conceptual framework was developed linking customer familiarity with and knowledge about fraud prevention measures, customer loyalty and relationship quality.

Vishal Goyal, Dr. U S Pandey, Sanjay Batra (2012) In the journal titled Mobile Banking in India: Practices, Challenges and Security Issues. This paper reviews the emerging research literature on m-banking. It is expected that the comprehensive list of references and assessments presented in this paper will provide a useful anatomy of young m-banking literature to anyone who is interested in m-banking and help stimulate further interest.

Rashad Yazdanifard, Wan Fadzilah Wan Yusoff, Alawa Clement Behora and Abu Bakar Sade (2011) They conducted the research on Electronic Banking Fraud; The Need to Enhance Security and Customer Trust in Online Banking. The paper discussed

Transferability:

Transferring funds from one bank account to another is the most basic m-banking activity. All the banking app-based transfers are now secured using two-step verification via app password and OTP-based transactions. The two-step verification is applicable in fund transfers, utility bill payments, and online shopping for the safety and convenience of customers.

Investment Management:

Many big banks offer the facility of securities trading through their banking app. It makes it easier for the customers to trade hassle-free. Also, m-banking enables customers to track their deposits and other investments from the convenience of their homes.

Digital Payments:

At present, all m-banking apps have a QR code reader for payment at merchant locations. So, the customer has to point at the QR code of the merchant at their shops and pay the price of the goods using the account details from the QR code.

Customer Service:

M-banking provides personalized service to customers through live chat, phone, notifications, etc. This helps customers to get the required assistance without visiting the bank directly.

BENIFITS OF MOBILE BANKING

1. **Convenience:** Check account balances, find ATM locations, transfer funds, and even deposit checks.
2. **Timesaving:** No longer need to visit a credit union location to perform the everyday tasks mentioned above.
3. **Bank on the go:** You don't even need a desktop computer. Bank from the train, airport, or backseat of a cab.
4. **Easy to monitor:** Stay on top of daily transactions to protect against fraud.
5. **Good for budgeting:** With access to your money at your fingertips, you can check your balance before you spend and make sure you're on track to meet budgeting goals.

people's attitude towards online banking and the level of transparency about bank frauds and security that will help to gain back customer's trust. They concluded that protection and improving security is critical for enhancing customer trust.

Khanna & Arora (2009) A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry: This paper identifies the causes responsible for the frauds happening in electronic banking. It aims to find out the various fraud preventions taken by the employee working in the banking sector in order to stop fraudulent practices. The researchers have used primary data to collect the information and targeted mostly the banking employees. The study signifies the importance of training that should be provided to the employees in order to prevent fraud. The researchers have identified that the various implementation that has been taken up by the banks are not up to the mark. This paper identifies that the main reasons for bank frauds are overburdened staff, lack of training provided, low compliance level, competition.

Sunanda Sen (2009) In the journal titled Speculation, Scams, Frauds and Crises: Theory and Facts the author critically analyses and gives an outlook about various scams and frauds known in the digital sector. The analysis outlined above helps to explain the successive crises in the global financial markets as have currently come out into the open.

Pulella Murali Mohan (2000) This research report titled An Analytical Study on Bank Frauds and Scams in India sets its main objectives as to study the types and classifications of bank frauds, to identify the reasons and causes of bank frauds. This also helps to recommend ways and means to mitigate the menace of frauds and scams in India along with briefly examine the suitability of law to deal with the frauds. The Study mainly concerned with nationalized public sector banks, which have been victims of frauds as also of scams, past and present.

R. Bandyopadhyay and K. V. Patel (1987) In the journal titled Development Banking in Rural Areas the authors mainly focus on the twenty-ninth report of the Estimates Committee of the Eighth Lok Sabha and examining various aspects of social banking' in relation to the State Bank of India. Through this feature, the authors try to point out the relevance as well as the concerns for the development done in banking sectors of rural areas.

CHAPTER - 3
THEORITICAL FRAMEWORK

DEFINITION OF BANKING FRAUDS

Bank fraud is the use of potentially illegal means to obtain money, asset, or other property owned or held by a financial institution or to obtain money from depositor by fraudulently posing as a bank or other financial institution in many instances, bank fraud is a criminal law. While the specific elements of particular banking fraud laws vary depending on jurisdictions, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft. For this reason, bank fraud is sometimes considered a white-collar crime.

WHAT IS ONLINE BANKING FRAUD?

An online banking fraud happens whenever a criminal can access and transfer funds from an individual's online bank account. As fraud generally refers to any intentional act aimed at depriving an individual of a legal right, online banking fraud narrows the scope of the illegal activity, which has to happen online and results in an economic loss. Online banking fraud refers to any illicit activity completed on the financial institution's web application or native mobile apps for money management, bank transfers, instant payments, and money lending.

FEATURES OF MOBILE BANKING

M-banking has features that ensure customers can access their accounts and carry out financial transactions on the go. Some key features of m-banking are:

Accessibility:

M-banking offers 24-hour access to all customers. Customers can log in to their app and view and track their account balances anytime. Besides, they can engage in fund transfers even during bank holidays.

Security:

The banks recognize the importance of providing a secure environment to customers for transactions based on the banking app. Hence, m-banking asks for SMS access, location access, biometric access, and application password from the customers to ensure their privacy and security.

6. **Mobile Deposit:** Depositing checks is no longer a hassle. Simply use your smartphone camera and mobile app to take a picture of the front and back. Deposit processing times are the same as if you brought the check to a branch.
7. **Apply for a loan:** if we Need a credit card, personal loan, or car loan there is No need to go to the branch when you can apply for financing through the mobile app.
8. **No cost to you:** Mobile banking is a free service for all Palisades Credit Union customers.
9. **Accessing the bank 24/7:** Unlike a bank branch, mobile banking conveniently gives you access to your account anytime you like — with some exceptions, such as planned maintenance updates and unexpected outages. This ease of accessibility saves you time. Mobile check deposit, for example, a feature most banking apps offer, allows you to deposit a check on the go or from the comfort of your couch. Mobile banking can also help alleviate concerns for those who might have experienced in-person discrimination.
10. **Strengthening security:** Banks are in the business of guarding your assets — including transactions made using their mobile apps. Though nothing is foolproof, there are ways you can step up security precautions if you're concerned about mobile banking security. Financial institutions often require a username and password to sign into a mobile app and offer additional safety features to further safeguard your account. Multi-factor authentication, for example, requires at least two kinds of verification to prove that it's really you. The first are the account credentials (your username and password) followed by a text with numeric code sent to your phone that needs to be submitted to gain access to the account. Further, some mobile devices and some bank apps let you log in by scanning your face or fingerprint as yet another way to protect your digital bank account without trading convenience.
11. **Tracking expenses:** When it comes to managing and sticking to a budget, tracking all of your expenses is the part that requires the most labor, and it may lead you to give up on budgeting altogether. Mobile banking apps can do much of that labor for you, by keeping track of your expenses tied to a particular account and organizing them into spending categories. You can see a breakdown of total expenses for things like utilities, dining, transportation and more. By reviewing your spending patterns, you should gain a clearer

understanding of where your money is going and can identify areas where you may need to make adjustments.

NEED FOR E-BANKING

Instead of approaching to the branch in person in order to withdraw cash or deposit a cheque, through online banking any inquiry or transaction can be processed, via internet, at any time. Online Banking also helps in secure transactions. It reduces the fear of carrying cash all the time. Online banking services have increasingly become a 'need to have' rather than a 'nice to have' Thus the online banking is considered to be more of a norm as it is the cheapest way of providing banking services to customers. Banks have always been in the forefront of harnessing technology in order to improve their services and efficiency.

SECURITY ISSUES IN MOBILE BANKING

Some of the security risks that we should definitely want to avoid and to be aware of. They are as follows:

1. Using a fake mobile banking app

Some scammers have created fake mobile bank apps to get you to enter your password and other private details. Once they have that information, they can turn around and use it to access your real bank account and take out your money. Always read reviews and make sure you're dealing with the real app for your bank before downloading one or trying to log in. You can also try going to your bank's website and clicking on the link to the download page for its mobile app to make sure you're using the right one.

2. Using your mobile banking app on public Wi-Fi

Public Wi-Fi might enable you to save your monthly cell phone data, but it also makes it much easier for hackers to access your phone and see what you're doing. It is possible for them to hack into your phone when you're using cellular data, too, but that is much harder to do. Always stick to cellular data if you need to access your financial accounts in public, or better yet, wait until you're on a private Wi-Fi network to log into your bank account.

3. Bank account Not updating your phone's operating system or apps

Installing updates can be a pain and can keep you from accessing your phone or apps for a while. However, you should always do it anyway. Some of these updates are important security patches that fix flaws in an app that might let hackers more easily access your data. Outdated software is also easier to hack in general. Whenever your phone notifies you about an update, install it as soon as it's feasible, especially if it's for your mobile banking app.

4. Storing passwords and PINs on your phone

You might decide to keep a note on your phone with your bank account password or PIN if you're prone to forgetting it, but this is dangerous, too. If you lose your phone and a would-be thief finds it, they can easily gain access to your financial accounts, and you probably won't even notice until your money is already gone. Try to memorize your passwords, especially your bank account password, so you don't need to store them on your phone or computer.

5. Using an easy password

The days when "Password" was considered a secure password are long behind us if they ever existed at all. Fortunately, most online accounts, including mobile banking apps, no longer allow you to use such simplistic passwords. You must choose something that has a mix of capital and lowercase letters with some numbers and symbols thrown in. These types of passwords are more difficult to hack, so using one of them helps keep your account secure.

You should also use different passwords for all of your online accounts -- or at least use a different password for your mobile banking app -- so that hackers who gain access to one of your online accounts can't break into all of them. Changing your password every couple of months, even if you don't need to, can also keep hackers from accessing your banking information.

6. Not password protecting your phone

Modern smartphones let you enter a passcode or open your phone with a fingerprint scanner so that no one else can access your phone without your permission. This extra layer of security can prevent others from hacking into your mobile banking account or gaining access to other personal information stored on your phone that might help them answer your bank's security questions. Take advantage of these security features to keep your bank account and other personal information protected.

7. Not signing up for security alerts

Security alerts are messages sent to your phone or email that tell you about new or suspicious activity regarding your bank account. It might be a login from a new device or a purchase that seems suspicious. These alerts can help you quickly identify when your identity has been compromised so you can take action to stop the thief from draining your account. Enrol in these alerts if your bank offers them and check your bank accounts regularly for signs of suspicious activity.

Mobile banking apps are really useful, and they're not going away anytime soon. But they're also not immune to attack. Avoiding the seven above mistakes is crucial if you want your bank account to remain private.

How To Protect Yourself Against Mobile Banking Security Risks

The risks of mobile banking apps may sound scary. But if you maintain a high level of mobile security, using apps can be just as safe as banking at a branch in person (not to mention more convenient).

To stay safe while banking on your phone, follow these tips:

- Only download apps from official app stores
- Don't skip operating system or app updates
- Secure your bank accounts and devices with strong passwords and 2FA (Two Factor Authentication)
- Avoid using "rooted" or "jailbroken" devices
- Stick to mobile data when accessing your banking app
- Don't respond to unsolicited calls, emails, or texts from your bank
- Use antivirus software with malware and phishing protection

- Sign up for credit monitoring to alert you about suspicious activity

COMMON TYPES OF ONLINE BANKING FRAUDS

1. Vishing

Scammers use a phone call to get out sensitive information like your login details, username, transaction passwords, card PINs, OTPs, CVVs, URNs, grid card values, or personal data like your birth date or mother's maiden name. Often, fraudsters pose as bank representatives and trick you into giving your personal and financial information. You must not provide any of your personal or banking information over the phone when you receive a call asking for the same.

2. Phishing

Phishing is the activity that intends to 'fish' your confidential banking information. It may involve receiving an email that allegedly seems to be from a well-known institution like a bank or a trusted website. You must be aware and not click on such emails. Note that your bank would never request your private information, such as your password, login details, or OTP, among other such information.

3. Spear Phishing

Spear phishing is a focused phishing attempt that is delivered by email. It seems to have come from a reliable source and often originates from a colleague, boss, close friend, or relative. If you click on attachments or malicious links in the email, fraudsters can easily access sensitive information stored on your device. Always avoid clicking on such fishy emails.

4. Skimming

For committing this fraud, scammers usually hide a small gadget called a skimmer in the card slots of ATMs or merchant payment terminals, which can read and record your card information. Fraudsters even use a carefully placed camera to record your PIN. It is advisable to stay alert whenever you visit an ATM booth to prevent such banking fraud.

5. SIM Swap

Under SIM swap, a fraudster gets a new SIM card from your mobile service provider in your name using your registered mobile number. The scammer conducts financial transactions from your bank account by receiving the OTP and alerts needed. You must immediately report to your mobile service provider if your phone or SIM card is lost or has stopped working.

6. Smishing

Smishing uses SMS or text messaging to scam you. Smishing scammers use toll-free phone numbers and message links to target you. You may receive a message stating that your accounts need to be updated with a link directing you to sign up for some new scheme. By clicking on such phishing links sent in the message, your confidential details may get compromised. To save yourself from smishing, you must not click on any link without knowing its source.

7. Website Spoofing

Building a fake website to commit fraud is called website spoofing. Phishers use names, pictures, logos, and even website codes to make spoof sites appear authentic. You are urged to enter your details on such fake websites. One must enter details on a website only after checking the presence of 'HTTPS' in the URL.

8. Malware Attack

A malware attack is malicious software developed by cyber criminals that can cause damage to the operating system of your smart device. Through this software, fraudsters can access your confidential banking information and use it to remove money from your bank account. It would be best to keep your devices secure with malware protection software.

NATURE OF ELECTRONIC FRAUDS IN INDIA

Computer frauds can take the form of corrupting the program(s) and even breaking into the system via a remote sensor by a computer programmer or specialist. The manipulation of computer and other Information and Communication Technology (ICT) to defraud banks gives more insight into the latent friction of technological revolution. When computer was invented, the intention of its inventors is to hasten

data processing with effortless ease. That, it has been doing efficiently by giving timely and accurate information.

But like other mechanical and/or electrical electronics devices, it has equally lent itself to heinous acts. What is meant to assist in daily data operations has turned out to be an undoing. While basking in the euphoria of its efficiency, banks are also grasping with its fraudulent manipulations. The liability of computer to control manipulations, frauds and forgeries continue to give the banking system nightmares. Any type of act distinctly associated with computer or data manipulation in which victim involuntarily suffer or could have suffered losses, injuries or damage or in which perpetrator receive or could have received gain is referred to as a "Computer crime". The adoption of ICT in banking is generally referred to as electronic banking (e-banking) and the implementation strategies of banking services have become a subject of fundamental importance and concern to all banks and indeed a pre-requisite for local and global competitiveness. This is because it directly affects the management decisions, plans, and products and services to be offered by banks. The internet and indeed, the e-banking

have continued to change the way banks and their corporate relationships are organised worldwide and the variety of innovations in service delivery. In the 2003 report of the technical committee on e-banking of the Central Bank of India (CBN) defines e-banking as a means whereby banking business is transacted using automated processes and electronic devices such as personal computers, telephones, internet, card payments and electronic channels. It further states that some banks practise electronic banking for informational purpose, some for simple transactions such as checking account balance as well as transmission of information, while others facilitate funds transfer and other financial transactions. Many systems involve a combination of these capabilities.

ADVANTAGES OF ADDRESSING BANKING FRAUDS

1. Security

Awareness of internet banking can help customers understand the importance of protecting their account information and adopting security measures such as strong passwords, two-factor authentication, and avoiding phishing scams.

2. Financial literacy

Internet banking can help increase financial literacy by allowing customers to monitor their account activity and learn about their spending habits.

3. Create awareness

By addressing online banking frauds, it can be reduced, and it helps to take necessary measures to protect the economic value of people and prevent frauds.

4. Business efficiency

For businesses, internet banking can streamline financial operations, reduce administrative tasks, and improve cash flow management.

5. Convenience

Internet banking provides customers with 24/7 access to their accounts, which allows them to perform financial transactions at their own convenience without having to physically visit a bank.

6. Timesaving

Internet banking eliminates the need to stand in long queues at banks, saving time and energy.

7. Cost-effective

Internet banking can help customers save money by avoiding transaction fees or reducing the need for paper-based transactions.

HOW TO PREVENT E-BANKING FRAUDS?

1. Biometric authentication

Biometric authentication is an identification technique that relies on a customer's unique physical characteristics, such as their voice, facial features, or fingerprints, to verify their identity. Each of these characteristics is known as biometric data. Biometric authentication has quickly become a popular security measure with financial institutions because customers' biometric data cannot be

stolen, forgotten, or lost. Although fraudsters can spoof a customer's biometric data, it is far more challenging to do so than it is to steal their identity or credentials. To get the greatest value out of biometric authentication, banks should pair it with other technologies and controls to create a truly multi-layered security strategy.

2. Two-factor and/or multi-factor authentication

Two-factor and multi-factor authentication are identification techniques that require banking customers to provide two or more pieces of evidence to verify their identity and are fairly standard security measures that, like biometric authentication, should be layered with the other technologies shown here to create a comprehensive anti-fraud strategy.

3. Host regular fraud awareness training

Bank employees are a popular target for cybercriminals particularly for phishing attacks and other forms of social engineering so it's essential to educate staff about recognizing potential fraud and what to do if they suspect that they've been compromised.

4. Be on the lookout for internal fraud

With banking fraud, sometimes the call comes from inside the house. Employees can expose their employers to substantial risk, whether accidentally.

5. Create a database of known threats

It's crucial that banks be aware of and on the lookout for active and emerging threats. By collecting fraud data from internal and external sources, banks can gain a comprehensive view of the fraud landscape and make more informed risk decisions. Financial institutions can also use such a database to support fraud awareness training and enable employees to recognize a broader range of potential threats.

6. Educate banking customers

Customer fraud awareness is every bit as important as employee fraud awareness and can help a bank's customers protect themselves against would-be threat actors. Adding educational resources to an existing knowledge base similar to what Wells Fargo has done with its fraud education library, can be an effective means of keeping customers in the know.

7. Monitor transactions in real time

Transaction monitoring is not only essential to comply with KYC and anti-money laundering laws, but also an effective way to detect fraudulent activity. For transaction monitoring to be successful, banks must first develop behavioural profiles that establish a baseline for each customer's normal activity. Once an institution has created a behavioural profile for a customer, it can monitor that customer's transactions against the baseline and proactively flag any anomalous activity.

REMEDIES PROVIDED BY THE BANKING REDRESSAL FORUM RELATING TO BANKING FRAUDS

1. Document the issue/complaint

The employee should make an initial effort to resolve the grievance with their immediate supervisor. The first step is to write a letter to the grievance redressal committee/concerned department head/supervisor containing all relevant details of the issue. The supervisor's decision is final unless it is unreasonable, arbitrary, or irrational.

2. Problem identification

A supervisor should identify the problem and assess the situation.

3. Collecting the information

When the problem has been identified, the supervisor should collect all relevant information about the grievance before developing a plan of action.

4. Analyse

5. To find the root of the problem, the supervisor must study various aspects such as the employee's history, frequency of occurrences and management practices.

6. Decision making & Implementation

The management work out several alternative courses of action, and the consequences of each course on the employee and the administration are evaluated. A final decision is reached based on which course of action will benefit all parties concerned and is implemented.

7. Take action

If a grievance refers to a higher authority under this procedure and the outcome does not meet their expectations, both parties can agree to appoint an arbitrator.

VARIOUS LEGISLATIVE MEASURES FOR E-BANKING FRAUDS

1. As per the RBI guidelines each bank and its branch have to have the formation of the special committee with the reasonable number of members. The committee formed on take care of the problems regarding banking frauds and what efficient preventive steps that may be taken so as to forestall such banking frauds.
2. In keeping with the RBI guidelines each and each bank in India or foreign banks having branch in India must have compulsorily a separate department specifically for managing the banking frauds on find the ways to regulate over banking frauds and also the cases which come to the bank must be resolved by them or they have to guide to the purchasers as how their cases is resolves and also the fraudster may be caught and therefore the money may be recovered.
3. As per the RBI norms each bank must have a review council. The duty of the fraud review council is to determine the schemes implemented for bringing down the quantity of banking frauds is effective or not the rules, norms and laws framed regarding banking frauds are properly implemented or not.
4. It's one among the obligations of the bank. Banks have to have security policy and find it approved by board of directors before implementing the identical. Banks must have a separate department for taking care of the protection of the knowledge system through which e-banking transactions are done and also the data is saved in system should have great security.

5. The RBI has issued an inventory of requirements which are to be taken by the banks from their customers before opening the account or any time after this guideline is issued from the prevailing customers. The aiming to the sentence knows your customer means the bank should know their customer before going in a relation with them and opening the account.
6. Banks have to make their customers aware of the danger involved in using the net banking services and on what precautionary steps to be taken by them so as to stop the identical. According to the RBI it the requirement and duty of the bank to create their customer aware of the preventive measures to be taken when using internet banking services. The online page of the bank must contain such details. Also, the bank is required to be displayed at the place which is well accessible to customers at the bank such details. Frequently and timely bank can pass away the information of preventive measures to their customers by sending them messages on the mobile number of the customer registered with the bank.
7. Banks most significant duty is to train their customers because this is often the case within which within the common language understood the shoppers are educated but they're said uneducated within the field of e-banking services. The requirement to incline proper information's and guidelines and time to time changes what are happening within the E-banking services. Banks have to make customers know different or kind of e-banking frauds there are being committed and therefore the remedial measures are to be told to them which is able to ultimately help in preventing the e-banking fraud cases and should help in stopping the commission of e-banking frauds. And during this manner bank can show their concern towards the shoppers and an honest reputation and goodwill are often built up by the banks by doing such reasonably things as organizing free seminars on this subject and then on. And this can be one in all the rules of the RBI also which the banks need to follow compulsorily.

8. Banks need to submit the report of review of internet industry to the bank of India time to time. The timely review that's the working and functioning of the net banking industry must be reported to the RBI. This is often done to verify that are the banks having full proof safe and secured internet industry and are they upgrading the web banking industry and also to test whether the banks are maintaining the minimum standards of internet industry. This may make sure that the shoppers are safe or not and can be within the interest of the general public at large.
9. Banks need to inform about the preventive measures to be taken by the purchasers while using the e-banking services. The bank should display the identical at the acceptable place where the customer has quick access to the identical and also the information is to be displaced in number of languages say per se English, Hindi, Marathi, Gujarati closes to on depends upon the locality where the bank is situated and also the people leaving around and having the bank accounts within the mobile banking Security issues in mobile banking.

VARIOUS LEGISLATIVE MEASURES FOR E-BANKING FRAUDS

As per RBI report the total number of fraud cases in the banking sector in FY23 were 13530 involving total amount of ₹30252 Crore. Of this almost 49% or 6659 cases were in the digital payment - card/internet category. The Government of India has taken several measures to enhance digital security and prevent cybercrimes, including money laundering, in recent years. Some of the key initiatives are:

1. Indian Computer Emergency Response Team (CERT-In):

The government has established CERT-In as the national nodal agency for handling cyber security threats and incidents.

2. Information Technology (Amendment) Act, 2008:

This act provides a legal framework for e-commerce and digital transactions in India and also lays down provisions for dealing with cybercrimes.

3. Cybercrime Investigation Cell:

The government has set up Cybercrime Investigation Cells in various states to investigate and prosecute cybercrimes.

4. National Cyber Security Policy:

The government has launched a National Cyber Security Policy to strengthen the country's cyber security framework and ensure the protection of critical information infrastructure.

5. Cyber Swachhta Kendra:

This is a botnet cleaning and malware analysis centre, which aims to tackle the spread of malicious software and strengthen the security of India's cyber space.

6. Awareness Programs:

The government is conducting various awareness programs and training sessions for citizens and organizations to educate them on the importance of cyber security and ways to prevent cybercrimes.

7. Data Protection Laws:

The government is in the process of developing a data protection law to safeguard the personal data of citizens and prevent its misuse.

Recently Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) has been developed by the Indian Cyber Crime Coordination Centre (I4C) under Ministry of Home Affairs of Government of India, for quick reporting of financial cyber frauds and monetary losses.

In total of 800 odd FIs (Financial Institutions – Banks, insurance companies etc) in India, only 259 have registered with I4C which makes it very pathetic to reduce the cyber frauds. It has so far intercepted transactions worth ₹602 Cr since its inception

in April 2021. There are certain recommendations and reforms to be implemented suggested by the Indian Government. They are:

- The FIs have been asked to be registered with the CFCFRMS
- Banks have been asked to appoint nodal officers to coordinate with agencies
- States also have been asked by the Government to ensure data protection.
- Suspension of 70 lakh mobile numbers: If the authorities detect any frauds, they suspend the Mobile numbers that initiated the fraud. This has been implemented.
- 4-hour delay in UPI transactions: Whenever there is a transaction between two new numbers, transaction for next four hours after the first transaction will be freeze. This reform is yet to be implemented.
- After taking a new UPI number, transaction up to a maximum of ₹50,000 is allowed in first 24 hours.

CHAPTER -4

DATA ANALYSIS AND INTERPRETATION

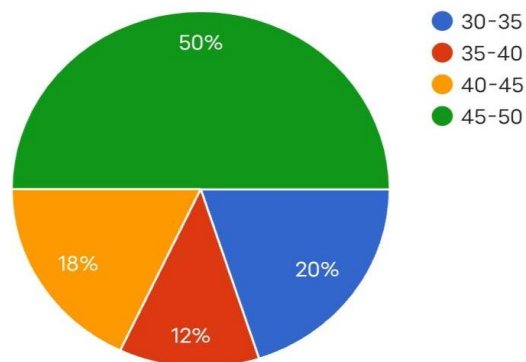
4.1 CLASSIFICATION SHOWING THE AGE GROUP OF PEOPLE

Table 4.1 showing the classification of age group of people

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
30-35	10	20
35-40	6	12
40-45	9	18
45-50	5	50
Total	50	100

Source- Primary Data

Figure 4.1 showing the classification of age group of people



Interpretation: From the above data 50% of people belong to 45-50 years, 20% of people are 30-35 years 18% of people belong to 40-45 years, and 12% of people are 35-40 years.

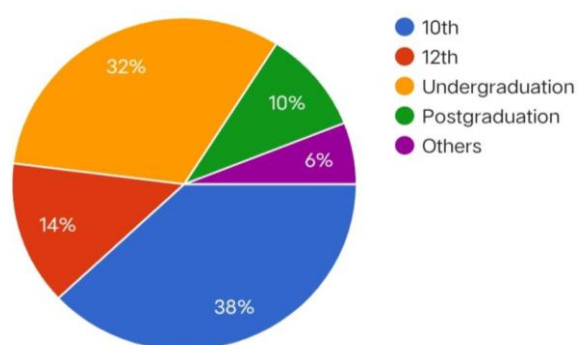
4.2 CLASSIFICATION SHOWING THE EDUCATIONAL QUALIFICATION OF PEOPLE

Table 4.2 showing the classification of educational qualification of people

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
10th	19	38
12th	7	14
Under graduation	16	32
Postgraduation	5	10
Others	3	6
Total	50	100

Source- Primary Data

Figure 4.2 showing the classification of educational qualification



Interpretation: From the above data 38% of people completed their 10th standard, 32% of people completed under-graduation, 14% of people completed 12th, 10% people completed post-graduation, 6% of people have other educational qualification.

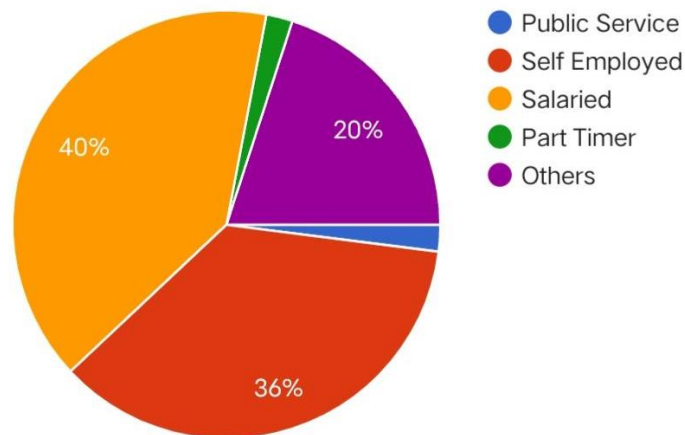
4.3 CLASSIFICATION SHOWING THE OCCUPATION OF PEOPLE

Table 4.3 showing the classification of occupation of people

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Salaried	20	40
Self employed	18	36
Public service	1	2
Part Time	1	2
Others	10	20
Total	50	100

Source -Primary Data

Figure 4.3 showing the classification of occupation of people



Interpretation: From the above data 40% of people are salaried, 36% of people are self-employed, 20% people are part of other occupations, 2% of people are public servant and part-timer.

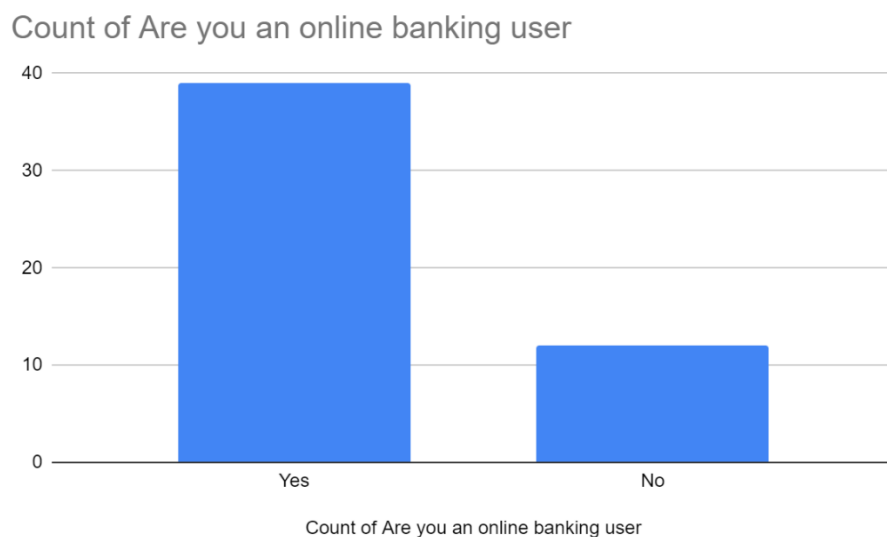
4.4 CLASSIFICATION SHOWING THE NUMBER OF ONLINE BANKING USERS

Table 4.4 showing the number of online banking users

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Online banking user	38	76
Not online banking user	12	24
Total	50	100

Source- Primary Data

Figure 4.4 showing the number of online banking users



Interpretation: From the above data 76% of people are online banking users and 24% of people do not use online banking services

4.5 CLASSIFICATION SHOWING THAT HOW OFTEN DO YOU USE ONLINE BANKING SERVICES

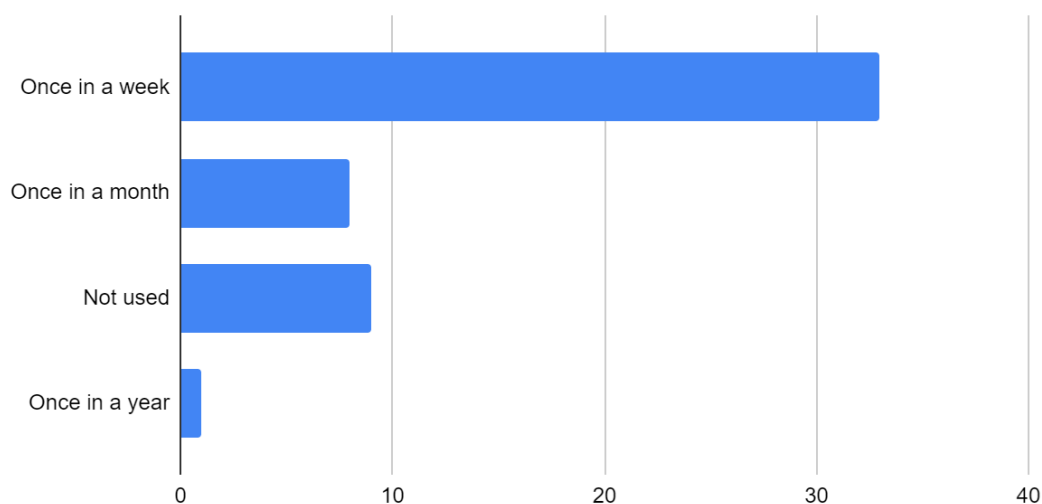
Table 4.5 showing that how often do you use online banking services

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Once in a week	32	64
Once in a month	8	16
Once in a year	1	2
Not used	9	18
Total	50	100

Source -Primary Data

Figure 4.5 showing that how often do you use online banking services

Count of How often do you use online banking services



Count of How often do you use online banking services

Interpretation: From the above data 64% of people uses online banking services once in a week, 18 % uses once in a year, 16% uses once in a month and 2% people not used online banking services.

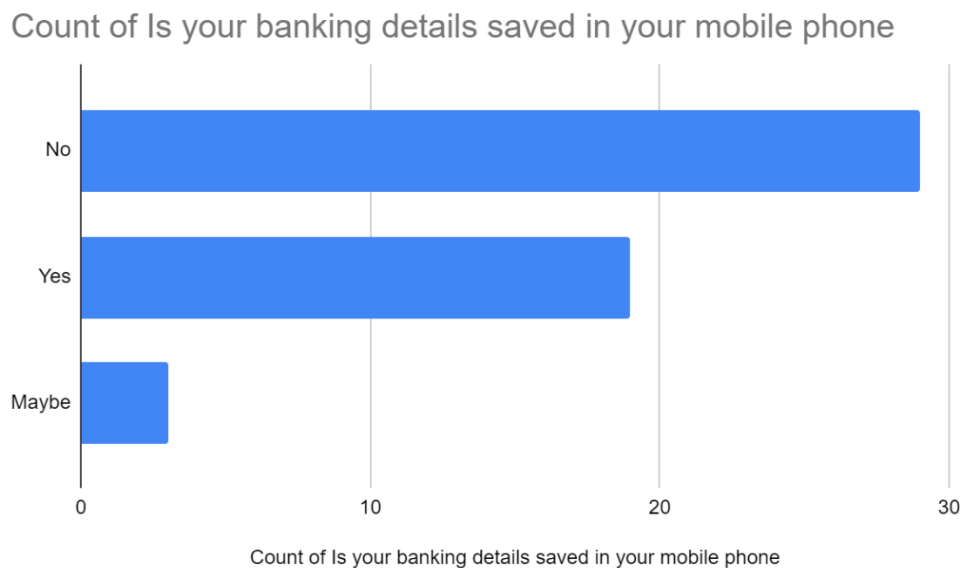
4.6 CLASSIFICATION SHOWING THE NUMBER OF PEOPLES WHO'S BANKING DETAILS SAVED IN YOUR MOBILE PHONE

Table 4.6 Table showing that the number of peoples who's banking details saved in your mobile phone

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Yes	36	18
No	58	29
Maybe	6	3

Source -Primary Data

Figure 4.6 showing that the number of people who's banking details saved in mobile phone



Interpretation: From the above data 29% of people have not saved their banking details on their phone, 18% have saved their banking details on their phone and 3% of people may have saved their details on their phone.

4.7 CLASSIFICATION SHOWING THAT HOW MANY MONTHLY BILLS ARE PAID USING ONLINE BANKING

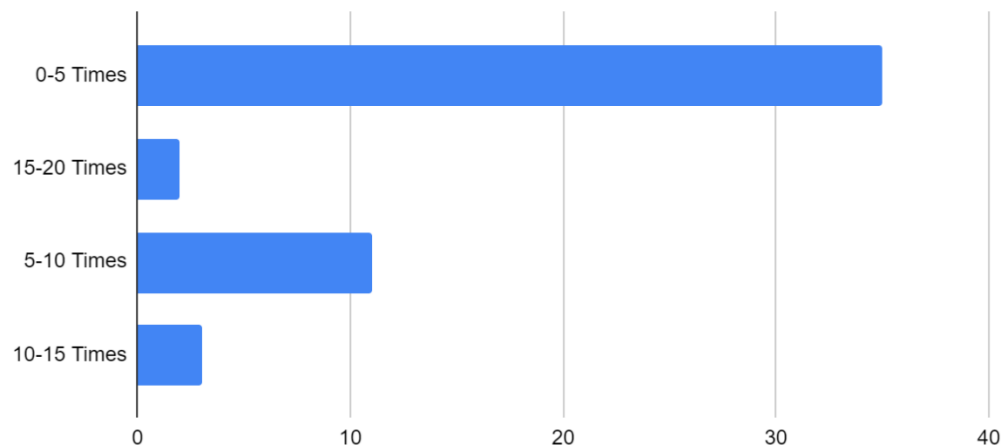
Table 4.7 Table showing that how many monthly bills are paid using online banking

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
0-5	35	70
5-10	11	22
10-15	2	4
15-20	2	4
Total	50	100

Source- primary Data

Figure 4.7 Figure showing that how many people using monthly bills are paid using online banking

Count of How many of your monthly bills are paid using online banking



Count of How many of your monthly bills are paid using online banking

Interpretation: From the above data 70% of people pay their 0-5 monthly bills using online banking services, 22% people pay 5-10 monthly bills online, 4% of people pay 10-15 and 15-20 bills using online banking services every month

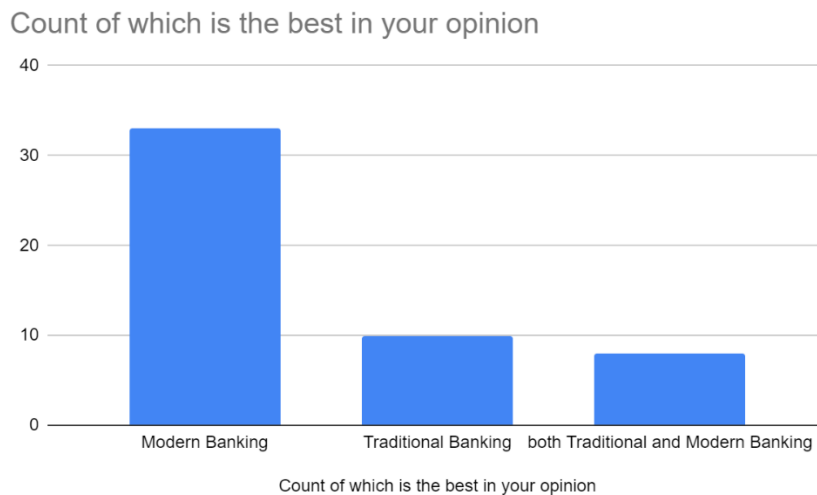
4.8 CLASSIFICATION SHOWING THE BEST MEDIUM ACCORDING TO THE OPINION OF THE TARGET MARKET

Table 4.8 Table showing the best banking service medium according to the opinion of the target market

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Traditional Banking	10	20
Modern Banking	33	66
Both Traditional and Modern Banking	7	14
TOTAL	50	100

Source- Primary Data

Figure 4.8 Figure showing the opinion of the target market on the best banking service medium



Interpretation: From the above data 66% of people suggest Modern Banking services as the best, 20% suggest traditional banking services, and 14% of people suggest both traditional and modern banking as the best in their opinion.

4.9 CLASSIFICATION SHOWING THE DIFFERENT ONLINE BANKING PLATFORM USED BY THE PEOPLE

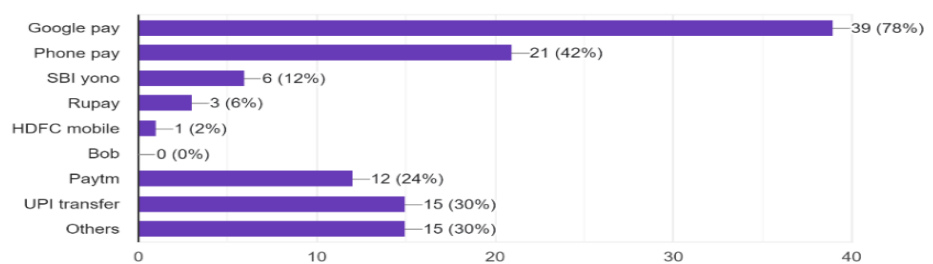
Table 4.9 showing the different online banking platforms used by the people

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Google Pay	39	78
Phone Pay	21	42
SBI yono	6	12
RuPay	3	6
HDFC Mobile	1	2
BoB	0	0
PayTM	12	24
UPI transfer	15	30
Others	15	30
TOTAL	50	100

Source- Primary Data

Figure 4.9 Figure showing the number of people using various online banking platforms

Which online banking platforms do you use
50 responses



Interpretation: From the above data 78% of the people use Google Pay, 42% of the people use Phone Pay, 30% of the people use UPI Transfer and other banking platforms other than the specified.

4.10 CLASSIFICATION SHOWING THE USAGE OF VARIOUS BANKING SOFTWARE APPLICATION PROVIDED BY THE BANK BY THE PEOPLE

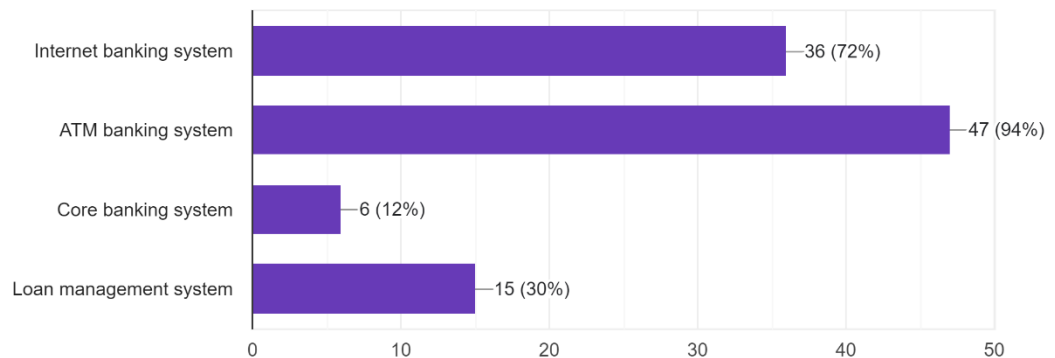
Table 4.10 showing the usage of various banking software application provided by the banks by the people

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Internet Banking System	36	72
ATM Banking System	47	94
Core Banking System	6	12
Loan Management System	15	30
TOTAL	50	100

Source- Primary Data

Figure 4.10 showing the usage of various banking software application provided by the banks by the people

Do you use any of the following types of banking software application provided by the banks
50 responses



Interpretation: From the above data 94% of people uses for ATM banking system, 72% of people uses internet banking system and 12% of people uses core banking system.

4.11 CLASSIFICATION SHOWING THE SATISFACTION OF THE PEOPLE IN USING ONLINE BANKING SERVICE PROVIDED BY THEIR BANK

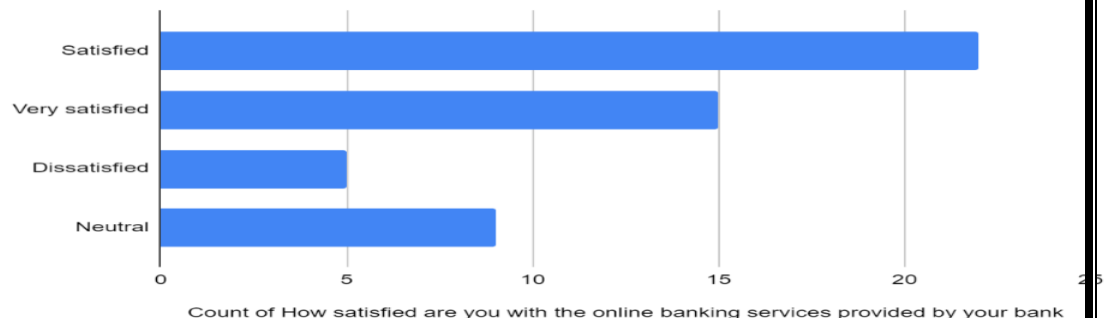
Table 4.11 showing satisfaction of people in using online banking services provided by their bank

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Very Satisfied	14	28
Satisfied	22	44
Neutral	9	18
Dissatisfied	5	10
Very Dissatisfied	-	-
TOTAL	50	100

Source- Primary Data

Figure 4.11 showing satisfaction of people in using online banking services provided by their bank

Count of How satisfied are you with the online banking services provided by your bank



Interpretation: From the above data 44% of the people are satisfied with the online banking services provided by their bank, 28% of the people are very satisfied, 18% of the people are naturally satisfied and 10% of the people are dissatisfied.

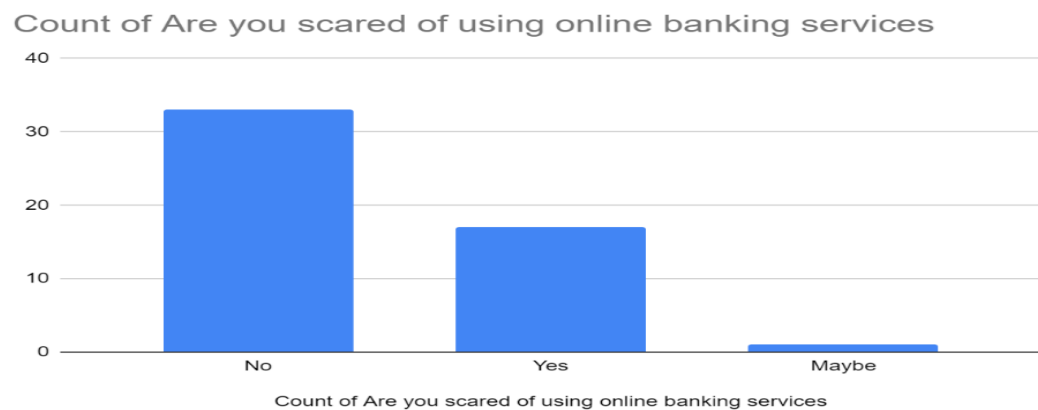
4.12 CLASSIFICATION SHOWING THE NUMBER OF PEOPLE WHO FEAR USING ONLINE BANKING SERVICES

Table 4.12 showing the number of people who fear using online banking services

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Yes	17	34
No	32	64
May Be	1	2
TOTAL	50	100

Source- Primary Data

Figure 4.12 showing the number of people who fear using online banking services



Interpretation: From the above data 64% of the people are not scared of using online banking services. Whereas 34% of the people fear using online banking services and only 2% of the people are in a neutral situation.

4.13 CLASSIFICATION SHOWING THE NUMBER OF PEOPLE WHO HAVE EXPERIENCED BANKING FRAUDS

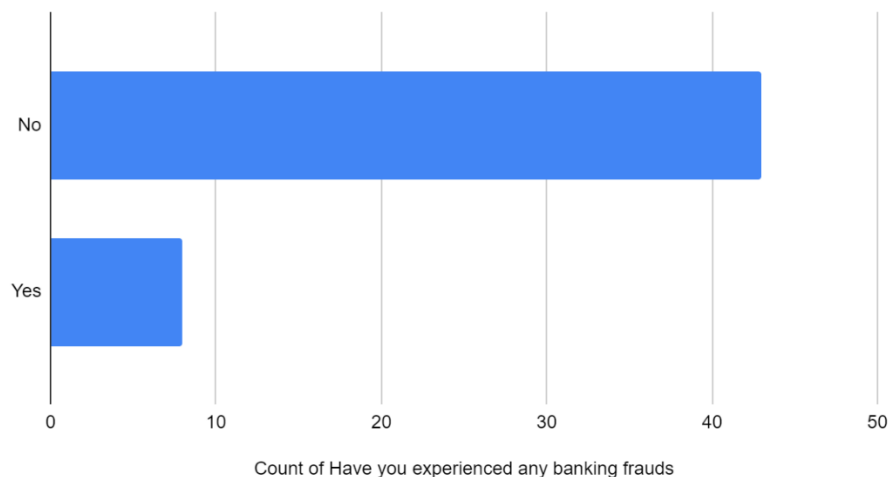
Table 4.13 showing the number of people who have experienced banking frauds

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Yes	8	16
No	42	84
TOTAL	50	100

Source- Primary Data

Figure 4.13 showing the number of people who have experienced banking frauds

Count of Have you experienced any banking frauds



Interpretation: From the above data 84% of the people have not experienced any kind of banking fraud. Whereas 16% of the people have experienced banking frauds.

4.14 CLASSIFICATION SHOWING THE AWARENESS OF PEOPLE ABOUT EXISTING TYPES OF ONLINE BANKING FRAUDS

Table 4.14 showing the number of people who are aware about any of the existing types of online banking frauds

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Identity Theft	30	60
Skimming	9	18
Phishing	8	16
Credit card frauds	25	50
Chargeback frauds	3	6
Advance fee scam	14	28
Malware	3	6
Scamming through Government schemes	18	36
Others	6	12
TOTAL	50	100

Source- Primary Data

Figure 4.14 showing the number of people who are aware about any of the existing types of online banking frauds



Interpretation: From the above data 60% of the people are aware of identity theft, 50% of the people are aware of various credit card frauds and 36% of the people are aware about various scams through government schemes.

4.15 CLASSIFICATION SHOWING THE SOURCE THAT PEOPLE KNOW ABOUT ONLINE BANKING FRAUDS

Table 4.15 showing the source how people know about online banking frauds

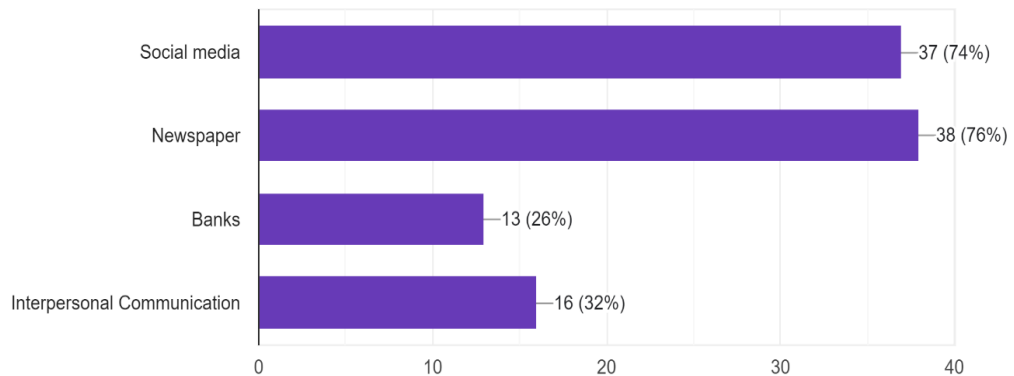
CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Social media	37	74
Newspaper	38	76
Banks	13	26
Interpersonal communication	16	32
TOTAL	50	100

Source- Primary Data

Figure 4.15 Figure showing the source how people know about online banking frauds

From what sources you get to know about the online banking frauds

50 responses



Interpretation: From the above data 76% of people know about online banking frauds through newspaper, 74% through social media, 32% through interpersonal communication and 26% through Banks.

4.16 CLASSIFICATION OF PERSONS WHO HAVE BEEN VICTIMS OF ONLINE BANKING FRAUDS.

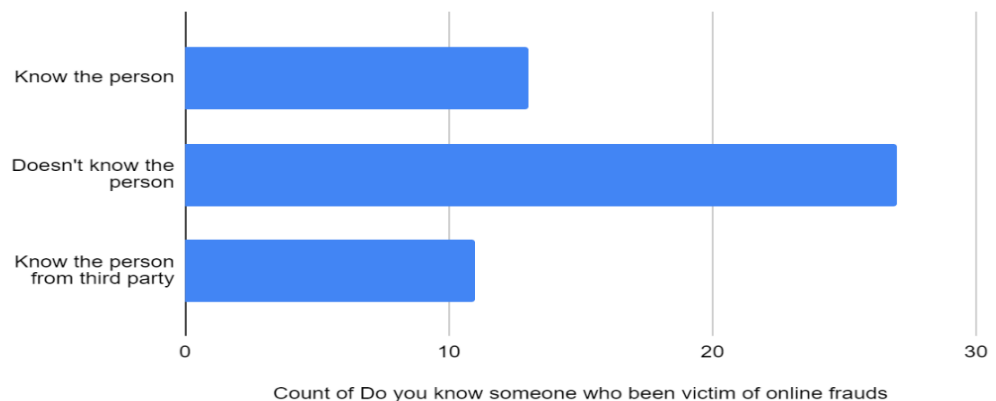
Table 4.16 showing the number of persons who have been the victims of online banking frauds.

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Know the person	12	24
Know the person from third party	11	22
Does Know the person	27	54
TOTAL	50	100

Source - primary Data

Figure 4.16 showing the number of people who have been victims of online banking frauds.

Count of Do you know someone who been victim of online frauds



Interpretation: From the above data 54% of the person Doesn't know the victims of online banking frauds, 24% of people know the victims, 22% know the person from third party

4.17 CLASSIFICATION SHOWING DIFFERENT WAYS TO PREVENT BANKING FRAUDS

Table 4.17 showing different ways to prevent banking frauds

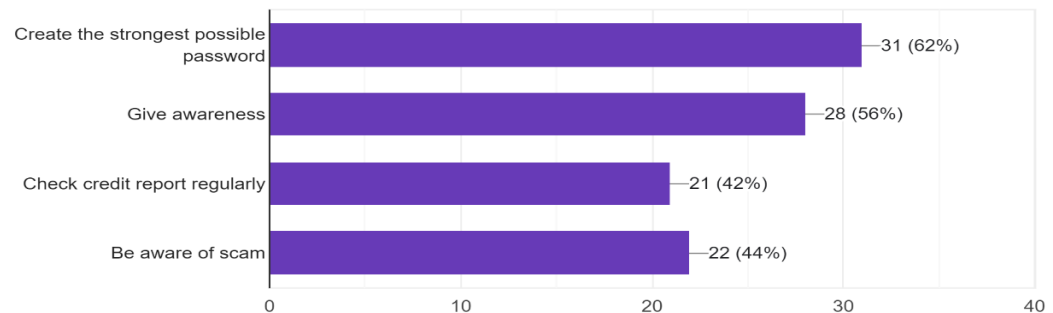
CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Create the strongest possible password	31	62
Give awareness	28	56
Check credit report properly	21	42
Be aware of scam	22	44
TOTAL	50	100

Source - Primary Data

Figure 4.17 showing different ways to prevents banking frauds

Which of these ways you opt to prevent banking frauds

50 responses



Interpretation: From the above data 62% of people suggest that create the strongest possible password to prevent banking frauds, 56% people suggest Give awareness, 44% people suggest that Be Aware of scams and 42% of people suggest that check credit report properly.

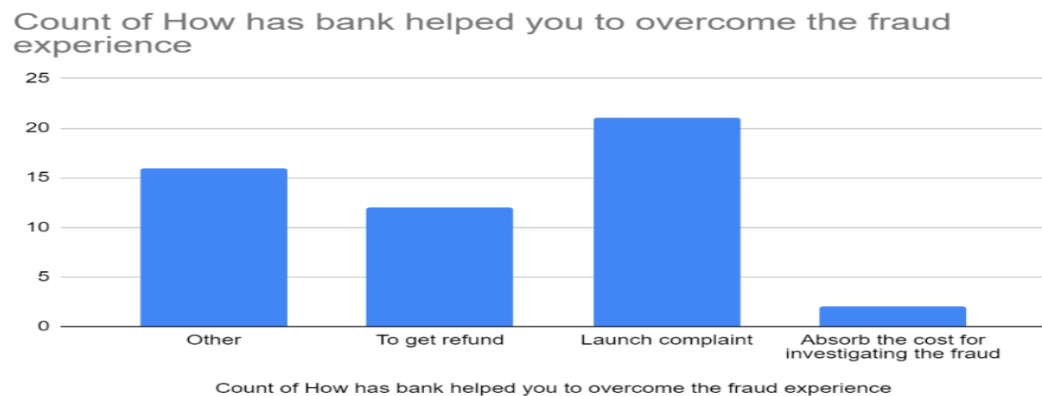
4.18 CLASSIFICATION SHOWING HOW BANK HELP YOU TO OVERCOME THE FRAUDS EXPERIENCE

Table 4.18 showing how banks help peoples to overcome the frauds experience

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Launch complaint	21	42
To get refund	12	24
Absorb the cost for investigating the frauds	2	4
Others	15	30
TOTAL	50	100

Source - Primary Data

Figure 4.18 showing how banks help peoples to overcome the frauds experience



Interpretation: From the above data 42% of people suggested to launch complaint, 30% of people preferred any other means to overcome the fraud experience, 24 % would likely to get refund, and 4% of people preferred to absorb the cost for investigating the frauds

4.19 CLASSIFICATION SHOWING AWARENESS ABOUT THE IMPACT OF ONLINE FRAUDS FACED BY THE ONLINE BANKING USERS

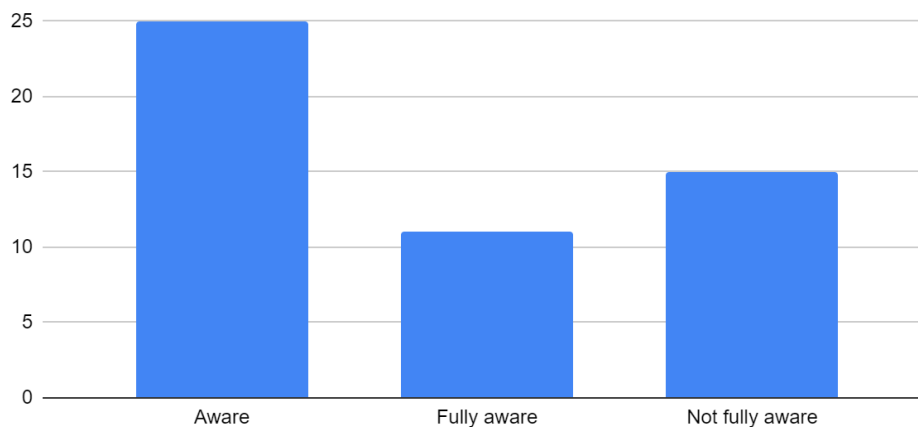
Table 4.19 showing awareness about the impact of online frauds faced by the online banking users

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Fully aware	10	20
Aware	25	50
Not fully aware	15	30
Not aware	-	-
TOTAL	50	100

Source– Primary Data

Figure 4.19 showing the level of awareness about the impact of online frauds faced by online banking users

Count of What level of awareness do you have about the impact of online frauds faces by online banking users



Count of What level of awareness do you have about the impact of online frauds faces by online b...

Interpretation: From the above data 50% are aware of online banking frauds, 30% are not fully aware and 20% of people are fully aware about the impact of online banking frauds.

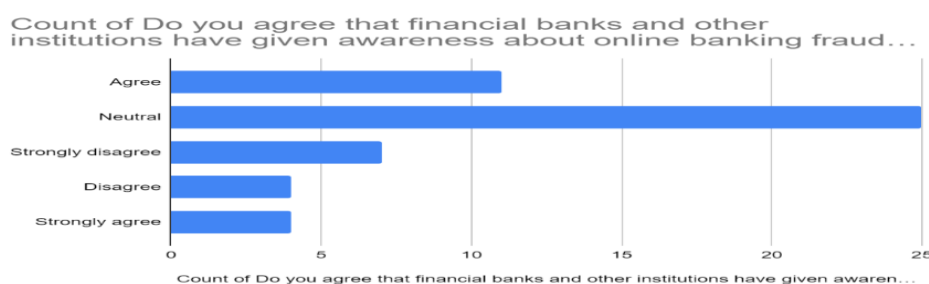
4.20 CLASSIFICATION SHOWING THE LEVEL OF AWARENESS GIVEN BY FINANCIAL BANKS AND OTHER INSTITUTIONS ABOUT ONLINE BANKING FRAUDS PREVAILING IN INDIA.

Table 4.20 showing the level of awareness given by financial banks and other institutions about online banking frauds prevailing in India.

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Strongly agree	4	8
Agree	11	22
Neutral	25	50
Disagree	4	8
Strongly disagree	6	12
TOTAL	50	100

Source- Primary Data

Figure 4.20 showing the level of awareness given by financial banks and other institutions about online banking frauds prevailing in India.



Interpretation: From the above data 50% of people have neutral opinion that financial banks and other institutions have given awareness about online banking frauds prevailing in India, 22% are agree to the statement, 12% are strongly disagree, 8% are strongly agree and disagreed.

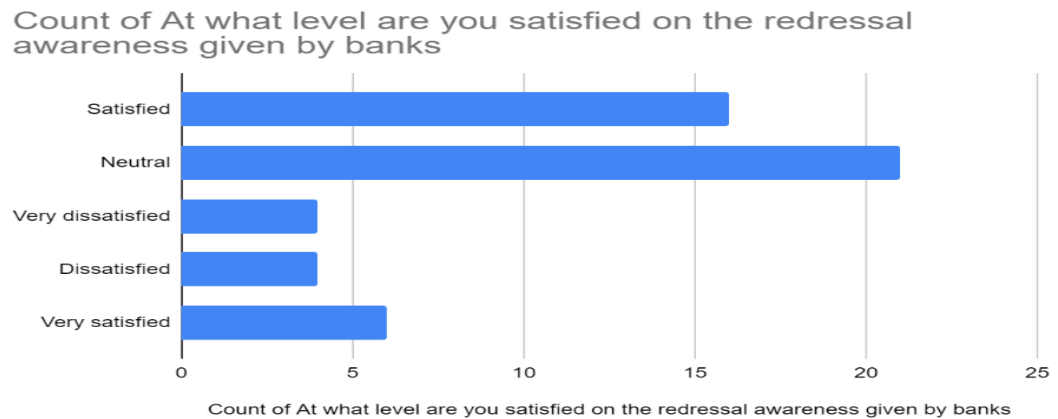
4.21 CLASSIFICATION SHOWING SATISFACTION OF THE REDRESSAL AWARENESS GIVEN BY BANK

Table 4.21 satisfaction of people on redressal awareness given by banks

CATEGORY	NO. OF RESPONDENTS	PERCENTAGE (%)
Very satisfied	6	12
Satisfied	16	32
Neutral	21	42
Dissatisfied	4	8
Very dissatisfied	3	6
TOTAL	50	100

Source– Primary Data

Figure 4.21 showing satisfaction of people on redressal awareness given by banks



Interpretation: From the above data 42% of people have opinion Neutral on the satisfaction of redressal awareness given by banks, 32% of people are satisfied, 12% of people are very satisfied, 8% are Dissatisfied and 6% are very Dissatisfied.

4.22 CLASSIFICATION SHOWING DIFFERENT FORM OF COMMUNICATION THAT PREFERRED BY THE BANKS IN ORDER TO INCREASE THE LEVEL OF RISK AND AWARENESS ON ONLINE FRAUDS

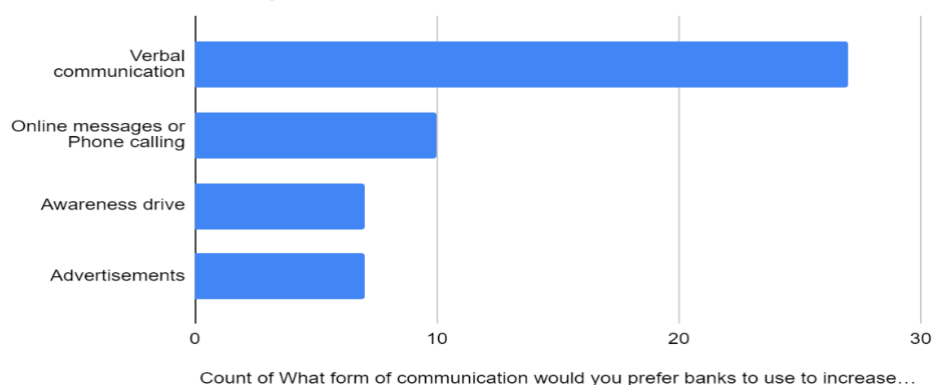
Table 4.22 showing different form of communication that preferred by the banks in order to increase the level of risk and awareness on online frauds

CATEGORY	NO. OF RESPONDENT	PERCENTAGE (%)
Verbal communication	27	54
Awareness drive	7	14
Online messages or phone calling	10	20
Advertisement	6	12
TOTAL	50	100

Source- Primary Data

Figure 4.22 showing different form of communication that preferred by the banks in order to increase the level of risk and awareness on online frauds

Count of What form of communication would you prefer banks to use to increase your level of risk and awareness on online...



Interpretation: From the above data 54% of people preferred verbal communication for banks in order to increase the level of risk and awareness on online frauds, 20% are online messages or phone calling, 14% of people prefer Awareness drive and 12% are Advertisement.

CHAPTER - 5

FINDINGS, SUGGESTIONS AND CONCLUSION

5.1 FINDINGS

- 50 percent of people belong to 45-50 years in the primary data collected from the public.
- A majority of 38 percent of people completed their 10th standard in the data collected.
- A majority of 40 percent of people are salaried in the data collected.
- 76 percent of people are online banking users.
- 64 percent of people use online banking services once in a week.
- 29 percent of people have not saved their banking details on their phone.
- 70 percent of people pay their 0-5 monthly bills using online banking services.
- 66 percent of people suggest Modern Banking services as the best.
- 78 percent of the people use Google Pay as their major online banking platform.
- 94 percent of the people use ATM Banking services.
- 44 percent of the people are satisfied with the online banking services provided by their bank.
- 64 percent of the people are not scared of using online banking services.
- 84 percent of the people have not experienced any kind of banking fraud.
- 60 percentage of the people are aware of identity theft only.
- 76 percent of people know about online banking frauds through newspapers.
- 54 percentage of the people Don't know any victims of online banking frauds.
- 62 percent of people suggested creating the strongest possible password to prevent banking frauds.
- 42 percent of people suggested to launch complaint to overcome the fraud experience.
- 50 percent are aware of online banking frauds.
- 50 percentage of people have neutral opinion that financial banks and other institutions have given awareness about online banking frauds prevailing in India.
- 42 percentage of people have Neutral opinion on the satisfaction of the redressal awareness given by banks.

- 54 percentage of people preferred verbal communication for banks in order to increase the level of risk and awareness on online frauds

5.2 SUGGESTIONS

- The educated managers and other high authorities should not only do their job, but they also should socially engage with the customers.
- Conduct several awareness programs on how to use online banking and on how to fully avail all the online banking services provided by the banks.
- Strong awareness should be provided to illiterate people in order to spread the use of banking services to the underdeveloped society.
- Banks should be more transparent about banking procedures to save the customers from fraud.

5.3 CONCLUSION

From the mid-1990s, banks usually carried down their activities by making face to face connections with their customers which ensured loyalty. The rapid development of internet and modern electronic gadgets from the mid-2000s converted the traditional face to face method to online (faceless connection) method. And this made a drastic increase in the number of cybercrimes related to online banking.

The main objective of the study was to check the level of awareness about online banking frauds, measures against banking frauds among the middle-aged adults. The findings of the study were positive that the majority among the random respondents were aware about many of the online banking fraudulent activities around them. Even though they were aware, it is pity to know that a few of them still have a history of banking fraud experienced. This fact made the study more relevant in the scenario. From this study, it was able to understand the satisfaction level of the customers in the online banking services provided by the respective banks and the level of trust of people to their banks. The study has gathered relevant evidence proving the above statements.

In conclusion, online banking has gained momentum through various platforms and banking applications in recent years. To maintain this and ensure transparency and safety, banks should ensure safety and security in their services to customers and also maintain fair and frequent communication with their customers. This can help them to gain the trust and loyalty of the customers. Banks should also be more

transparent in the procedure after the fraudulent activities and also should promote various awareness programs in order to make people feel more secure to invest in them. On the other hand, Government and RBI should develop appropriate measures to decrease the number of crimes related to online banking. Thus, this study can be considered as an eye-opener to the banking industry to provide reforms in their existing services in the online sector.

BIBLIOGRAPHY

JOURANAL ARTICLES:

Dr. Sukhamaya Swain, Dr. Lalata K Pani (2016) *Frauds in Indian banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures*. International Journal of Business and Management Invention. Volume 5 Issue 7.

Vishal Goyal, Dr. U. S.Pandey, Sanjay Batra (2012) *Mobile Banking in India: Practices, Challenges and Security Issues*. International Journal of Advanced Trends in Computer Science and Engineering. Volume 1, No.2.

Mohan,Murali,Pulella; (2000) *An Analytical Study on Bank Frauds and Scams in India*. (Chapter III, V, VII, VIII)

Dr. Gurmeet Singh, Dr. Simanpreet (2023) *Bank Frauds Reported in India: A Case Study*. Journal of Pharmaceutical Negative Results. Volume 14, Special Issue 2.

Dr. Eneji, Samuel Eneji; Angib, Maurice Udie; Ibe, Walter Eyong; Ekwegh, Kelechukwu Chimdike. (2019) *A Study of Electronic Banking frauds detection and control*. International Journal of Innovative Science and Research Technology. Volume 4, Issue 3, March – 2019.

Dr. Seema Thakur (2018) *Electronic Banking Frauds in India: Effects and Controls*. International Journal of Science and Research: 823-829

Dr. Prakash Pinto and Amit Donald Menezes (2016) *Banking Frauds and Ways to Prevent them*. International Journal of Current Research and Modern Education: 238-243

Dr. Anita Manna and Mr. Rupesh D Dubey (2017) *E-Banking Frauds and Frauds Risk Management*. Tactful Management Research Journal: 20-23

Rachel Baker (2018) *Awareness Creation on E-Banking Frauds Prevention: A Knowledge Management Perspective for E-Security and Customer Relationship Building*. Strategica 2018 University of South Africa: 656-672

Abhilasha Sharma and Dr. C P Gupta (2021) *Banking Frauds in India: Trends and Legal challenges*. International Journal of Education, Modern Management, Applied Science & Social Science: 276-280

Bhavin P P and Dr. D Mahila Vasanthi Thangam (2019) *Banking Frauds in India; A case study analysis*. Journal of Emerging Technology and Innovative Research. Volume 6, Issue 1: 29-35

Abu Bakar Sade, Alawa Clement Behora, Wan Fadzilah Wan Yusoff, and Rashad Yazdanifard (2011) *Electronic Banking Frauds; The Need to Enhance Security and Customer Trust in Online Banking*. International Journal in Advances in Information Science and Service Sciences 3(10.61): 505-509

Ms. Sarika Digamberrao Gudup (2016) *The Study of Frauds and Safety in E-Banking*. Anveshana's International Journal of Research in Regional Studies. Law, Social Science, Journalism and Management Practices, Volume 1 issue 8: 213-216

Rute Abreu, Fatima David and Liliane Segura (2016) *E-banking services: Why fraud is important*. Journal of Information Systems Engineering & Management, 1:2 (2016), 111-121

Aravind T Sajeev, Archana R Nair and Dr. Prasanth A P (2023) *A Study on awareness of E-Banking Frauds with Reference to bank customers in Kerala*. Eur. Chem. Bull. 2023, 12(Special Issue 6), 5184-5198

Ilker Kara (2021) *Electronic Banking (e-Banking) Fraud with Phishing Attack Methods*. European Journal of Science and Technology. Avrupa Bilim ve Teknoloji Dergisi.

Sen, Sunanda (2009) *Speculation, Scams, Frauds and Crises: Theory and Facts*. Economic and Political Weekly (Vol. 44, No. 12)

Shabbir, Aysha; Shabir, Maryam; Javed, Rehman, Abdul; Chakraborty, Chinmay; Rizwan, Muhammed (2021) *Suspicious Transaction Detection in Banking Cyber-Physical Systems*.

Wodo, Wojciech Dr.; Blaskiewicz, Przemyslaw, Dr. (2021) *Evaluating the Security of Electronic and Mobile Banking*. Computer Fraud and Security (Vol. 2021, Issue 10, 8-14)

Bandyopadhyay, R.; Patel, K., V. (1987) *Development Banking in Rural Areas*. Economic and Political Weekly (Vol. 22, No. 16)

Priyanka Datta, Sarvesh Tanwar, Surya Narayan Panda (2020). *Security and Issues of M-Banking: A Technical Report*. 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). Amity University, Noida, India. June 4-5, 2020.

Khanna, Ashu, Arora, Bindu (2009) *A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry.* International Journal of Business Science & Applied Management (Vol.4, Issue 3, pg 1-21)

Hoffmann, O I Arvid; Birnbrich, Cornelia (2012) *The impact of fraud prevention on bank-customer relationships- An empirical investigation in retail banking.* International Journal of Bank Marketing (Vol. 30 No. 5, 2012 pp. 390-407)

A. Ali, Mostafa; Hussin, Nazimah; A. Abed, Ibtihal (2019) *E-banking fraud Detection: A Short Review.* International Journal of Innovation, Creativity and Change (pg. 67)

Singh, Charan; Satishkumar, Dixit, Divyesh; Antony, Kiran; Agarwala Mohit; Kant, Ravi; Nayak Siddharth; Mukunda. S; Pattanayak, Deepanshu; Makked, Suryaansh; Singh, Tamanna; Mathur, Vipul (2016) *Frauds in the Indian Banking Industry.* IIM Bangalore Research Paper No. 505

WEBSITE:

Theory on banking frauds:

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

<https://www.cleafy.com/insights/what-is-online-banking-fraud-and-how-to-prevent-it>

<https://www.aubank.in/blogs/8-different-types-of-digital-banking-frauds>

<https://testbook.com/banking-awareness/internet-banking-awareness>

<https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=3407>

<https://www.fool.com/the-ascent/banks/articles/7-security-risks-mobile-banking-how-avoid-them/>

<https://www.identityguard.com/news/risks-of-using-mobile-banking-apps>

<https://www.wallstreetmojo.com/mobile-banking/#h-mobile-banking-features>

<https://www.bankrate.com/banking/checking/benefits-of-mobile-banking/#why-should>

<https://www.palisadesfcu.org/blog/mobile-banking-benefits>

<https://iasbaba.com/2023/02/day-73-q-3-evaluate-the-measures-taken-by-the-government-to-enhance-digital-security-and-prevent-cyber-crimes-including-money-laundering-discuss-the-role-of-international-cooperation-and-diplomacy/>

<https://www.zeebiz.com/personal-finance/banking/news-rbi-reserve-bank-of-india-rbi-annual-report-economy-indian-economy-rbi-governor-rbi-shaktikanta-das-rbi-data-rbi-private-sector-banks-digital-payments-237869>

<https://pib.gov.in/PressReleaseDetail.aspx?PRID=1980562>

ANNEXURE

QUESTIONNAIRE

Note: This interview schedule is prepared as part of doing Bachelor's Degree of Commerce at St. Teresa's College (Autonomous), Ernakulam. Your kind co-operation in filling is requested. All the responses will be used for academic purpose only.

BASIC QUESTIONS

➤ Name _____

➤ Age

- a) 30-35
- b) 35-40
- c) 40-45
- d) 45-50

➤ Education qualification

- a) 10th
- b) 12th
- c) Undergraduate
- d) Postgraduate
- e) Others

➤ Occupation

- a) Public service
- b) Self employed
- c) Salaried
- d) Part timer
- e) others

➤ Which bank you have account in _____

MAIN QUESTIONS

1. Are you an online banking User?
 - a) Yes
 - b) No

2. How often do you use online banking service
 - a) daily
 - b) once in a week
 - c) once in a month
 - d) once in a year
 - e) not used

3. Is your banking details saved in your mobile phone
 - a) Yes
 - b) No
 - c) May be

4. How many of your monthly bills are paid using online banking?
 - a) 0-5 times
 - b) 5-10 times
 - c) 10-15 times
 - d) 15-20 times

5. which one is best in your opinion traditional banking or online banking
 - a) Traditional banking
 - b) Online banking
 - c) Both traditional and online banking

6. Which online banking platform do you use?
 - a) Gpay
 - b) Phonepay
 - c) SBI yono
 - d) Rupay
 - e) HDFC mobile

- f) Advance fee scam
- g) Malware
- h) Scamming through Govt schemes
- i) Others

12. From what sources you get to know about the online bank frauds

- a) social media
- b) newspaper
- c) banks
- d) interpersonal communication

13. Do you know someone who been victim of online frauds

- a) know the person personally
- b) know the person from a third party
- c) doesn't know any person

14. Which of these ways do you opt to prevent banking frauds?

- a) Create the strongest possible password
- b) Give awareness
- c) Check your credit report
- d) Be aware of scam

15. How has the bank helped you to overcome the fraud experienced?

- a) Launch complaint
- b) To get refund
- c) Absorb the cost for investigating the frauds
- d) Other

16. what level of awareness do you have about the impact of online frauds faced by online banking users.

- a) fully aware
- b) partially aware
- c) Aware
- d) fully not aware
- e) not aware

17. Do you agree that banks and other financial institutions have given awareness about online banking frauds prevailing in India

- a) strongly agree
- b) agree
- c) neither agree or disagree
- d) disagree
- e) strongly disagree

18. At what level are you satisfied on the redressal awareness given by banks

- a) very much satisfied
- b) Satisfied
- c) Neutral
- d) Unsatisfied
- e) Very unsatisfied

19. what form of communication would you prefer banks to use to increase your level of risk and awareness on online frauds

- a) verbal communication
- b) awareness drive
- c) online messages or phone calling
- d) advertisements

20. Do you have any suggestions for further improvement in banking services in your area to avoid bank fraud?

- a) _____
- b) _____
- c) _____