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 BANKING FRAUDS AMONG YOUNGSTERS WITH SPECIAL REFERENCE TO KUZHUPPILLY PANCHAYAT"** submitted to Mahatma Gandhi University in partial fulfillment of the requirement for the award of Degree of Bachelor in Commerce is a record of the original work done by **Ms. Akshara Sajy, Ms. Alaina Ann Roy, Ms. Nikitha Evegin** under my supervision and guidance during the academic year 2021-24.

Project Guide

Ms. SNEHA ABRAHAM	**Smt.JiniJustinD'Costa**
Assistant Professor	**(Head of the Department)**
Department of Commerce(SF)	**Department of Commerce (SF)**

Viva Voce Examination held on **ExternalExaminer(s)**

DECLARATION

We **Ms. Akshara Sajy, Ms. Alaina Ann Roy, Ms. Nikitha Evegin**, final year B.Com students, Department of Commerce (SF), St. Teresa's College (Autonomous) do hereby declare that the project report entitled "**A STUDY ON BANKING FRAUDS AMONG YOUNGSTERS WITH SPECIAL REFERENCE TO KUZHUPPILLY PANCHAYAT"** submitted to Mahatma Gandhi University is a bonafide record of the work done under the supervision and guidance of **Ms. Sneha Abraham**, 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 **AKSHARA SAJY**

DATE: **ALAINA ANN ROY**

NIKITHA EVEGIN

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 **Ms. Sneha Abraham**, 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.

AKSHARA SAJY

ALAINA ANN ROY

NIKITHA EVEGIN

CONTENTS

LIST OF TABLES

LIST OF FIGURES

‘A STUDY ON BANKING FRAUDS AMONG YOUNGSTERS WITH SPECIAL REFERENCE TO KUZHUPPILLY PANCHAYAT’

CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

Finance plays a crucial role in shaping economic landscapes, and in India, it is a dynamic sector that undergoes constant evolution. With a diverse financial ecosystem encompassing banking, capital markets, and emerging fintech, India's financial sector contributes significantly to the country's economic growth. The Reserve Bank of India (RBI) acts as the central regulatory authority, steering monetary policies and ensuring financial stability. The Indian stock markets, represented by BSE and NSE, serve as key platforms for equity trading. Additionally, the government's initiatives like demonetization and GST have aimed to streamline financial processes. As India continues its journey towards economic development, the finance sector remains integral, influencing investment, entrepreneurship, and overall fiscal well-being.

In a developing nation like India, banks and banking services have become a crucial part of any normal Indian citizen’s life because each of its services are individually designed to make money management and personal finance more efficient and easier. According to 2021 data, 78 percent of Indians above the age of 15 years have an account at the bank. This indicates that banking services have become increasingly accessible to Indian youth, offering a wide range of services and functions, from banking to loans and investments. However, this convenience has also led to a rise in banking frauds among this demographic.

In the recent economic times banking frauds are becoming more popular among the Indian economy. Banking frauds happening in today's economy has become more deceitful and cunning with the use of technology, operated under the wrong hands. According to the RBI annual report 2022-23, the most number of banking frauds have occurred in the digital payment category. In this modern era, especially among the youth, people are more inclined to using digital platforms for transactions varying from day to day purchases to huge sum settlements. With limited experience in financial matters and the eagerness to explore digital platforms, many youngsters fall prey to these fraudulent activities.

Digital banking frauds often exploit vulnerabilities in online banking systems. To heighten awareness of banking frauds among the youth several key strategies can be adopted such as conducting education initiatives, spreading online safety awareness, using secure banking apps etc. Therefore by combining these strategies and fostering a culture of proactive vigilance, the youth can better safeguard themselves against banking frauds.

1.2 STATEMENT OF THE PROBLEM

Banking refers to the industry and practice of accepting deposits, lending funds, and providing various financial services to individuals, businesses, and governments. It encompasses activities such as storing money, issuing loans, facilitating transactions, managing investments, and offering financial advice. In essence, banking is the backbone of economic activity, facilitating the circulation of money and the efficient allocation of resources.

Limited research might be found on the specific factors contributing to banking frauds among youngsters in the context of Kuzhuppilly Panchayat, such as socio-economic influences, awareness levels, and the role of local institutions. Additionally, exploring the effectiveness of preventive measures or educational programs specifically tailored for this demographic within the mentioned locality could be an area where research is lacking. Understanding the unique challenges and patterns of banking fraud in a localized context like Kuzhuppilly Panchayat can contribute valuable insights to the broader discourse on financial security and fraud prevention.

In recent times, the landscape of banking fraud has undergone a notable shift, especially among the younger demographic. This study focuses on exploring banking frauds prevalent among the youth, with a unique emphasis on the Kuzhuppilly panchayat. Moreover, it aims to delve into the level of awareness and

understanding among the population about the relatively new threat of "juice jacking". By analyzing these factors, this study seeks to shed light on the evolving nature of financial security challenges and the crucial need for awareness in safeguarding against such risks in today's digital era.

1.3 SIGNIFICANCE OF THE STUDY

This study holds significant importance as it aims to delve into the unique challenges and patterns of banking fraud within Kuzhuppilly Panchayat, thereby offering specific insights that contribute to a more nuanced understanding of the issue. By informing policymakers, financial institutions, and local authorities, it facilitates the design of targeted interventions and preventive measures tailored to the needs of the young population in the region, ultimately fostering a more secure financial environment. Moreover, the study's findings have the potential to extend beyond Kuzhuppilly Panchayat, contributing to the broader goal of enhancing financial literacy and security in similar socio-economic contexts. Through the practical insights generated, this study not only addresses banking fraud but also serves to promote financial well-being and create a secure financial landscape for the youth both locally and potentially on a wider scale.

1.4 OBJECTIVES

1.To analyze the level of awareness among people about different banking scams and frauds.
2.To identify the different mechanisms used by banks to prevent banking scams and frauds.
3.To identify the level of satisfaction of the various redressal mechanisms adopted by banks.
4.To examine the people’s level of awareness about the banking fraud juice jacking.

1.5 RESEARCH METHODOLOGY

1.5.1 Research Design

The present study is quantitative and analytical in nature. It is quantitative because it involves numerical expression. And it is analytical since it examines, analyses and interprets collected data in order to arrive at conclusion.

Research Instrument: Empirical research was implemented as our study was based on observations as well as measurements and our conclusions were drawn from verifiable evidence.

1.5.2 Collection of data: Both primary and secondary data were used for data collection

- **Primary data:** The data which is collected from primary sources that is a source of origin from where the data is generated, they are collected for the first time by an investigation or any agency for any statistical analysis. For collecting primary data we use the method of questionnaire. The questionnaire is a major technique for collection of primary data. The questions were asked and the data was collected individually from each respondent by interviewing them in Kuzhuppilly

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

1.5.3 Sample Design: Information was collected from the people of Kuzhuppilly which forms the universe of the study. The number of sampling units from the universe is called the size of the sample. From the universe, about 100 people were selected and were asked about their banking status and habits.

Sample size: Out of the total people in Kuzhuppilly, a sample size of 100 was selected for survey.

1.5.4 Sampling Technique: Stratified random sampling technique was followed for the study. One of the reasons to adopt this technique is that all are aware about this topic. Statistically, to arrive at conclusions, data were analyzed by using percentage analysis. MS Word, MS Excel, Power Bi were the software used to analyze and present the data.

Sampling Method ——————————> Stratified Random Sampling Method

1.5.5 Tools for analysis: The collected data were interpreted with the help of graphical tools like pie chart, bar graph, histogram, line graph, cumulative frequency and cross tabulation for better understanding.

1.6 SCOPE OF THE STUDY

This study on banking frauds will focus on understanding the prevalence, types, and impacts of fraudulent activities within the banking sector. Geographically, the proposed study is confined to the Kuzhuppilly panchayat in Kerala. The study will explore various types of frauds, including identity theft, phishing, insider fraud, and cyberattacks, along with the detection and prevention mechanisms employed by banks and regulatory bodies. Analytically, it will assess the extent of banking frauds and their implications on financial institutions, customers, and the economy. Finally, the study will provide recommendations for enhancing fraud detection and prevention strategies, strengthening regulatory oversight, and educating stakeholders to effectively combat banking frauds.

1.7 LIMITATIONS

- The geographical area of this study is confined to the Kuzhuppilly area only.
- The size of the sample compared to the population is small and hence it might not signify the ideas of the entire population.
- The lack of knowledge of customers about the various banking frauds and its preventive methods can be a major limitation.

CHAPTER II

REVIEW OF LITERATURE

Banking scams and frauds have emerged as a formidable challenge in the financial sector, with the advent of digital technology providing new avenues for criminal activities. A literature review on this topic would encompass an analysis of the various methods employed by fraudsters, the impact on consumers and financial institutions, and the countermeasures that can be implemented to mitigate these risks.

The awareness of banking scams among youngsters is a critical area of study, especially in an era where digital transactions are becoming the norm. A literature review on this topic would explore the extent to which young people are informed about the risks associated with online banking and the prevalence of fraudulent schemes targeting this demographic.

The refined articles that have investigated show in detail about banking scams and its awareness among youngsters. The articles are:

- **ASHU KHANNA AND BINDU ARORA (2009)**- In their examination entitled "A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry" endeavored to discover the issues related to the internal control segment of the banking industry that can be responsible for banking frauds. The study describes how much a banking employee should be aware of the various frauds and its prevention methods.It also aims to prove how a strong system of internal costal and good employment practices and training can lead to fewer banking frauds and better preventive actions.

- **DANIEL RATHINARAJ, CHENDRAYAN CHENDROYAPERUMAL (2010)-** This paper seeks to address and analyze some issues related to the use of cyberspace for fraud by cyber scammers especially Financial Fraud and the techniques used. It will also provide an analysis of the existing legislative and regulatory framework and their efficiency in combating this form of cross-border crime taking India as a case study. This paper presents the historical

origin of financial frauds and presents a small survey of some popular financial frauds committed in the recent years in India.

- **KUNDU, S. AND RAO, N., (2014)-** have studied the cases of fraud. A map of the typological trend strategy was adopted for prevention and implementation. Bank frauds arise due to unawareness, situational pressures, and liberal approaches. It was hard to identify in time and significantly harder to book the frauds on account of perplexing and legal prerequisites and procedures. In the dread of harming the banks' notoriety, frequently the cases of frauds are not generally uncovered.

- **PANI, L.K., SWAIN, S. AND SWAIN, S., (2014**)- This study discusses the various facets of fraud in the Indian banking sector and evaluated the statistics included with fraud premise secondary data available from reliable sources, and furthermore investigated the same. Each type, namely KYC associated and other technological features, was discussed with reasons, and they also discussed the different aspects of fraud in the Indian banking system.

- **CHARAN SINGH, DEEPANSHU PATTANAYAK, DIVYESH DIXIT, KIRAN ANTONY, MOHIT AGARWALA, RAVI KANT, S MUKUNDA, SIDDHARTH NAYAK, SURYAANSH MAKKED, TAMANNA SINGH, VIPUL MATHUR (IIM BANGALORE RESEARCH PAPER, 2016)-** The Indian banking sector has experienced considerable growth and changes since the liberalization of the economy in 1991. Though the banking industry is generally well regulated and supervised, the sector suffers from its own set of challenges when it comes to ethical practices, financial distress and corporate governance. 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.

- **YEGO, J.K., (2016)-** found that fraud is recognized as a crucia. crisis within the bank, even supposing the relative extent of fraud conducted was simple and

comparatively small. Currently, most banks use standard procedures to detect and prevent fraud. However, these procedures do not perform well. The Fraud Triangle (FT) functioned energetically to identify the motifs of bank frauds explained by the respondents. Yet, from this study, the author discovered that the FT is not successful in illuminating the predatory and collusive nature of instances such as the Kenyan bank fake - a major problem in the bank. Bhasin, M.L., 2016, conducted a survey based on a questionnaire in 2012- 13 among 345 bank staff "to know their opinion towards bank frauds as well as evaluate the aspects that influence the extent of their compliance point." And also discussed that "there were poor employment practices as well as lack of effective training; weak internal control systems, over-burdened staff and low compliance levels on the part of bank managers, officers, and clerks

- **RAMANA, S.V. AND KRISHNA, S.G., (2017)-** presented a detailed survey on banking fraud. The authors identified and explained the methods to determine and prevent fraud in small banking products. Further to this, they reported that the Indian banking sector was undergoing the pressure owing to the rise in fraud events in recent years. Retail banking is more procedure and volume- driven, and so amplified the fraud incidents in that area; increasing the need to stimulate a wider audit of procedures and preventing fraud. Business intelligence systems provide different ways to enhance the decision-making process.

- **ANTHALA, H.R., (2018)**- This study revealed the frauds and misconduct committed by criminals, outsiders, customers and employees of the banks and financial institutions and other State, Central and Local bodies, private and public sectors. Jeyanthi, P. M. (2018) specifies the Internet of People, Things & Services (loPTS) as the visualization where people, things and services are effortlessly integrated into the internet as active participants which exchange data about itself and their perceived nearby environments over a network-based infrastructure.

- **Dr D MAHILA VASANTHI THANGAM AND BHAVIN PP (2019)**- In this analysis “Banking frauds in India; A case analysis” discusses about the various

banking frauds happening around in India and also the legal actions taken against them. The study also includes the involvement of bank officials in these frauds. It also breaks down the various banking frauds happening in different sectors of the economy such as public, private and cooperative sectors. The study concludes by depicting public sectors are more vulnerable to banking frauds and the authorities have to take more vigilant steps in preventing them

- **PRIYANKA DATTA, SARVESH TANWAR, SURYA NARAYAN PANDA, AJAY RANA (2020)-** 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.

- **DEBABRATA SINGH, ANIL K SHARMA (2021)-** In the research study "Digital banking: A study of fraudulent practices in Indian banks" unveils about how digitalisation of banking services contributes towards raising banking frauds. The advancement in digitalisation has its advantages as well as its challenges. The study concludes with the impact of digitalisation on raising cyber frauds in the Indian banking sector.

- **Dr BHAVIK U SWADIA and BAXI MINOUTI KAIVALYA (2021)-** The paper "Study on banking frauds scenario in India" aims to study challenges of the banking sector in the modern economic environment. The banking sector has gone through a lot of changes through increasing economic variables working at both national and global level which not only enabled them to open new opportunities but also resulted in challenges for the banking sector.

- **NAMOSHA VEERASAMY PROCEEDINGS OF THE ECCWS 2021 20TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY, 449, (2021)-** This paper takes a closer look at this developing threat. These public charging stations are now being fraudulently used by attackers to gain access to sensitive information. Scammers are now using USB

chargers as a method to steal data or install malware. However, users may be unaware of the potential risk. In this research, the malicious use of USB charging stations found in spots popular with travelers are revealed. In addition, protective measures are described in order to help users from falling victim to this latest cyber threat. Attackers try to take advantage of the situation in that most users trust their mobile devices more than their desktop devices. In addition to data theft, malicious attackers could also cause destruction of our mobile devices.

- **ROHAN PRASAD GUPTA, BAPPADITYA BISWAS* MONEY LAUNDERING AND TERRORISM FINANCING IN GLOBAL FINANCIAL SYSTEMS, 304-324, (2021)-** In today's dynamic world, banking scams and frauds that are committed by willful defaulters are more technical and complex in nature. To tackle these crimes, banks need to improve their working system and technologies. In this chapter, cases of recent banking scams in India have been analyzed to find out the operational loopholes present in the system which led to such a crisis. Further, the measures taken by the Government of India to detect and prevent such scams have been discussed.

In conclusion, the awareness of banking frauds among youngsters is a vital component in safeguarding the financial future of this digitally native generation. As they navigate an increasingly online world, it is imperative that they are equipped with the knowledge and tools to recognize and prevent fraudulent activities. The literature suggests that while youngsters are generally in favor of digital banking products, there is a pressing need for enhanced educational programs that specifically address the risks associated with online financial transactions.

The impact of financial scams on young people can be profound, affecting not only their financial stability but also their trust in the banking system and their mental health. Therefore, it is crucial for parents, educators, and financial institutions to collaborate in fostering an environment of informed vigilance. By doing so, they

can empower young individuals to become savvy consumers who can contribute positively to the economy while protecting themselves and their assets from potential threats.

Ultimately, the collective effort to improve awareness of banking frauds among youngsters will not only benefit the individuals but also strengthen the integrity of the financial system as a whole. As the research indicates, prevention is better than cure, and proactive measures are essential in the fight against the ever-evolving landscape of banking frauds.

CHAPTER III

THEORETICAL FRAMEWORK

3.1 INTRODUCTION

Banking refers to the system of financial institutions, such as banks and credit unions, that provide various financial services to individuals, businesses, and governments. Banking services mainly include accepting deposits, lending money, facilitating transactions, and offering various financial products like savings accounts, loans, and credit cards. Banking plays a crucial role in the economy by facilitating the flow of money and enabling economic activities.

3.2 FUNCTIONS OF BANKING

Banks in India offer a wide range of banking services, such as savings and checking accounts, loans (personal, business, and mortgages), credit cards, investment services, and electronic banking options like online and mobile banking. Banks are fundamental to the financial infrastructure of any economy, serving as intermediaries between savers and borrowers and facilitating a wide range of financial activities. Here's an introduction to the functions of banking:

There are two types of functions of banks:
1. Primary functions
2. Secondary Functions

Both the types of functions of bank are explained below in detail:

3.2.1 Primary Functions of Bank

Banking serves several primary functions crucial to the functioning of modern economies. Banks facilitate the process of financial intermediation by gathering funds from depositors and channeling them to borrowers. This intermediation function allows for efficient allocation of capital in the economy, enabling

businesses to invest and grow, and individuals to finance their consumption needs. Banks provide payment services, allowing individuals and businesses to easily and securely transfer money domestically and internationally through various channels such as checks, electronic transfers, and debit/credit cards. Moreover, banks play a crucial role in risk management by assessing the creditworthiness of borrowers, managing liquidity, and diversifying their assets to mitigate financial risks. Lastly, banks contribute to economic stability by acting as lenders of last resort, providing liquidity during times of financial distress, and implementing monetary policies set by central banks to regulate the money supply and influence interest rates. Overall, banking functions are integral to the efficient functioning and stability of modern economies.

All banks have to perform two major primary functions namely:

1. Accepting of deposits
2. Granting of loans and advances

Accepting of Deposits

A very basic yet important function of all the commercial banks is mobilizing public funds, providing safe custody of savings and interest on the savings to depositors. Bank accepts different types of deposits from the public such as:

1. Saving Deposits: It Encourages saving habits among the public. It is suitable for salary and wage earners. The rate of interest is low. There is no restriction on the number and amo unt of withdrawals. The account for saving deposits can be opened in a single name or in joint names. The depositors just need to maintain a minimum balance which varies across different banks. Also, the Bank provides ATM cum debit card, cheque book, and Internet banking facility.

2. Fixed Deposits: Also known as Term Deposits. Money is deposited for a fixed tenure. No withdrawal money during this period allowed. In case depositors withdraw before maturity, banks levy a penalty for premature withdrawal. As a

lump-sum amount is paid at one time for a specific period, the rate of interest is high but varies with the period of deposit.

3. Current Deposits: They are opened by businessmen. The account holders get an overdraft facility on this account. These deposits act as a short term loan to meet urgent needs. Bank charges a high-interest rate along with the charges for overdraft facility in order to maintain a reserve for unknown demands for the overdraft.

4. Recurring Deposits: A certain sum of money is deposited in the bank at regular intervals. Money can be withdrawn only after the expiry of a certain period. A higher rate of interest is paid on recurring deposits as it provides a benefit of compounded rate of interest and enables depositors to collect a big sum of money. This type of account is operated by salaried persons and petty traders.

Granting of Loans & Advances

The deposits accepted from the public are utilized by the banks to advance loans to the businesses and individuals to meet their uncertainties. Bank charges a higher rate of interest on loans and advances than what it pays on deposits. The difference between the lending interest rate and interest rate for deposits is bank profit. Bank offers the following types of Loans and Advances:

1. Bank Overdraft: This facility is for current account holders. It allows holders to withdraw money anytime more than available in bank balance but up to the provided limit. An overdraft facility is granted against collateral security. The interest for overdraft is paid only on the borrowed amount for the period for which the loan is taken.

2. Cash Credits: a short term loan facility up to a specific limit fixed in advance. Banks allow the customer to take a loan against a mortgage of certain property (tangible assets and / guarantees). Cash credit is given to any type of account holders and also to those who do not have an account with a bank. Interest is charged on the

amount withdrawn in excess of the limit. Through cash credit, a larger amount of loan is sanctioned than that of overdraft for a longer period.

3. Loans: Banks lend money to the customer for short term or medium periods of say 1 to 5 years against tangible assets. Nowadays, banks do lend money for the long term. The borrower repays the money either in a lump-sum amount or in the form of instalments spread over a pre-decided time period. Bank charges interest on the actual amount of loan sanctioned, whether withdrawn or not. The interest rate is lower than overdrafts and cash credits facilities.

4. Discounting the Bill of Exchange: It is a type of short term loan, where the seller discounts the bill from the bank for some fees. The bank advances money by discounting or purchasing the bills of exchange. It pays the bill amount to the drawer(seller) on behalf of the drawee (buyer) by deducting usual discount charges. On maturity, the bank presents the bill to the drawee or acceptor to collect the bill amount.

5. Buyer Credit: It is the credit availed by an Importer from overseas lenders (i.e. Banks & Financial Institutions) for payment against his imports. The overseas bank usually lends the Importer based on a letter of credit, bank guarantee issued by the importer bank.

6. Suppliers Credit: Under such credit facility an exporter extends credit to a foreign importer to finance his purchase. Usually the importer pays a portion of the contact value in cash and issues a Promissory note as evidence of his obligation to pay the balance over a period of time. The exporter thus accepts a deferred payment from the importer and may be able to obtain cash payment by discounting or selling such promissory note created with his bank.

7. Letter Of Credit: When a buyer or importer wants to purchase goods from an unknown seller or exporter. He can take assistance from the bank in such buying or importing transactions. Bank issues a letter of credit addressed to the supplier or exporter after it, supplier or exporter will supply the goods to such unknown buyer

or importer. A signed Invoice with Letter Of Credit is presented to the bank of buyer/importer and the payment is made to the seller/exporter directly by the bank.

8. Bank Guarantee: It is a guarantee issued by a banker that, in case of an occurrence or non-occurrence of a particular event, the bank guarantees to fulfil the loss of money as stipulated in the contract. It may of various types like Financial Guarantees, Performance
Guarantees and Deferred Payment Guarantee.

3.2.2 Secondary Functions of Bank

Secondary functions of banking encompass a diverse array of services beyond the core functions of deposit-taking and lending. These functions include providing auxiliary services like safe deposit boxes for secure storage of valuables, currency exchange to facilitate international transactions, and financial advisory services to assist customers with investment decisions. Banks also serve as trustees and executors, managing assets on behalf of clients and administering trusts and estates. Additionally, they act as intermediaries in the sale and purchase of securities, aiding in the functioning of financial markets and providing liquidity to investors. Furthermore, banks play a vital role in promoting economic development by offering financing to small businesses and entrepreneurs, thereby fostering innovation and growth. Overall, these secondary functions complement the primary roles of banks, enhancing the convenience, security, and efficiency of financial transactions while contributing to the overall stability and development of the economy.

The secondary functions of banking are explained in detail below:

1. Safe Deposit Lockers: Banks offer safe deposit lockers to customers for securely storing valuable items such as important documents, jewellery, or other valuables. These lockers provide an additional layer of security beyond traditional home safes.

2. Financial Advice: Many banks provide financial advisory services to their customers. This can include guidance on investment options, retirement planning, and other aspects of personal finance. Financial experts within the bank may offer advice tailored to individual customer needs.

3. Foreign Exchange: Services: Banks facilitate currency exchange for customers involved in international transactions. This includes buying and selling foreign currencies, providing travellers cheques, and offering services related to international trade and remittances.

4. Trustee and Executor Services: Banks can act as trustees or executors in wills and trusts. This involves managing and distributing assets according to the terms of a will or trust document. This service ensures the orderly transfer of wealth to beneficiaries.

5. Agency Functions: Banks often act as agents for the purchase and sale of securities. Customers can authorize their banks to buy or sell stocks, bonds, and other financial instruments on their behalf. This streamlines the process for investors who may not want to handle these transactions directly. These secondary functions complement the primary role of banking, which involves accepting deposits and providing loans. They enhance the overall financial services that banks offer to meet various customer needs.

3.3 TYPES OF BANKS

1. Central Bank/Banker's Bank: The central bank of India is the Reserve Bank of India (RBI). The RBI is responsible for regulating and supervising the Indian banking system. It also manages the country's monetary policy and foreign exchange reserves.

2. Scheduled Banks: Scheduled banks are commercial banks that are regulated by the RBI. They are included in the Second Schedule of the Reserve Bank of India

Act, 1934. Scheduled banks can be classified into three categories: public sector banks, private sector banks, and foreign banks.

3. Commercial Banks: Commercial banks are the most common type of bank in India. They provide a wide range of financial services to individuals and businesses, including savings accounts, loans, and investment products.

4. Public Sector Banks: Public sector banks are owned and operated by the government of India. They account for a significant share of the Indian banking system. Example: State Bank of India , Punjab National Bank ,Bank of Baroda, Canara Bank , Bank of India .

5. Private Sector Banks: Private sector banks are owned and operated by private individuals or companies. They have played an increasingly important role in the Indian banking system in recent years. Example : Axis Bank , HDFC Bank , ICICI Bank , Yes Bank.

6. Foreign Banks: Foreign banks are branches of foreign banks that operate in India. They offer a range of financial services, including corporate banking, investment banking, and retail banking. Example: National Australia Bank, DBS Bank Ltd.

7. Regional Rural Banks: Regional rural banks (RRBs) were established in 1975 to provide banking services to rural areas. They are sponsored by commercial banks and the government of India. RRBs play an important role in promoting financial inclusion and rural development.

8. Non-Scheduled Banks: Non-scheduled banks are not subject to the regulation of the RBI. They are typically smaller banks that cater to a specific niche market.

9. Local Area Banks: Local area banks (LABs) were established in 2013 to provide banking services to underserved areas. They are sponsored by commercial banks and the government of India. LABs play an important role in promoting financial inclusion.

10. Payment Banks: Payment banks were set up in 2015 to offer basic banking services such as savings accounts, money transfers, and bill payments. They cannot offer loans or credit cards. Payment banks are designed to promote financial inclusion and cashless transactions.

11. Small Finance Banks: Small finance banks (SFBs) were set up in 2015. They provide banking services to underserved segments of the population, such as small businesses and farmers. SFBs can offer a range of financial services, including savings accounts, loans, and investment products.

12. Specialized Banks: Specialized banks are banks that focus on a specific sector of the economy, such as agriculture, industry, or trade. Some examples of specialized banks in India include: The National Bank for Agriculture and Rural Development (NABARD) and The Industrial Development Bank of India (IDBI).
One of the most important responsibilities that a bank or financial institution has is to protect the integrity of the institution by working hard to protect the financial assets that it holds. In order to do so, the bank or financial institution must be certain to address the issue of bank fraud.

3.4 WHAT IS BANK FRAUD?

Bank fraud is defined as the illegal act of an individual attempting to acquire money from a financial institution. It is the criminal act of deliberately obtaining financial assets from a bank by giving out false information to the bank or using pretense.

3.4.1 Types of Banking Frauds

Banking frauds can range from small scale operations to large scale operations which in cases include upto multi-million-dollar operations.It is important that each and every individual should be aware of the various banking frauds and to know how to respond in each cases.

The various types of banking frauds are listed below in detail.

ACCOUNTING FRAUD

It is a kind of fraud which occurs when the financial institution misinterprets its financial position by either making some changes or by omitting some information in such a way that on the outside it appears to be a perfect company with an excellent financial position. Businesses mainly do this for easily availing loans from banks.

The organization purposefully does this manipulation of their financial statement to make it appear to the outside parties that it is gaining more profits within the company where in reality it might not be right. When the banks review the financial statements, they provide loans, trusting that those statements were true. When the time comes to repay the loan the company faces difficulties in repayment since they do not have sufficient income as mentioned in the statements. In such cases the company becomes insolvent, the bank will face huge losses due to failure in repayment by the company. A classic example of accounting fraud is the Lehman Brothers scandal.

BILL DISCOUNTING FRAUD

Bill discounting fraud involves manipulating or falsifying bills of exchange or invoices to secure loan or credit from a financial institution. This fraudulent practice might include inflating the value of the bills or presenting fictitious bills to obtain funds or credit that wouldn't otherwise be granted. It's a form of financial deception that can lead to significant financial losses for the lending institution involved.

Bill discounting fraud can be explained with the help of a simple example- a dishonest company submits inflated invoices to a bank for discounting. These invoices claim payments for goods and services that were never delivered. The bank, unaware of the fraudulent activity, provides funds based on the face value of these invoices. The company then uses the funds obtained through this fraudulent means for its own purposes, without any intention of fulfilling the obligations stated in the

invoices. This results in the bank suffering losses when they realize the invoices were false and the goods or services were never provided as claimed.

FORGED OR FRAUDULENT DOCUMENTS

Forged or fraudulent documents are fabricated or altered papers, contracts, ID's or records that are intentionally created to mislead or manipulate others. Forging of documents can happen in ways such as adding unnecessary information, omitting various important information or by completely altering the documents. In banking, an example of a forged document might involve someone creating a counterfeit cheque with a fake signature or altering the details on a legitimate check to redirect funds to their accounts. Another example can be falsifying the financial statements of the company to create a picture perfect financial position of a company either for any personal gains or for availing loans easily from the banks.

FORGERY AND ALTERED CHEQUES

The above mentioned fraud involves altering the various elements of a cheque this may include creating a fake signature, altering the details on a legitimate cheque like changing the name of the recipient or by changing either the name or the amount of the cheque. The fraudster can make it look like an authorized transaction. The banks can face huge losses due to this kind of forgery.

The person who commits the crime of cheque forgery is seriously punished under section 138 of the Negotiable Instrument Act,1881. An example of a forged check could involve someone stealing a check book or obtaining a copy of a genuine check. They might then alter the payee's name, the amount, or the date on the check to divert funds to themselves or someone else.

FRAUDULENT LOAN APPLICATIONS

A fraudulent loan application occurs when an individual or entity intentionally provides false, misleading, or fabricated information on a loan application to secure

funds from a financial institution. This information could include inflating income, providing fake employment details, misrepresenting assessor and hiding existing debts.

The goal is to deceive the lender into approving a loan that the applicant may not qualify for based on their true financial situation. This type of fraud can lead to financial losses for the lending institution and potential legal consequences for the applicant upon discovery. In order to minimize fraudulent loan application the banks can implement stronger security measures to prevent future occurrences. This can include improved identity verification processes, enhanced document scrutiny, or employing advanced technology for fraud detection.

EMPTY ATM ENVELOPE DEPOSITS

Empty ATM envelope deposits involve a fraudulent scheme where an individual deposits an empty envelope into an ATM instead of one containing cash or a check. The person may do this deliberately, hoping to deceive the bank into crediting their account with the amount they claim to have deposited. This type of fraud relies on the delay between the time of deposit and the bank's verification of the envelope's contents. When the bank processes the deposit and finds it empty, it results in a discrepancy between the claimed deposit amount and the actual deposited funds, leading to potential financial losses for the bank.

IDENTITY THEFT OR IMPERSONATION

Identity theft or impersonation in banking occurs when someone unlawfully obtains and uses another person's personal information, such as their name, social security number, bank account details, or other identifying data, to access financial accounts, apply for loans, or conduct transactions without authorization.

This fraudulent practice involves assuming the identity of another individual to exploit their financial resources, potentially causing financial harm to the victim whose identity has been stolen. This can lead to unauthorized access to funds,

fraudulent purchases, or even taking out loans or credit lines under the victim's name without their knowledge or consent. This form of identity theft can severely impact the victim's credit history and financial stability while benefiting the fraudster who exploits the stolen identity for their gain.

MONEY LAUNDERING

Money laundering is a process used to disguise the origins of illegally obtained money, making it appear as though it came from legitimate sources. It involves a series of transactions or activities that aim to conceal the true source of funds acquired through illegal activities such as drug trafficking, corruption, fraud or other criminal activities. Money laundering is illegal and is aimed at concealing the true source of illegal funds to evade detection by law enforcement or financial regulators. Governments and financial institutions implement measures and regulations to prevent and detect money laundering activities. Money launderers often attempt to disguise the movement of funds by using shell companies, overseas bank accounts, or anonymous online wallets.

The process typically involves three main stages, they are

1. Placement- Illegally obtained money is introduced into the financial system. This can involve cash into bank accounts, purchasing assets etc.

2. Layering- The funds are the moved or transferred through a series of complex transactions or layers to make the tracing the original source difficult.

3. Integration- At this stage, the money is reintroduced into the economy in a way that makes it appear legitimate.

PHISHING OR INTERNET FRAUD

Phishing is a type of cybercrime where fraudsters attempt to trick individuals into revealing sensitive information such as usernames, passwords, credit card details, or other personal information by posing as a legitimate entity. This is often done

through deceptive emails, messages, or websites that appear to be from trusted sources like banks, government agencies, or well known companies.

The fraudulent communication usually contains urgent or enticing language to prompt the recipient to click on a link, provide personal information, or download an attachment. Once the victim interacts with these fraudulent elements, the attackers gain access to their sensitive data, which can then be used for identity theft, financial fraud, or other malicious activities. Phishing attacks can also occur through phone calls or text messages, known respectively as vishing (voice phishing) and smashing (SMS phishing).

PRIME BANK FRAUD

Prime bank fraud is a type of financial scam that promises high returns with little or no risk by supposedly investing in exclusive or secret financial instruments offered by "prime banks" or elite financial entities. However, there are no legitimate prime bank instruments available to the general public. These schemes typically target individuals or investors with the promise of extraordinary profits through secret or unique financial products.

Perpetrators of prime bank fraud often claim to have access to programs or instruments that are purportedly only available to a select few or are reserves for high net worth individuals, promising guaranteed returns or high yields. In reality, these schemes are fraudulent and do not involve any legitimate financial instruments. Investors are lured into depositing their money into these scams, which ultimately leads to significant financial losses for the victims when the promised returns fail to materialize. Authorities strongly warn against engaging in any investment opportunity that claims involvement with prime banks or offers unusually high returns with low or no risk.

ROGUE TRADERS

Rogue traders are individuals who work within financial institutions and engage in unauthorized or excessively risky trading activities, often resulting in substantial financial losses for their employers. These traders might act independently, bypassing established risk management protocols or manipulating financial markets for personal gain.

These rogue traders can take positions that go against their employer's policies to make unauthorized trades, or deliberately misrepresent their activities to cover up losses. Their actions often result in significant financial damages to the financial institutions they work for, sometimes leading to severe repercussions such as financial penalties, loss of investor confidence and in extreme cases the collapse of the institution. Famous examples of rogue traders include Nick Leeson,whose unauthorized trades led to the collapse of Barings Bank in the 1990.

WIRE TRANSFER FUND

A wire transfer is a method of electronically moving money from one person or entity to another. It involves the direct transfer of funds from one bank account to another bank account to another, often across different financial institutions.

The below mentioned pattern is a way in which a wire transfer occurs:

1.Initiation- The process begins when the sender provides instructions to their bank or financial institution to transfer a specific amount of money to the recipient's account. The sender needs details like the recipient's name, account number, the receiving bank's name, and possibly additional information and the SWIFT code (for international transfers)

2.Authorisation- The sender's bank verifies the authenticity of the request and the availability funds. Once confirmed they debit the sender's account by the transferred amount, plus any applicable fees.

3.Transfer- The sender's bank then electronically send the specified amount to the recipient's bank through a secure network, often involving intermediary banks or financial entities to facilitate transfer

4.Recipient by recipient's bank- The recipient's bank receives the funds and credits the recipients account accordingly. The time taken for the recipient to access the funds can vary based on the policies of the receiving bank and nature of the transfer.

5.Confirmation- Both the sender and recipient receive confirmation from their respective banks, confirming the completion of the wire transfer.

Wire transfer fraud involves the misuse of wire transfer systems to deceive individuals or entities into sending money under false pretences.this type of fraud involves trickery, social engineering, or hacking to persuade victims to transfer funds to the fraudsters account.The several common scenarios for wire transfer frauds include-Business Email Compromise, Phishing, False invoices or services, Investment scams, Romance scams.

Wire transfer fraud exploits trust, manipulation or vulnerabilities in communication channels to deceive victims into transferring money to accounts controlled by the fraudsters. Once the funds are transferred ,they can be challenging to recover and victims often suffer financial losses.

PAYMENT CARD FRAUD

Payment card fraud involves unauthorized or fraudulent use of credit cards, debit cards, or any other payment cards to make purchases or access funds without the cardholder's consent. There are various types of payment card fraud:

1. Counterfeit Cards: Fraudsters create fake cards by copying the information contained on a legitimate card's magnetic stripe or chip. These counterfeit cards are then used for unauthorized transactions.

2. Card-Not-Present (CNP) Fraud: This occurs when card information (card number, expiration date, CVV code) is stolen and used for online or phone transactions where the physical card is not required.

3. Lost or Stolen Card Fraud: Criminals use lost or stolen cards to make unauthorized purchases or cash withdrawals before the cardholder can report it missing.

4. Skimming: Fraudsters use skimming devices to capture card information when the card is swiped at compromised ATMs, gas pumps, or other card readers. They then use this information to create counterfeit cards or make online purchases.

5. Identity Theft: This involves stealing a person's personal information, including card details, to open new accounts or apply for new cards in the victim's name.

6. Account Takeover: Fraudsters gain access to a cardholder's account by obtaining login credentials or personal information. They then make unauthorized transactions, change account details, or transfer funds.

Payment card fraud can lead to financial losses for cardholders, financial institutions, and merchants. Cardholders are often protected by their card issuer's fraud prevention measures and are typically not held liable for unauthorized transactions if reported promptly. To combat payment card fraud, measures like using secure websites for online transactions, monitoring accounts regularly for suspicious activity, and promptly reporting lost or stolen cards are essential. Additionally, financial institutions employ various security measures like EMV chip technology, tokenization, and fraud detection systems to prevent and detect fraudulent transactions.

3.5 AFTER EFFECTS OF BANKING SCAMS:

1. Skimming

Skimming is a method used by identity thieves to capture payment and personal information from a credit card holder. Several approaches can be used by fraudsters to procure card information, with the most advanced approach involving a small device called a skimmer that reads the information stored in a card's magnetic strip or microchip.

While scammers can't withdraw cash without the card pin, they can use the card to pay via contactless if this feature is enabled on the card. It is also possible to scan contactless cards through bags using an RFID reader, which is more likely to happen in busy areas such as cities and public transport. Additionally, some retailers and merchants have been known to abuse customer bank information by stealing copies of the credentials while using the card during a purchase.

2. Mobile banking fraud

Similarly to online banking fraud, this type of banking fraud attempts to convince the target to voluntarily give away information or transfer their money into another account. The scammer will usually try to convince the target that they need to move money to prevent themselves from losing the money, protecting their assets. They may even make up fake offences and demand that the target pay fines for 'committing' them.

3. In-person (stealing card and PIN)

In-person fraud – often committed by looking over an individual's shoulder using an ATM or distraction tactics – can be a dangerous type of financial fraud because it can sometimes mean that the scammer will have access to their target's bank card and PIN.

Sometimes the scammer may engage the target in conversation to learn more identifying information about them. Like skimming, the card can be used in various

ways, but with the addition of the PIN and any other information, the options are opened up to include shopping in face-to-face retail.

4. Counterfeit card fraud

This is a more common type of financial fraud in countries that have not yet fully adopted chip and PIN systems for bank cards. Like in skimming, the scammer will take the information from the magnetic strip, but with counterfeit card fraud, they will then transplant that onto another magnetic card to continue using it.

5. CEO fraud

CEO fraud, also known as Business Email Compromise (BEC) or whale phishing, is a type of financial fraud that occurs when a fraudster impersonates a senior manager or CEO to pressure an employee to make a payment.

The way CEO fraud works is usually via an email to the accounts team of a company that appears to be from a senior member of staff. The email requests an urgent payment to a partner or supplier.

A recent example involves The Scoular Company. They were victims of CEO fraud and lost more than $17 million after fraudsters, claiming to be the company's CEO, sent emails to an employee instructing them to transfer funds to what appeared to be the company's accounting firm. However, this was a fake request and the funds were sent to a scam artist.

6. Invoice fraud

This bank fraud example targets businesses by impersonating a supplier, usually via email, asking to update the bank details invoices are paid into. This might look entirely innocent if the fraudster has hacked the supplier's info, as the request will appear to be authentic.

A notable example of invoice fraud dates back to 2013-2015 when Facebook and Google were victims of fraud that cost them more than $100 million. In this

particular case of online banking fraud, a Lithuanian hacker impersonated an Asian manufacturer and sent fake invoices to the tech giants.

7. Online banking fraud

Online banking fraud can come in many guises, including phishing, malware attacks, catfish scams and clone websites. With so much banking done online, it's not surprising that this is a common type of bank fraud.

Fraudsters are becoming highly skilled at creating convincing emails and websites, making it difficult for victims to protect themselves. An online bank fraud example may involve the scammer posing as bank staff and telling the target that their account has been compromised and they need to transfer money to another account. Or, a scammer may ask their target to 'confirm' their PIN, account password or verifying details over email, again posing as legitimate bank staff.

8. APP scams

Authorized Push Payment (APP) scams include any scam where the target must willingly decide to move the money out of their account. It is a common tactic used in some types of financial fraud, but it can also be accomplished over the phone or face-to-face. Usually, the scammer will inform the target of a change in their account (often a data breach that puts their money at risk) and ask them to either confirm their password, PIN or other sensitive information to prove who they are. APP scams are an example of bank fraud that can be more difficult to recover from. Banks often won't automatically refund any money lost if they believe that the target gave it out willingly or was negligent with their information, even if they were under pressure to do so.

9. Card not received

This occurs when a bank sends out a new or replacement card to a customer, but it is intercepted along the way. It most commonly occurs in shared residences (such as a block of flats or a house share) if the post is not sufficiently secure upon arrival.

If the card is new, the PIN code should be sent in a separate letter, but this won't stop a scammer from using the card for contactless or online purchases. Card not received fraud can be harder to detect because the targeted individual might not notice the card is missing at first.

10. Card identity theft

This type of bank fraud can involve taking over a legitimate bank account and impersonating the owner or using stolen or faked documents to open an account under someone else's name.

11. Non-delivery of goods

This scam involves the sale of a product that then never arrives – it is not the fault of a postal or courier service, but the recipient of the money had no intention of sending the product. In an age of online shopping and small businesses, the non-delivery of goods becomes a very real issue.

12. Cheque fraud

A typical cheque fraud scam is where someone sends you a cheque, asks you to deposit the money in your account and then requests you forward most of the funds by wire transfer, e-Transfer, or money order somewhere else. Examples of where this can occur include a job posting for an Internet collection agent, a lottery or inheritance notification, or overpayment for something you're selling where you're asked to return the extra funds.

13. Loan fraud

Similarly to card identity theft, this type of financial fraud involves taking out a loan under someone else's name using stolen or faked documents. This can be to utilise another person's better credit or to avoid paying the loan back.

14. Insurance fraud

Insurance fraud occurs when an insurance company, agent, adjuster or consumer commits a deliberate deception in order to obtain an illegitimate gain. It can occur during the process of buying, using, selling, or underwriting insurance. Insurance

fraud may fall into different categories from individuals committing fraud against consumers to individuals committing fraud against insurance companies.

15. Juice Jacking

Juice jacking is a security exploit in which an infected USB charging station is used to compromise devices that connect to it. The exploit takes advantage of the fact that a mobile device's power supply passes over the same USB cable the connected device uses to sync data.

CHAPTER IV

DATA ANALYSIS AND INTERPRETATION

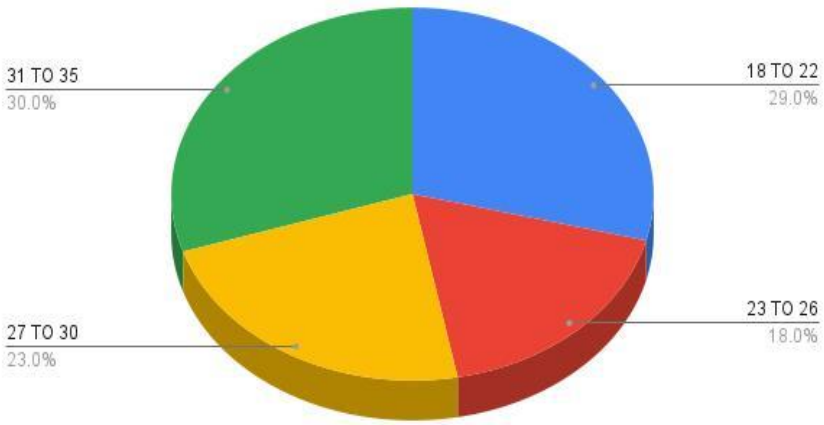
4.1 AGE OF THE RESPONDENTS

TABLE 4.1 SHOWING AGE OF THE RESPONDENTS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGES
18 TO 22	29	29%
23 TO 26	18	18%
27 TO 30	23	23%
31 TO 35	30	30%
TOTAL	**100**	**100%**

(Source Primary Data)

FIGURE 4.1 SHOWING AGE OF THE RESPONDENTS



INTERPRETATION

Out of the 100 respondents ,30% of respondents come under the age category of 31-35. 29% of the respondents come under 18-22. 23% of the respondents come under the age group of 27-30. And the remaining 18% comes under the age 31-35.

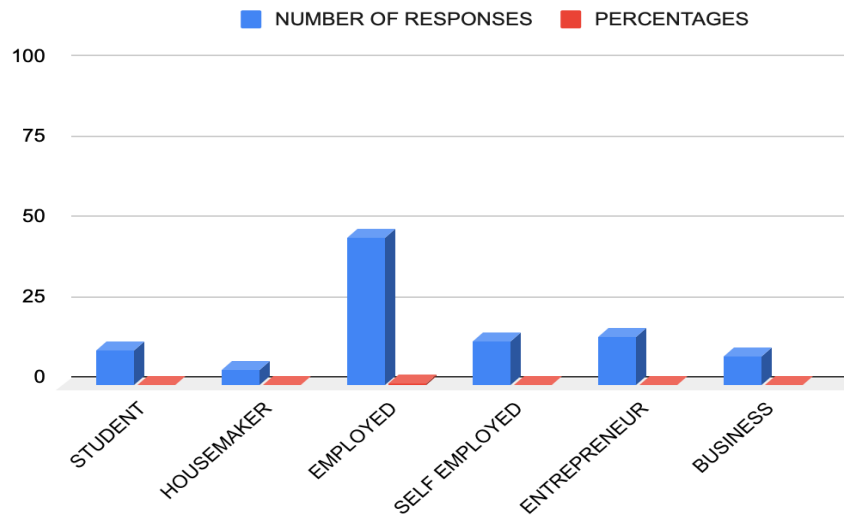
4.2 OCCUPATION OF THE RESPONDENTS

TABLE 4.2 SHOWING THE OCCUPATION OF THE RESPONDENTS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGES
STUDENT	11	11%
HOUSEMAKER	5	5%
EMPLOYED	46	46%
SELF EMPLOYED	14	14%
ENTREPRENEUR	15	15%
BUSINESS	9	9%
TOTAL	**100**	**100%**

(Source: Primary Data)

FIGURE 4.2 SHOWING THE OCCUPATION OF THE RESPONDENTS



INTERPRETATION

Out of the 100 respondents received 46% of respondents are employees. 15% of the respondents are entrepreneurs. 14% of the respondents are self-employed, 11% of them are students whereas 9% of the respondents are undertaking businesses. And the remaining 5% are housemakers.

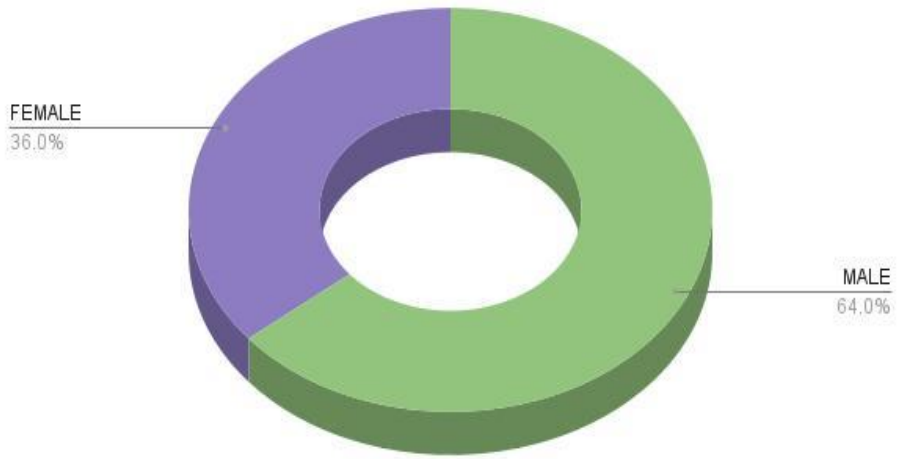
4.3 GENDER OF THE RESPONDENTS

TABLE 4.3 SHOWING GENDER OF THE RESPONDENTS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
MALE	64	64%
FEMALE	36	36%
TOTAL	**100**	**100%**

(Source: Primary Data)

FIGURE 4.3 SHOWING GENDER OF THE RESPONDENTS



INTERPRETATION

Out of the 100 respondents received 64% are males and 36% are Females. So male respondents are more than female respondents.

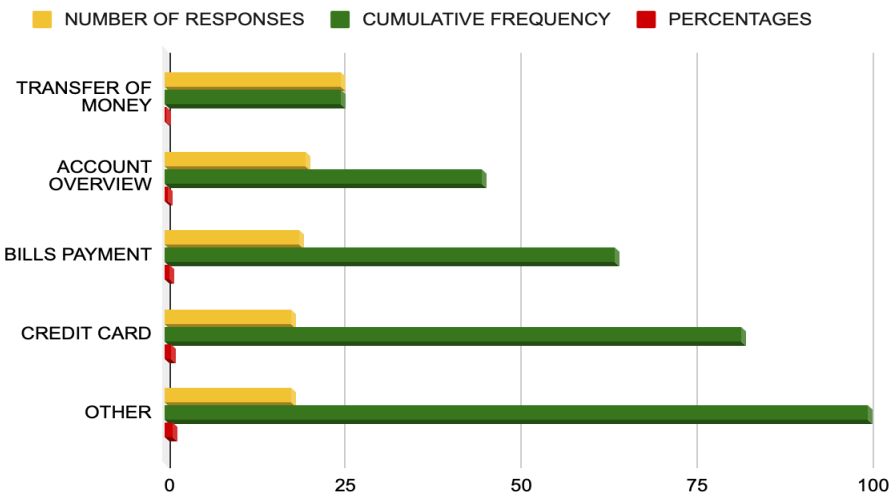
4.4 USAGE OF VARIOUS TYPES OF BANKING SERVICES

TABLE 4.4 SHOWING THE USAGE OF VARIOUS TYPES OF BANKING SERVICES

PARTICULARS	NUMBER OF RESPONSES	CUMULATIVE FREQUENCY	PERCEN TAGES
TRANSFER OF MONEY	25	25	25%
ACCOUNT OVERVIEW	20	45	45%
BILLS PAYMENT	19	64	64%
CREDIT CARD	18	82	82%
OTHER	18	100	100%
TOTAL	**100**		

(Source: Primary Data)

FIGURE 4.4 SHOWING THE VARIOUS TYPES OF BANKING SERVICE



INTERPRETATION

Out of the 100 respondents received, transferring of money was used by 25%. 20% avail the service of account overview. 19% of the respondents use it for bills payment. Credit card services are availed by 18% of the respondents and the rest 18% use other banking services

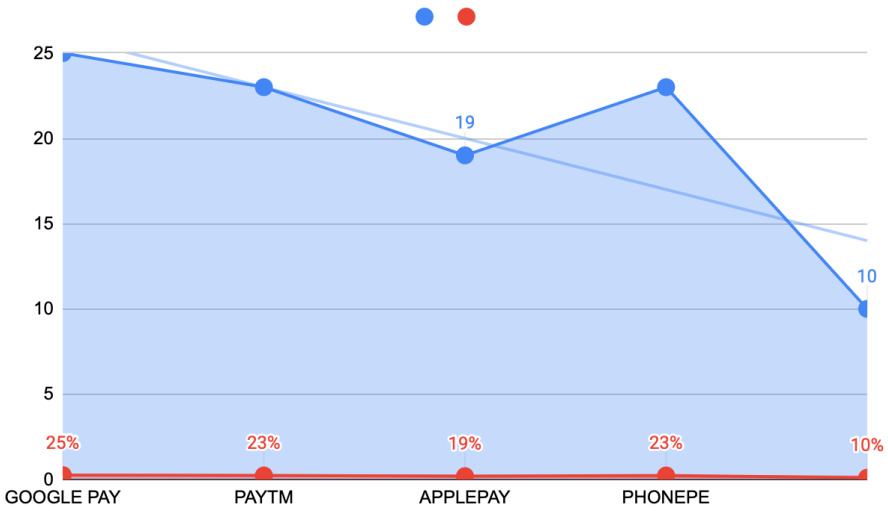
4.5 USAGE OF VARIOUS TYPES OF E-PAYMENTS

TABLE 4.5 SHOWING THE USAGE OF VARIOUS TYPES OF E-PAYMENTS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
GOOGLE PAY	25	25%
PAYTM	23	23%
APPLEPAY	19	19%
PHONEPE	23	23%
OTHER	10	10%
TOTAL	**100**	**100%**

(Source Primary Data)

FIGURE 4.5 SHOWING THE USAGE OF VARIOUS TYPES OF E-PAYMENTS



INTERPRETATION

Out of the 100 respondents, 25% use Google Pay. 23% use Paytm, whereas 23% use Phone Pe 19% of the respondents use ApplePay. And the rest 10% use other e-payment methods. Hence the most used e payment app is Google Pay,

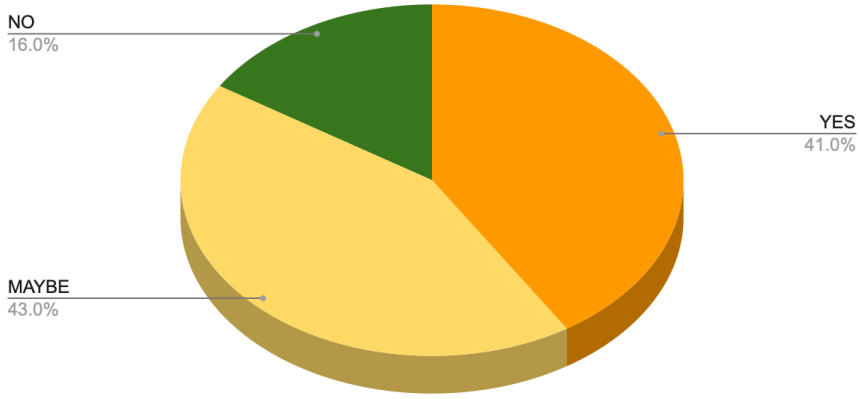
4.6 AWARENESS LEVEL OF BANKING FRAUDS AMONG THE RESPONDENTS

TABLE 4.6 SHOWING THE AWARENESS LEVEL OF BANKING FRAUDS AMONG THE RESPONDENTS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
YES	41	41%
MAYBE	43	43%
NO	16	16%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.6 SHOWING THE AWARENESS LEVEL OF BANKING FRAUDS AMONG THE RESPONDENTS



INTERPRETATION

Out of the 100 respondents, 41 of them are aware of the banking frauds happening around and 43 of them are partly aware about them, whereas 16 of them weren't aware of the same.

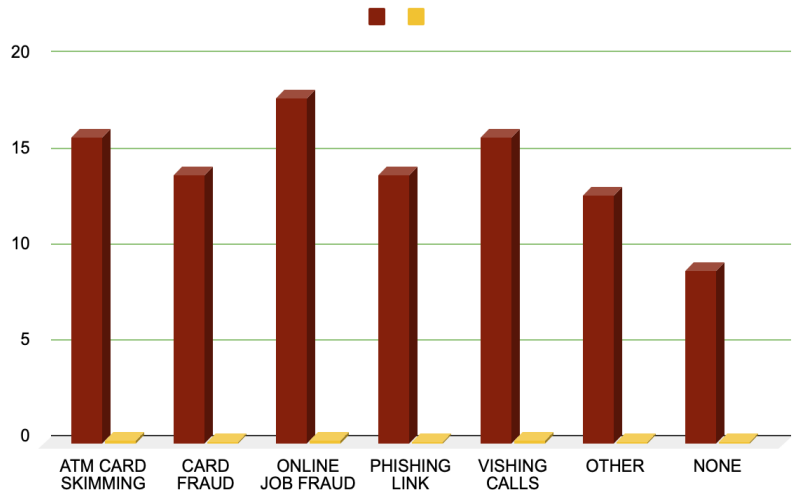
4.7 AWARENESS OF THE VARIOUS TYPES OF BANKING SCAMS

TABLE 4.7 AWARENESS OF THE VARIOUS TYPES OF BANKING SCAMS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
ATM CARD SKIMMING	16	16%
CARD FRAUD	14	14%
ONLINE JOB FRAUD	18	18%
PHISHING LINK	14	14%
VISHING CALLS	16	16%
OTHER	13	13%
NONE	9	9%
TOTAL	**100**	**100%**

(Source Primary Data)

FIGURE 4.7 SHOWING THE AWARENESS OF THE VARIOUS TYPES OF BANKING SCAMS



INTERPRETATION

Out of the 100 respondents, 18% of them are aware of online job frauds,16% of atm card skimming, 16% of them about vishing calls, card frauds by 14%, phishing links by 14% and 13%of them are aware of other banking scams other than listed whereas 9% of them aren't aware any of the banking scams

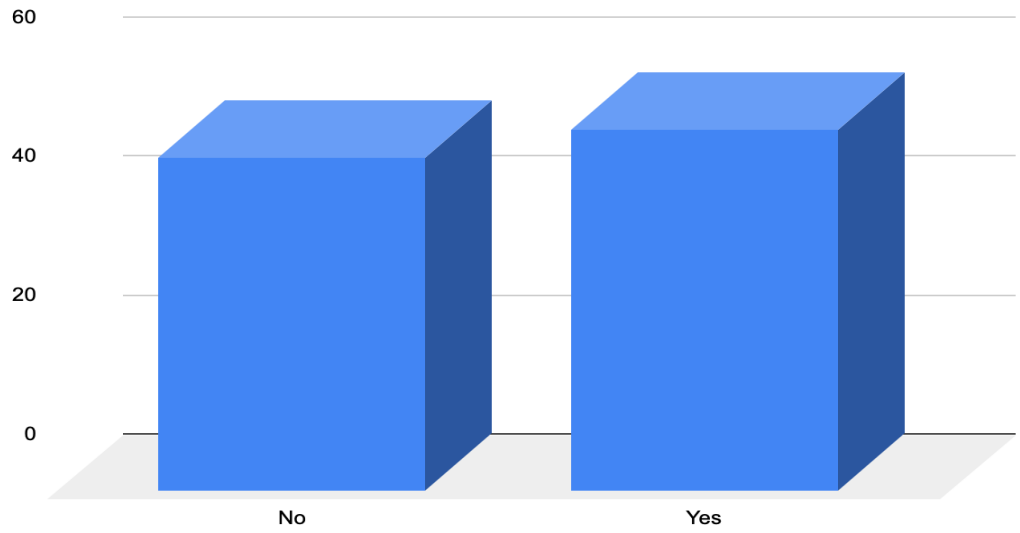
4.8 RESPONDENTS WHO RECEIVED UNSOLICITED EMAILS REGARDING THEIR BANKING INFORMATION

TABLE 4.8 RESPONDENTS WHO RECEIVED UNSOLICITED EMAILS OR TEXT MESSAGES REGARDING THEIR BANK INFORMATION

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
YES	52	52%
NO	48	48%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.11 RESPONDENTS WHO RECEIVED UNSOLICITED EMAILS OR TEXT MESSAGES REGARDING THEIR BANK INFORMATION



INTERPRETATION

Out of all 100 responses,52% of the people have received unsolicited messages asking for their banking information while 48% of the people have not received unsolicited messages asking for their banking information.

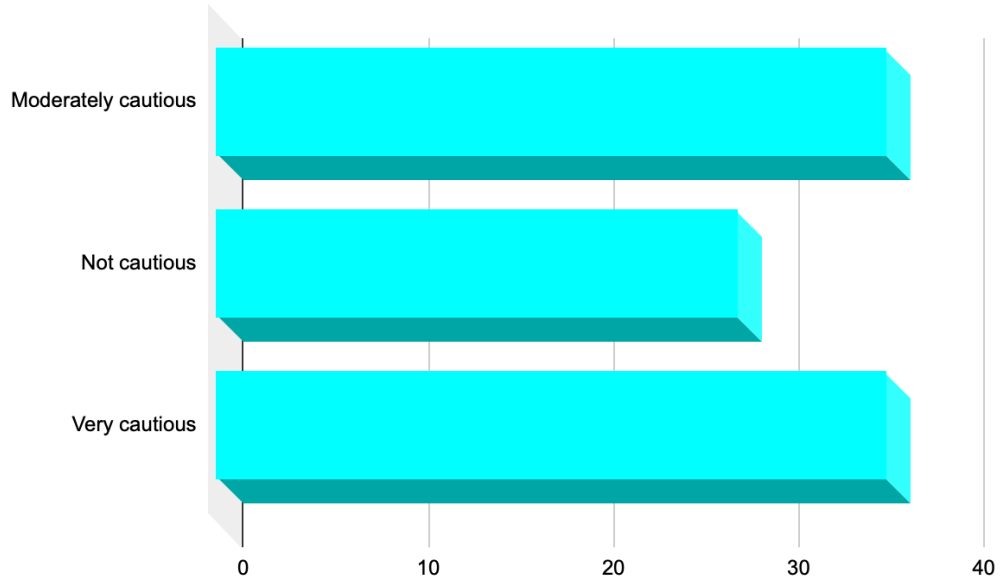
4.9 LEVEL OF CAUTIOUSNESS OF RESPONDENTS WHILE SHARING BANKING INFORMATION

TABLE 4.9 SHOWING PEOPLE WHO ARE CAUTIOUS ABOUT SHARING THEIR BANKING INFORMATION OVER THE PHONE.

PARTICULARS	NO. OF RESPONSES	PERCENTAGE
VERY CAUTIOUS	36	36%
MODERATELY CAUTIOUS	36	36%
NOT CAUTIOUS	28	28%
TOTAL	**100**	**100**

(Sources Primary Data)

FIGURE 4.9 SHOWING PEOPLE WHO ARE CAUTIOUS ABOUT SHARING THEIR BANKING INFORMATION OVER THE PHONE



INTERPRETATION

Out of all 100 responses, 36% are very cautious, 36% are moderately cautious whereas 28% are not cautious about sharing their banking information over the phone.

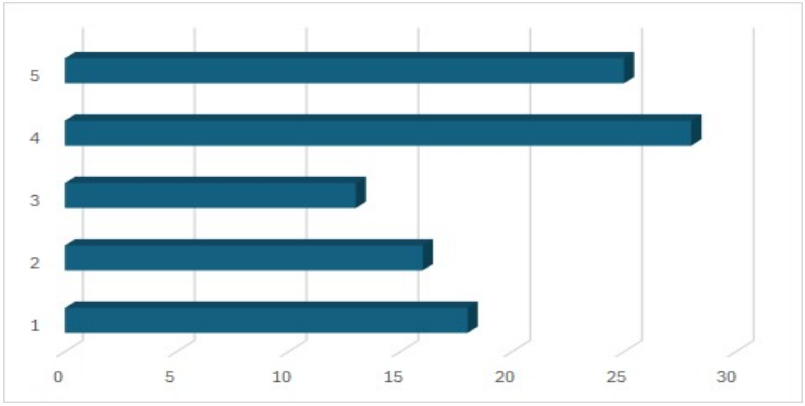
4.10 PEOPLE'S ABILITY TO IDENTIFY POTENTIAL BANKING SCAMS

TABLE 4.10 SHOWING PEOPLE'S ABILITY TO IDENTIFY POTENTIAL BANKING SCAMS

PARTICULARS	NO OF RESPONSES	PERCENTAGE
VERY CONFIDENT	18	18%
MILDLY CONFIDENT	16	16%
NEUTRAL	13	13%
NOT CONFIDENT	28	28%
UNCONFIDENT	25	25%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.10 SHOWING PERCENTAGE OF PEOPLE'S ABILITY TO IDENTIFY POTENTIAL BANKING SCAMS



INTERPRETATION

Out of the 100 responses received, 18% are very confident, 16% are mildly confident, 13% are neutral, 28% not confident and 25% of the respondents are unconfident in identifying potential banking and scam attempt.

4.11 MEASURES ADOPTED BY THE BANK TO EDUCATE AND PROTECT INDIVIDUALS FROM BANKING SCAMS

TABLE 4.11 MEASURES ADOPTED BY THE BANK TO EDUCATE AND PROTECT INDIVIDUALS FROM BANKING SCAMS

PARTICULARS	RECOMMENDING TO USE VERIFIED APPS ONLY		BE VIGILANT IN SHARING YOUR TRANSACTION DETAILS		CONDUCT WORKSHOPS ON HOW TO PROTECT ONE FROM BANKING SCAMS		ASKING NOT TO CLICK ON ANY SUSPICIOUS LINKS OR SMS OR EMAILS		ONLY BROWSE ON AUTHORIZED WEBSITES	
	Res	%	Res	%	Res	%	Res	%	Res	%
VERY SATISFIED	15	13%	19	23	23	23%	18	18%	22	22%
SATISFIED	18	18%	15	20	20	20%	23	23%	24	24%
NEUTRAL	23	23%	15	20	20	20%	18	18%	17	17%
DISSATISFIED	26	26%	28	19	19	19%	17	17%	20	20%
VERY DISSATISFIED	18	18%	23	18	18	18%	24	24%	17	17%
TOTAL	**100**	**100%**	**100**	**100**	**100**	**100%**	**100**	**100%**	**100**	**100%**

(Sources Primary Data)

FIGURE 4.11 VARIOUS MEASURES ADOPTED BY THE BANK TO EDUCATE AND PROTECT INDIVIDUALS FROM BANKING SC

INTERPRETATION

Out of all 100 responses received, the respondents have recorded their level of satisfaction with each of the measures adopted by the bank to educate the individuals from banking scams in the following manner.

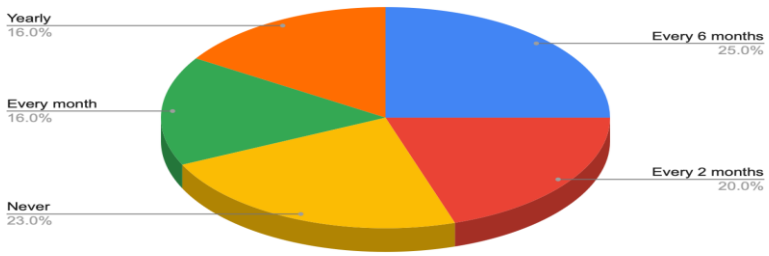
4.12 OPINION ON REVIEW OF BANK STATEMENTS FOR SUSPICIOUS ACTIVITY

TABLE 4.12 OPINION REVIEW OF BANK STATEMENTS FOR SUSPICIOUS ACTIVITY

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
EVERY MONTH	16	16%
EVERY 2 MONTHS	20	20%
EVERY 6 MONTHS	25	25%
YEARLY	16	16%
NEVER	23	23%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.12 OPINION ON REVIEW OF BANK STATEMENTS FOR SUSPICIOUS ACTIVITY



INTERPRETATION

Out of the 100 responses received, 16% of the people review every month, 20% review every 2 months, 25% every 6 months, 16% review yearly and the rest 23% never review their bank statements for any suspicious activities.

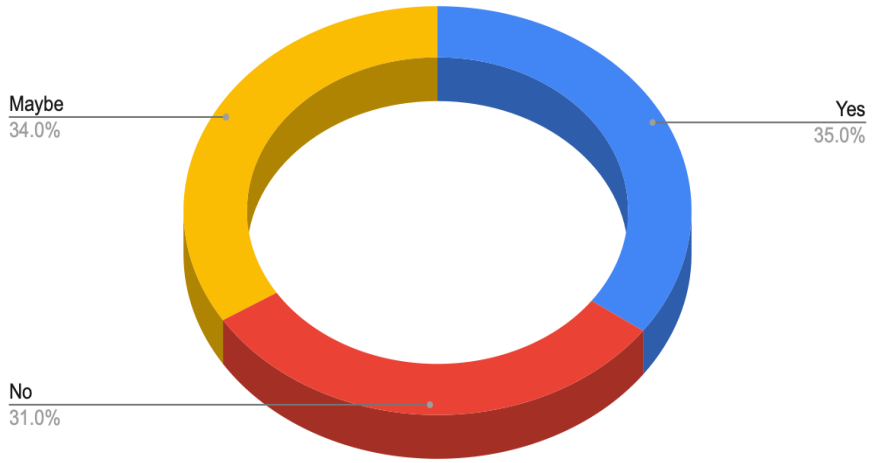
4.13 OPINION OF PEOPLE USING 2 FACTOR AUTHENTICATION

TABLE 4.13 OPINION ON USING 2 FACTOR AUTHENTICATION

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGES
YES	35	35%
NO	31	31%
MAYBE	34	34%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.13OPINION ON PEOPLE USING 2 FACTOR AUTHENTICATION



INTERPRETATION

Out of the 100 responses received, 35% use the 2 factor authentication, 31% don't use it, whereas 34% of the people are unsure about whether they use it or not.

4.14 OPINION ON PEOPLE ATTENDING WORKSHOPS ON FINANCIAL LITERACY AND BANKING SECURITY

TABLE 4.14 OPINION ON PEOPLE ATTENDING WORKSHOPS ON FINANCIAL LITERACY AND BANKING SECURITY

PARTICULARS	**NUMBER OF RESPONSES**	**PERCENTAGES**
YES	45	45%
NO	55	55%
TOTAL	**100**	**100**

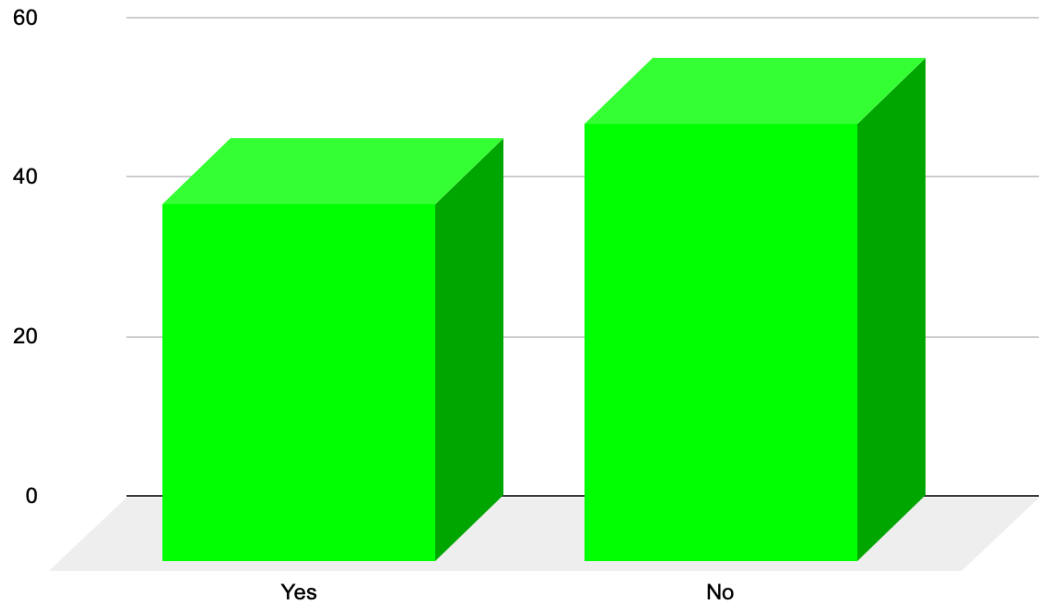
(Sources Primary Data)

CROSS TABULATION ANALYSIS ON THE GENDER OF THE RESPONDENTS

GENDER	**YES**	**NO**
MALE	21	33
FEMALE	19	27
TOTAL	**40**	**60**

(Sources Primary Data)

FIGURE 4.14 OPINION ON PEOPLE ATTENDING WORKSHOPS ON FINANCIAL LITERACY AND BANKING SECURITY



INTERPRETATION

Out of the 100 responses received 45% of the people have attended and 55% of the people have not attended workshops on financial literacy and banking security. In that 21 male and 19 female have attended and 33 male and 27 female have not attended.

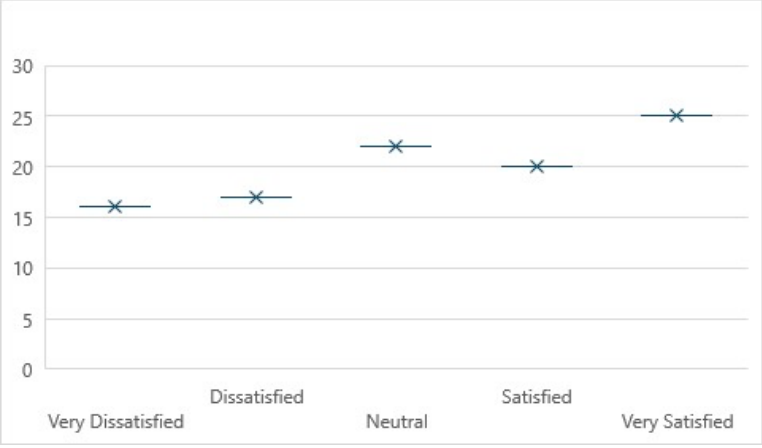
4.15 OPINION ON THE REDRESSAL MECHANISMS OF THE BANK

TABLE 4.15 OPINION ON THE REDRESSAL MECHANISMS OF THE BANK

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
VERY SATISFIED	25	25%
SATISFIED	20	20%
NEUTRAL	22	22%
DISSATISFIED	17	17%
VERY DISSATISFIED	16	16%
TOTAL	**20**	**100%**

(Sources Primary Data)

FIGURE 4.15 OPINION ON THE REDRESSAL MECHANISMS OF THE BANK



INTERPRETATION

Out of the 100 responses received, on a scale of 1 to 5(1 being very dissatisfied and 5 being very satisfied) are very satisfied, 25% are satisfied, 20% are satisfied, 22% are neutral, 17% are dissatisfied and 16% are very dissatisfied on the redressal mechanisms provided by the bank to address banking scams.

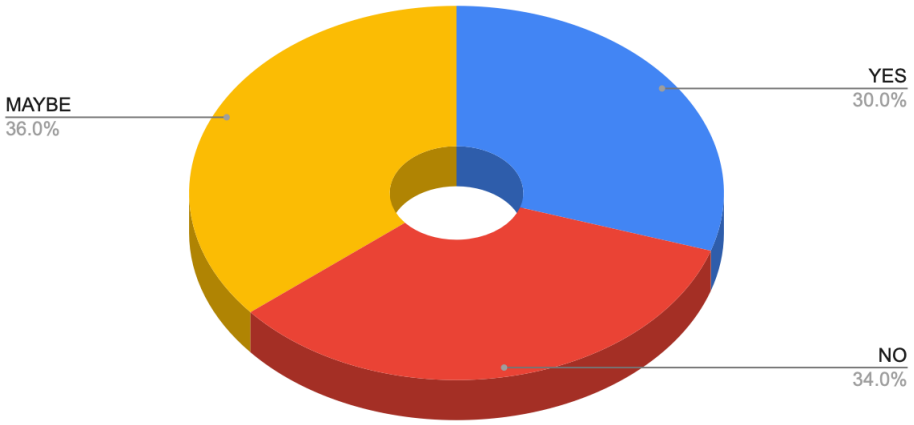
4.16 LEVEL OF KNOWLEDGE ABOUT THE TERM JUICE JACKING

TABLE 4.16 LEVEL OF KNOWLEDGE ABOUT THE TERM JUICE JACKING

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
YES	30	30%
NO	34	34%
MAYBE	36	36%
TOTAL	100	100%

(Sources Primary Data)

FIGURE 4.16 LEVEL OF KNOWLEDGE ABOUT THE TERM JUICE JACKING



INTERPRETATION

Out of 100 responses, 30% are aware about the term juice jacking calls, 34% are not aware about it, while 36% maybe aware of the term juice jacking.

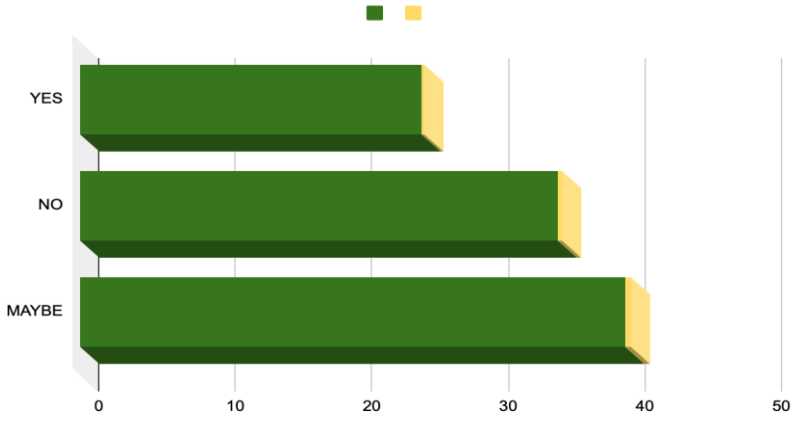
4.17 RESPONDENTS WHO HAVE USED PUBLIC CHARGING STATIONS TO CHARGE THEIR MOBILE DEVICES WHILE BEING OUT IN PUBLIC PLACES

TABLE 4.17 RESPONDENTS WHO HAVE USED PUBLIC CHARGING STATIONS TO CHARGE THEIR MOBILE DEVICES WHILE BEING OUT IN PUBLIC PLACES

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
YES	25	25%
NO	35	35%
MAYBE	40	40%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.17 RESPONDENTS WHO HAVE USED PUBLIC CHARGING STATIONS TO CHARGE THEIR MOBILE DEVICES WHILE BEING OUT IN PUBLIC PLACES



INTERPRETATION

Out of all 100 responses, 25% of the people have used public charging stations, while 35% of the people have not public charging stations, and 40% might have used public charging stations.

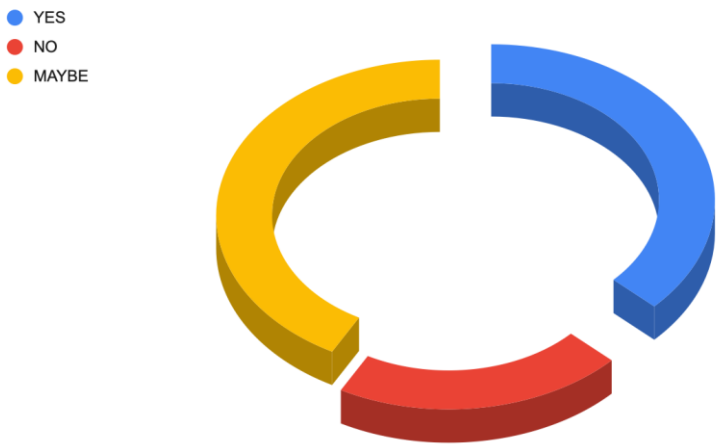
4.18 AWARENESS AMONG RESPONDENTS OF THE POTENTIAL RISKS OF LEAKAGE OF INFORMATION ASSOCIATED WITH USING PUBLIC CHARGING STATIONS

TABLE 4.18 AWARENESS AMONG PEOPLE ABOUT THE POTENTIAL RISKS ASSOCIATED WITH USING PUBLIC CHARGING STATIONS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
YES	37	37%
NO	21	21%
MAYBE	42	42%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.18 AWARENESS AMONG PEOPLE ABOUT THE POTENTIAL RISKS ASSOCIATED WITH USING PUBLIC CHARGING STATIONS



INTERPRETATION

Out of all 100 responses, 37% are aware of the potential risks associated with using public charging stations, 21% are not aware whereas 42% may have been aware of the risks.

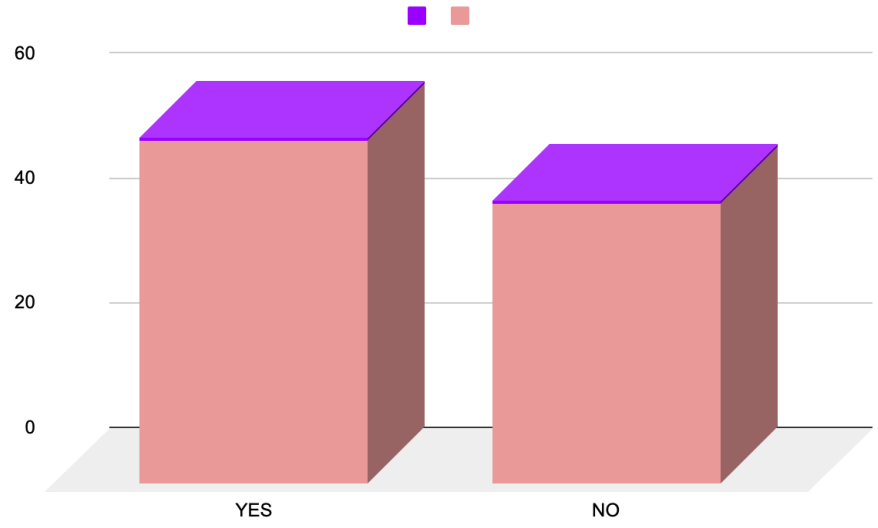
4.19 AWARENESS REGARDING PEOPLE WHO HAVE TAKEN PRECAUTIONS TO AVOID USING PUBLIC CHARGE STATIONS

TABLE 4.19 AWARENESS REGARDING PEOPLE WHO HAVE TAKEN PRECAUTIONS TO AVOID USING PUBLIC CHARGE STATIONS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
YES	55	55%
NO	45	45%
TOTAL	100	100%

(Sources Primary Data)

FIGURE 4.19 AWARENESS REGARDING PEOPLE WHO HAVE TAKEN PRECAUTIONS TO AVOID USING PUBLIC CHARGE STATIONS



INTERPRETATION

Out of the 100 responses received, 55% said yes to have taken precautions to avoid using public charging stations, 45% said no and have not taken any precautions to avoid using public charging stations.

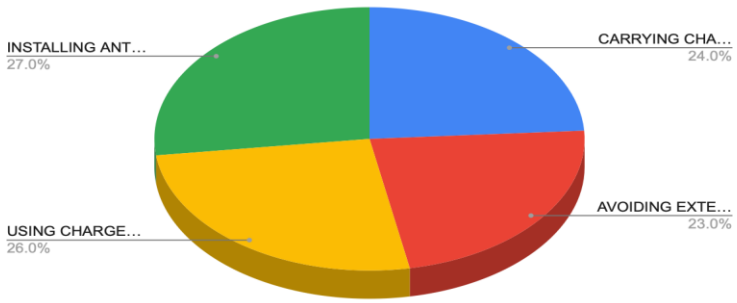
4.20 STEPS TAKEN BY THE INDIVIDUALS TO PROTECT THEMSELVES FROM THE RISKS JUICE JACKING

TABLE 4.20 STEPS TAKEN BY THE INDIVIDUALS TO PROTECT THEMSELVES FROM THE RISKS JUICE JACKING

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGES
CARRYING CHARGERS	24	24%
AVOIDING EXTERNAL ADAPTERS	23	23%
USING CHARGE ONLY CABLE	26	26%
INSTALLING ANTI VIRUS APPLICATIONS	27	27%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.20 STEPS TAKEN BY THE INDIVIDUALS TO PROTECT THEMSELVES FROM THE RISKS JUICE JACKING



INTERPRETATION

Out of all 100 responses received, 24% carried their own chargers, 23% avoided external adapters, 26% will use charge only cables, 27% install anti virus softwares.

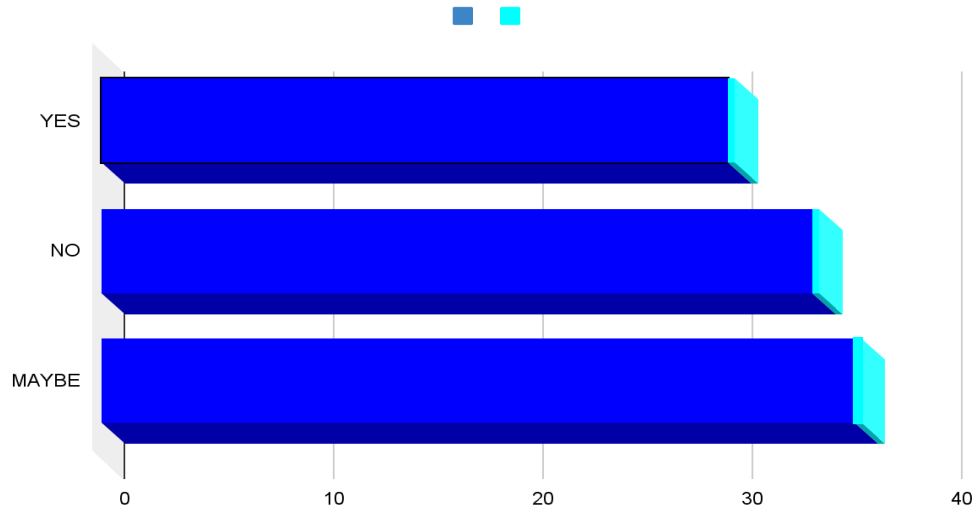
4.21 DATA LOSS FACED BY PEOPLE AFTER USING A PUBLIC CHARGING STATION

TABLE 4.21 DATA LOSS FACED BY PEOPLE AFTER USING A PUBLIC CHARGING STATION

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGE
YES	30	30%
NO	34	34%
MAYBE	36	36%
TOTAL	**100**	**100%**

(Sources Primary Data)

FIGURE 4.21 DATA LOSS FACED BY PEOPLE AFTER USING A PUBLIC CHARGING STATION



INTERPRETATION

Out of the 100 responses received, 30% faced problems such as data loss or unauthorized access, after using a public charging station, while 34% did not face such troubles, while 36% might have faced such troubles.

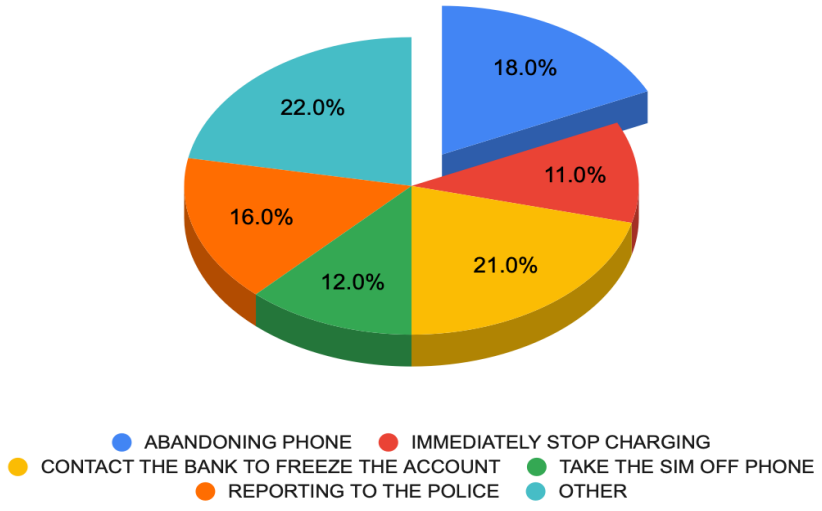
4.22 FIRST STEP TAKEN BY PEOPLE IF THEY BECOME VICTIMS TO JUICE JACKING

TABLE 4.22 FIRST STEP TAKEN BY PEOPLE IF THEY BECOME VICTIMS TO JUICE JACKING

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGES
ABANDONING PHONE	18	18%
IMMEDIATELY STOP CHARGING	11	11%
CONTACT THE BANK TO FREEZE THE ACCOUNT	21	21%
TAKE THE SIM OFF PHONE	12	12%
REPORTING TO THE POLICE	16	16%
OTHER	22	22%
TOTAL	100	100%

(Sources Primary Data)

FIGURE 4.22 FIRST STEP TAKEN BY PEOPLE IF THEY BECOME VICTIMS TO JUICE JACKING



INTERPRETATION

Out of the 100 responses received, 18% will abandon phone as the first measure, 11% will immediately stop charging, 21% will contact the bank to freeze the account, 12% will take the sim off phone, 16.00% will report to the police, meanwhile 22.00% mentioned others.

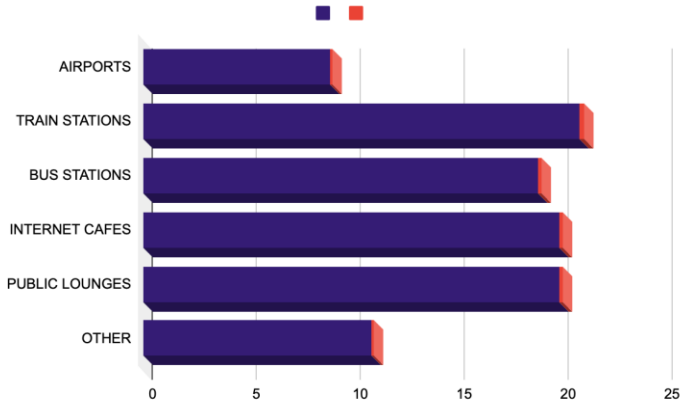
4.23 LIST OF PLACES WHERE JUICE JACKING COMMONLY EXISTS

TABLE 4.22 LIST OF PLACES WHERE PEOPLE BELIEVE JUICE JACKING COMMONLY EXISTS

PARTICULARS	NUMBER OF RESPONSES	PERCENTAGES
AIRPORTS	9	9%
TRAIN STATIONS	21	21%
BUS STATIONS	19	19%
INTERNET CAFES	20	20%
PUBLIC LOUNGES	20	20%
OTHER	11	11%
TOTAL	**100**	**100%**

(Source Primary Data)

FIGURE 4.22 LIST OF PLACES WHERE PEOPLE BELIEVE JUICE JACKING COMMONLY EXISTS



INTERPRETATION

Out of the 100 responses received from where people believe juice jacking commonly occurs, 9% belonged to airports, 21% to train stations, 19% to bus stations, 20% to internet cafes, 20% to public lounges and 11% chose others.

CHAPTER V

FINDINGS, SUGGESTIONS AND CONCLUSION

5.1 FINDINGS

●Most of the respondents belong to the male category (64%), followed by the female category (36%).

●Majority of our respondents are between the age category of 31 and 35 (30%).

●Majority of the respondents fall under the category of employees (46%).

●All the respondents (100%) hold a bank account of their own and also utilize online banking services.

●Majority of the respondents use online banking services for transfer of money (25%), followed by accounts overview (20%), bills payment (19%), other banking services (18%), and credit card management (18%).

●Most of the respondents use google pay (25%) as their main e payment method for utilizing financial transactions.

● Only 43% of the respondents from the study are aware of the banking frauds happening around them, whereas the rest 41% are partly aware and 16% are unaware.

● From the study it is revealed that the most known banking scam among the respondents is online job frauds (18%) followed by ATM card skimming (16%), vishing calls (16%), phishing links (14%), card frauds (14%), and other banking scams (13%). None of the scams are known by 9% of the respondents.

● From the data, 52% of the respondents have received unsolicited emails or text messages asking for banking information.

● It is clear from the study that 36% of the respondents are very cautious about sharing their banking information over the phone.

● Almost 45% of the respondents are very confident in their ability in identifying potential banking scams and fraud attempts.

●From the study that 25% of the respondents review their bank statement every six months for any suspicious activities.

● Around 35% of the respondents use 2 factor authentication to protect their online transactions.

● Only 45% of the respondents have attended workshops on financial literacy and banking security.

- Out of all the respondents only 30% of them are aware of the term juice jacking.
- Almost 25% of the respondents have used public charging stations for charging their phones while being out and among that only 37% of the people are aware of the potential risks associated with it such as leakage of personal data otherwise known as juice jacking.
- It is such that 55% of the respondents carry power banks or portable chargers to avoid the usage of public charging stations.
- All the respondents agreed to the fact that carrying their own chargers while traveling can be an effective step to protect themselves from the risk of juice jacking.
- 22% of the respondents agreed to immediately contact their banks if they encounter a juice jacking incident in the future, followed by contacting the bank to freeze the account (21%).
- Almost 27% of the respondents believe that the risk of juice jacking commonly exists in places like train stations (21%) followed by internet cafes (20%).

5.2 SUGGESTIONS

• Promote launching of targeted campaigns via social media, emails, and traditional media to educate people about common banking frauds.

• Offering workshops or online courses to teach individuals how to safeguard their financial information and recognize suspicious activities.

• Keeping customers informed about the latest fraud trends through newsletters, website updates, and mobile app notifications.

• Encouraging the use of multi-factor authentication for online banking transactions to enhance security.

• Providing easily accessible customer support channels for reporting suspicious activities and seeking guidance.

• Organizing community events or town hall meetings to discuss banking fraud awareness and prevention strategies.

• Incorporating financial literacy and fraud prevention topics into school curriculums and offer workshops at universities to educate students about banking fraud risks.

• Developing online tools or mobile apps that simulate common scam scenarios and provide tips on how to respond appropriately.

• Encouraging customers to regularly review their bank statements and credit reports for any unauthorized transactions or suspicious activity.

• Conducting regular security audits and assessments to identify vulnerabilities in banking systems and processes.

• Collaborating with other financial institutions to share best practices and insights on combating banking fraud.

• Try to provide incentives or rewards for customers who report suspicious activities or participate in fraud prevention programs.

• By creating interactive educational materials such as videos, infographics, and quizzes to engage customers and reinforce key fraud prevention concepts.

• Fostering a culture of vigilance and skepticism among employees and customers to encourage proactive identification and reporting of potential fraud attempts.

5.3 CONCLUSION

In conclusion, the study highlights significant gaps in awareness and preparedness within the community concerning financial security, particularly in the realm of e-payment services and the emerging threat of juice jacking. Despite the widespread usage of banking services, our research revealed a concerning lack of knowledge among bank users regarding various scams and fraud prevention measures. Moreover, the dissatisfaction with the bank's efforts to disseminate information on scams underscores the urgent need for more effective educational initiatives and proactive engagement from financial institutions. Additionally, the alarming ignorance surrounding the term "juice jacking" signifies a critical need for heightened awareness campaigns to educate the public about the risks associated with using public charging stations. Moving forward, addressing these awareness gaps and enhancing preventive measures will be crucial for safeguarding the financial well-being of individuals and strengthening trust in the banking sector amidst evolving technological threats.

BIBLIOGRAPHY

BOOKS AND JOURNALS

- B.R Sharma (2016) ,Bank Frauds: Prevention & Detection including Computers Internet, Smart Phones, ATMs & Credit Cards Crimes .
- Abhik Ray (2015) ,The Bank of India: 100 Years of Prudential Banking

WEBSITES

- https://www.investopedia.com/terms/b/bank.asp
- https://www.fraud.com/post/bank-fraud
- https://www.datavisor.com/wiki/types-of-bank-frauds/
- https://study.com/learn/lesson/bank-fraud-overview-examples.html
- https://global.hitachi-solutions.com/blog/fraud-prevention-in-banks/
- https://groww.in/blog/types-of-banking-frauds
- .https://www.techtarget.com/searchsecurity/definition/juicejacking#:~:text=Juice%20jacking%20is%20a%20security,device%20uses%20to%20sync%20data
- https://securityintelligence.com/articles/juice-jacking-is-it-real-or-media-hype/

ANNEXURE

QUESTIONNAIRE

1. Name

_____

2. Age

(a) between 18 and 22

(b) between 23 and 26

(c) between 27 and 30

(d) between 30 and 35

3. Occupation

_____

4. **Gender**

(a)Male

(b)Female

5. Are you a bank account holder ? .

(a) Yes

(b)No

6. Do you utilize online banking services?

(a)Yes

(b)No

7.Which all online banking services do you use?

(a) Transfer of money

(b) Account overview

(c) Bills payment

(d) Credit card management

(e) Other

8. From the following ,which all e-payment methods do you use for financial transactions?

(a) Google pay
(b) Paytm
(c) ApplePay
(d) PhonePe
(e)Other

9.Are you aware of the banking frauds happening around you?

(a)Yes
(b)No
(c) Sometimes

10. Which all banking scams are you aware of ?

(a) Vishing calls
(b) Phishing links
(c) ATM card skimming
(d) Online job fraud
(e)Card Fraud
(f)None
(g)Other

11. Have you ever received unsolicited emails or text messages asking for your personal or banking information?

(a)Yes
(b)No

12.Are you cautious about sharing your banking details over the phone, even if the caller claims to be from a reputable institution?

(a)Very cautious (b)Moderately cautious (c)Not cautious

13.On a scale of 1-5 how confident are you in your ability to identify potential banking scams and fraud attempts?(1 being very dissatisfied and 5 being very satisfied)

14.On a scale of 1 to 5, with 1 being 'Very Dissatisfied' and 5 being 'Very Satisfied,' how would you rate the various measures adopted by the banks and authorities to better educate and protect individuals from banking scams?
(Scale)
(a)Recommending to use verified apps only.
(b)Be vigilant in sharing your transaction details.
(c)Conduct workshops on how to protect one from banking scams.
(d)Asking not to click on any suspicious links or sms or emails
(e)Only browse on authorized websites only.
(f)Other

15.How often do you review your bank statements and transactions for any suspicious activities?

(a)Every month
(b)Every 2 months
(c)Every 6 months
(d)Yearly
(e) Never

16. Do you use two-factor authentication (2FA) or other security measures provided by your bank to protect your online transactions?

(a)Yes
(b)No
(c)Maybe

17.Have you attended any workshops or seminars on financial literacy and banking security?
If yes, did they provide useful information about protecting yourself from scams?

(a) Yes
(b) No

18. On a scale of 1 to 5, with 1 being 'Very Dissatisfied' and 5 being 'Very Satisfied,' how would you rate your overall satisfaction with the redressal mechanisms provided by the bank to address banking scams?

- 1 (Very Dissatisfied)
- 2 (Dissatisfied)
- 3 (Neutral)
- 4 (Satisfied)
- 5 (Very Satisfied)

19.Have you heard of the term juice jacking?

(a)Yes
(b)No
(c)Maybe

20.Have you ever used public charging stations to charge your mobile devices while being out in public places?

(a) Yes
(b) No
(c) Maybe

21.Are you aware of the potential risks associated with using public charging stations, such as leakage of your personal information including your bank details which is known as juice jacking?

(a) Yes
(b) No

(c) Maybe

22.Have you taken any precautions, such as carrying a power bank or portable charger, to avoid using public charging stations?

(a) Yes
(b) No

23.Based on what you know, what steps do you think individuals should take to protect themselves from the risks of data loss(otherwise known as juice jacking)

(a)Carry your own chargers
(b)Avoid using external adapters
(c)Use only a charging-only cable
(d)Install anti virus applications

24.Have you personally experienced any issues, such as data loss or unauthorized access, after using a public charging station?

(a)Yes
(b)No
(c)Maybe

25.If at all you come across a juice jacking incident in the future,what's the first step you will be taking?

(a) Abandoning your phone
(b) Immediately stop charging
(c) Contact the bank to freeze your account
(d) Take the SIM off your phone
(e) Reporting to the police
(f) Other

26.What all places do you believe that juice jacking commonly happens?

(a)Airports

(b)Train stations

(c)Bus stations

(d)Internet cafés

(e)Public lounges

(f)Other

27. Do you think more people should be aware of the concept of juice jacking?

_____