A STUDY ON CONSUMERS OPINION ON SECURITY AND PRIVACY CONCERNS IN E-BANKING SERVICES

Dissertation

Submitted by

NANDANA SREEPATHY: (SM23C0M013)

Under the guidance of

Ms. NIMA DOMINIC

In partial fulfillment of the requirement for the Degree of

MASTER OF COMMERCE

ST. TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

COLLEGE WITH POTENTIAL FOR EXCELLENCE

Nationally Re-Accredited with A++ Grade

Affiliated to

Mahatma Gandhi University

Kottayam-686560

March-2025

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 CONSUMERS OPINION ON SECURITY AND PRIVACY CONCERNS IN E-BANKING SERVICES" submitted to Mahatma Gandhi University in partial fulfillment of the requirement for the award of Degree of Master in Commerce is a record of the original work done by Ms. Nandana Sreepathy, under my supervision and guidance during the academic year 2024-25

Project Guide

Ms. NIMA DOMINIC

Assistant Professor

Department of Commerce (SF)

Smt. LEKSHMI C

(Head of the Department)

Department of Commerce (SF)

Viva Voce Examination held on....

External Examiner(s)

DECLARATION

I, Ms. Nandana Sreepathy, final year M.Com student (Finance), Department of Commerce (SF), St. Teresa's College (Autonomous) do hereby declare that the project report entitled "A STUDY ON THE CONSUMERS OPINION ON SECURITY AND PRIVACY CONCERNS IN E-BANKING SERVICES" submitted to Mahatma Gandhi University is a bonafide record of the work done under the supervision and guidance of Ms. Nima Dominic , 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.

Nandana

PLACE: ERNAKULAM **NANDANA SREEPATHY**

DATE: 25/04/2025

ACKNOWLEDGEMENT

First of all, I'm grateful to God Almighty for his blessings showered upon me for the successful completion of the project.

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

I'm grateful to our guide **Ms. Nima Dominic,** Department of Commerce (SF) of St. Teresa's College (Autonomous), Ernakulam for her valuable guidance and encouragement for completing this work.

I 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.

I would like to thank **Smt. Lekshmi C**, Head of the Department, for her assistance and support throughout the course of this study for the completion of the project.

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

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

NANDANA SREEPATHY

CONTENTS

ST.TERESA'S COLLEGE (AUTONOMOUS)
ERNAKULAM

Certificate of Plagiarism Check for Dissertation

Author Name	NANDANA SREEPATHY
Course of Study	Master of Commerce
Name of Guide	Ms. Nima Dominic
Department	Commerce (SF)
Acceptable Maximum Limit	20
Submitted By	library@teresas.ac.in
Paper Title	A STUDY ON CONSUMERS OPINION ON SECURITY AND PRIVACY CONCERNS INJ E-BANKING SERVICES
Similarity	4% AI-5%
Paper ID	3442736
Total Pages	53
Submission Date	2025-03-28 09:32:45

Nandana

Signature of Student

Signature of Guide

ST. TERESA'S COLLEGE LIBRARY ERNAKULAM

Checked By
College Librarian

* This report has been generated by DrillBit Anti-Plagiarism Software

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Internet Banking has grown in popularity in recent years because it provides a convenient, quick and low-cost way for costumer to conduct their financial transactions via a web interface. E banking services have reshaped the financial sector providing unmatched convenience and accessibility for both customers and businesses. E banking refers to the electronic facilitation of banking transaction includes a variety of services such as online account management, money transfer, bill payment and access to financial statements.

The growth of the internet and mobile technology has allowed banks to offer these services 24/7 enabling customer to manage their finance from anywhere in the world. This transaction not only simplifies banking operations but also improves the customer experience by minimizing time and providing immediate access to financial information. By advancing online banking technology by efficiently and suitable streaming digital banking management through digital channel.

E banking has transformed how people had managed their finances. Although the convenience and accessibility of online banking services have become widely accepted issues related to security and privacy have faced as key factor affecting customer trust and involvement. This study aims to explore customer's opinion on security and privacy concern associated with E banking services. Through an in-depth analysis we will explore user's view on the security of their financial information the effectiveness of the security measures adopted by banks and how these concerns influence their banking habit.

By gaining insight into this opinion is crucial for financial management to strengthen their security protocol and create a reliable environment that always with cash expectations. This study will add to the ongoing conversation about E banking security and privacy offers, valuable suggestions for banks to enhance their secure and hold customers confidence. Security and privacy concerns have become significant issue for consumers using E banking services. Important Data breaches, Phishing scams, and cyberattack have collected widespread attention heightening fears regarding the protection of personal and financial information. Consumers are becoming more selective about the security measures adopted by banks and how well their data is safeguarded.

As the financial sector becomes more digitally determined, recognizing and addressing consumer concerns has become essential not only for operational success but also as a strategic priority. This study aims to add value both academically and practically by examining the complex relationship between technological advancements, security, privacy, and the trust consumers place in e-banking services.

1.2 STATEMENT OF PROBLEM

E banking has grown tremendously over the past few years and also associated security and privacy concerns have emerged as significant barriers to adoption and trust. This study aims to fill a gap in understanding how consumers perceive security and privacy in e banking services. It also focuses on identifying the main factor that effect on consumers trust on E banking transactions. The goal of study is to identify the concerns of costumer on security and privacy issues in E banking services.

1.3 SCOPE OF THE STUDY

This study aims to investigate consumer opinions on security and privacy issues related to E banking services. It seeks to evaluate how aware consumers are of potential risks like identify theft, Phishing, and data breaches as well as their perceptions of how these risks impact their trust in online banking platforms. Additionally, the study will identify gaps in consumer understanding and offer practical recommendations for banks to improve their security measures and build consumer's trust. It will also recognize limitation related. This research aims to offer meaningful insights into the relationship between consumer behavior, cybersecurity and the increasing dependence on digital banking.

1.4 OBJECTIVES OF THE STUDY

- To study the security and privacy issue of E banking services.
- To examine and analyze the Pre-login and post-login security and privacy features.
- To measure the awareness level of consumers regarding the security of banking transactions.
- To study the relationship between security and privacy concerns and security and privacy satisfaction.

1.5 RESEARCH METHODOLOGY

Research methodology states to the systematic methods and procedures used to carry out research. It includes strategies, techniques, and tools that researchers use to collect, analyze, and interpret data offering a clear plan for how the research will be carried out.

1.5.1 RESEARCH DESIGN

The study applied descriptive research design. The sample of the study includes 150 consumers selected using convenience sampling. The data for study collected through structured questionnaires.

1.5.2 SAMPLE DESIGN AND SIZE

The sample was selected by convenience sampling Technique to gather information helpful for survey. A group of 150 samples were selected for the study.

1.5.3 COLLECTION OF DATA

This study makes use of primary data. Thus, the source of collecting data is a structured questionnaire. The questionnaire consists a set of multiple-choice questions. Secondary data is collected through internet, website, research journals and publications.

1.5.4 RESEARCH INSTRUMENTS FOR DATA COLLECTION AND ANALYSIS

In this study in order to find out the association between various independent variables tools like simple percentage calculation is applied. Thus, for a more comprehensive assessment, simple percentage were utilized to analyze the quantitative data.

1.6 LIMITATIONS OF THE STUDY

- The information provided by the people may be biased.
- Lack of awareness among people regarding detailed E banking security.
- The survey conducted on online, resulting in lack of physical presence.

1.7 CHAPTERIZATION

- Chapter 1 – Introduction.
- Chapter 2 – Review of Literature.
- Chapter 3 – Theoretical Framework.
- Chapter 4 – Data analysis and interpretation.
- Chapter 5 – Findings, suggestions, and conclusion.

CHAPTER II

REVIEW OF LITERATURE

Mahmoud Elkhodr, Seyed Shahrestani, Khaled Kourouche (2012) In this study the mobile machine emulator used for testing mimics real device features through issues may arise with actual phones. This project aims to differ financial institution clients a secure mobile app for accessing their accounts anytime, anywhere. Future efforts will include integrating location verification, allowing users to register their devices and helping institutions verify device use. This enhances e-banking security by adding extra features to the authentication process and automating it improving upon traditional SMS two factor authentication.

Elbek Musaev and Muhammed Yousoof (2015) In this study it revealed that while one institution login page is secure with a virtual keyboard, vulnerabilities were found on the registration page allowing for potential data interception. Bank web server security is not entirely foolproof, even advanced south korean banks have faced hacking attempts, though korea hasn't seen incidents as severe as those in Oman. Future work will explore financial security issues in Oman focusing on the protection of customer data. All banks use two factor authentication with HSBC providing physical security keys. Banks should build customer trust in new technologies and regularly evaluate the security of websites and mobile application.

Syeda & Prasad (2012) In this study the demand for security in online banking is critical. For the sector to continue to grow improvements in privacy and security are necessary. Once these issues are effectively addressed the future of electronic banking can be very promising. In this future customer will engage with their banks without concerns and bank will operate under a unified standard. Current security models for online banking heavily rely on user identification and verification methods, which are also the main areas where many vulnerabilities in internet banking system exist.

Abhipsa, Sai, & Rahul (2017) In this study the risk of privacy breaches is a significant concern for all mobile payment methods. This risk is particularly high if a user loss their mobile phone and even greater if the phone is unlocked or unprotected. Unauthorized access to the device can expose details of transactions made through services like PayTM, Freecharge and BHIM. The study also indicates that security vulnerabilities are inversely related to user's awareness of security threats, technology and phone features. While educating users is important, it is also recommended that operating system and app developers implement basic security measures, such as requiring phone passwords and login credentials as part of their design.

Ruilin (2015) In this study aimed at assessing current levels of client awareness regarding online banking security reveal a connection between awareness and behavior. Some results suggest the

need for further investigation. However, the study indicates that despite widespread fraud, overall client awareness of online banking security remains low, highlighting an urgent need for improvement. Additionally high awareness does not necessarily ensure secure behavior as the latter may not be directly influenced by the former.

Pranjal (2015) In this study the analysis of security issues in e-banking has related that these concerns have become a top priority for banks. Banking fraud is the main reason many individuals or potential clients and online banking as they perceive it to be highly vulnerable to fraud. A solution for consumers is to always look for identification that verifies the security of the website they are using. The ease of transferring funds between banks and across borders in an electronic environment also increases sensitivity to financial policy management. To understand the impact of e-banking on financial policy behavior policymaker require a solid analytical foundation.

Lallmahamood (2007) In this study it measures the impact of perceived security and privacy on the intention to use internet banking. It found that perceived usefulness is also a significant factor influencing users intention to adopt internet banking. It is essential to prioritize the security and safety of online banking. An extended Technology Acceptance Model (TAM) were employed to explore the relationship between perceived security, privacy, and two TAM beliefs perceived usefulness and perceived ease of use regarding the intention to use internet banking. Additionally factors like password security levels and the role of banks as e-payment gateways for e-commerce will help customer confidence and satisfaction.

Lukic (2015) In this study the most effective way to secure against attacks in e-banking include education, personal firewalls, secure socket layers, and server firewalls. A multi-layered security approach that combines firewalls, filtering switches, encryption, and digital certificates can protect client account information from unauthorized access. At a minimum, two-factor authentication should be implemented to verify the authenticity of data related to internet banking services. The first factor can be password, while the second can be a token, such as a smart card. For enhanced security a three-factor authentication process should be considered with the third factor being biometric verification.

Sailaja & Thamodaran (2016) In this study mobile, SMS, and phone banking are user-friendly banking technologies for both banks and customers. Many innovative banking features and services are being added to mobile banking. However there has also been an increase in cybercrimes, fraud, and threats. If banks and customers adhere strictly recommended precautions and security measures.

It is likely that even more significant in user-friendly digital payment transactions at merchant outlets will occur.

Moscato & Altschuller (2012) In this study highlights the importance of client awareness of security by examining the security policies of banks worldwide. These policies serve as tools for banks to manage their user's perceptions. The analysis reveals notable differences in anticipated security concerns across various regions. By understanding the e-commerce background of their target audiences, banks can more effectively manage their potential user's perception of security.

Hayikader, Hadi, & Ibrahim (2016) In this study explored various security issues related to mobile banking apps, examining both the technology involved and the security measures necessary to address these challenges. It is found that mobile banking apps should be built on a strong foundation to enhance security and support future developments. This approach ensures that the apps and their security systems remain resilient over time and require fewer resources for long term management. According to Sidi et al. (2013) most users are well aware of basic internet security measures while respondents with lower educational background lack the technical knowledge needed for online banking.

Adesuyi, Solomon, & Robert (2013) In this study that the current security measures in place for ATM's are insufficient to combat the evolving nature of ATM fraud, highlighting the need for improved security technology. Additionally, some banks have outdated security measures, making them less effective and allowing for potential fraud at ATM. The regulations and standards for e-banking require proper enforcement, as some financial institutions excessively breach these guidelines. The existing security implementations do not provide the necessary protection to safeguard electronic transaction, customer data and funds.

Kaur & Kumar (2013) In this study it found that many bank websites have design flaws that can lead to security breaches. In addition, the security policies of these banks lack a standardized framework and are inadequate, resulting in numerous security risks. A banks security postures is not solely dependent on the measures and practices it implements; it also relies on the awareness of customers using the banking channels and the quality of end-user devices. Hacker often opts for the easiest targets when attempting to exploit vulnerability.

Abu-Shanab & Matalqa (2015) In this study indicated that several factors influence the adoption of e-banking, including usefulness, ease of use, trust and social influence and which are significant in shaping user's intentions. Various fraud detection and prevention strategies have been introduced through numerous studies, some of which have effectively improved the accuracy of fraud detection

and preventions. However, no single approach addresses all the diverse risks and threats faced by e banking platforms. Researchers have suggested multiple authentication strategies, emphasizing the use of a multi-faceted approach, particularly incorporating biometric methods for enhanced security.

Aghaeirad, Fathi-Vajargah, & Afzali (2012) In this study it is designed to be very user friendly for bank clients, eliminating the need to remember multiple passwords for different accounts or separate passwords for online banking. Additionally, clients won't need to carry ATM cards or tokens from various banks. If they know their account numbers, they will only require a one-time password token to access their accounts at different from a nearby location.

Vrancianu & Popa (2010) In this study aims to analyze the potential threats to the security of e-banking services through a thorough review of existing literature. It seeks to identify tools and techniques that can protect consumer security in e-banking and presents findings from a pilot study regarding Romanian consumer perceptions of security related to e-banking services. The conclusion is that there is no single approach that addresses all the various risks facing e-banking platforms, instead a multi-layered security strategy is the best option for ensuring protection. Various solutions are available on the market with the common goal of adding an additional layer of security for consumers requiring them to manually confirm specific transactions.

Sravanthi (2016) In this study it found that technical issues often mislead consumers, making them vulnerable to hackers. Therefore, increasing awareness and providing proper guidance will benefit both customer and banking personnel in addressing e-banking challenges. Research on risks in e-banking shows that while it offers advantages, it also presents problems for both users and banking staff. Compliance, operational, and security risks are promoting banking personnel to focus on solutions through effective risk management strategies. E-banking facilities a higher level of support for costumers in fulfilling their needs.

Abreu, David, & Legcevic (2015) In this study emphasizes the importance of ethics in addressing daily moral issues arising from the use of e-banking services. While these services offer benefits for financial transactions, it is crucial to continuously mitigate security risks and vulnerabilities. The findings highlight various dangers, vulnerabilities, incidents, impacts, and responses effecting e-banking services. To alleviate these risks, fostering open dialogue is essential, as it promotes prevention and detection of evidence- based incidents. This approach not only encourages appropriate behavior but also aims to develop policies that ensure reasonable ethical standards and reduce fraud.

Liaqat, Faisal, surendran, & Thomas (2016) In this study it found that it is crucial for clients using online banking to be aware of the risks lead by cybercriminals, who use tactics such as hacking, phishing, vishing, identity theft, and social engineering to steal sensitive financial information. Only 31% of consumers are aware of these risks, focusing that nearly 70% have limited or no awareness of threats. Therefore, it is essential for e-banking clients to educate themselves about these methods used by cybercriminals.

Fernandes (2013) In this study it examines fraud detection strategies focused on maximizing accuracy while reducing costs. It starts with an overview of payment fraud in e-commerce, defining both fraud and e-fraud. As financial transactions become more digitized, opportunities for e-payment fraud are increasing. The paper concludes with a discussion on prevention and detection measures, including tools for identifying fraud, cost reduction, securing e-payment system and the need for awareness and education.

Garko, Abdulkarim, Gambo, H.B/Kudu, & Salisu (2015) In this study the emerging patterns of various types of fraud associated with ATM card usage, stemming from the revelation of four-digit PINs by certain ATM users in four randomly selected major cities in Nigeria. The paper then suggested a strategy to reduce fraud by altering the operation of existing ATM system to enhance user security, thereby preventing some potentially fraudulent activities.

Singh (2007) In this study it indicates a significant increase in phishing incidents, as shown by the data in various tables. This includes the number of phishing sites created, phishing emails received and financial losses experienced by both users and organizations. The primary reason for these losses and success of fraud is a lack of awareness among some users and service providers (such as banks, ISPSs, and retailers). There is a need for strict measures to educate users and for regular review of security related information for individual users.

Lokhande & Meshram (2015) In this study found that cybercrimes are widespread, with offenders using advanced tools like mobile SIM swapping, anonymizers, and phishing emails. Hacking websites promote various hijacking software, while criminals exploit user's unawareness of spam and phishing risks. It's crucial to implement spam and phishing filters in web browsers and for banks to actively educate customers about potential online banking threats.

Ebem, Yeagba, & Ugwuonah (2017) In this study analyzes the concept of identity theft, the tactics used by cybercriminals, and methods for recognizing social engineering scams. The researcher identified strategies for preventing and addressing these cybercrimes, suggesting that individuals,

banks and the government all have roles in combating identity theft starting with the individual online banking user.

Koskosas (2011) In this study the researcher concludes that understanding business goals and key success factor is crucial for developing an effective fraud prevention strategy, as well as recognizing the potential impact of not meeting these objectives (International Trade Machine (IBM) 2001). There is limited research on organization's experience with fraud prevention and essential factors for e-banking fraud measures, highlighting the need for further investigation into their significance.

Fighting Online Fraud: An Industry Perspective (2017) In this study it found that educating clients on preventing online banking fraud is only one aspect of a bank's fraud defense strategy. Implementing advanced technology that adapts to cybercriminal's changing tactics is crucial for securing the online channel. Clients must trust their bank's online security. Although challenges persist, banks must stay committed to combating online fraud effectively.

Shweta, & Dhirendra (2016) In this study identified an increasing demand for fast and accurate identity verification, authentication, and authorization. To address this, a protective layer for electronic transaction system is proposed to enhance cardholder verification, confirmation, authorization, and security clearances. This involves suggested security measures, including advanced keypad technology for ATMs/EDCs and a shield cover for these keypads. As a result, users will experience a greater sense of confidence and self-assurance in e-transactions.

Karovaliya, Karedia, Oza, & D.R. Kalbande (2015) In this study introduced a new concept to improve the experience and convenience of ATM transactions. It contains features like facial recognition and One-Time Passwords (OTP) for improved security. Facial recognition exclusively identifies users, using their face as a key, which reduces the risk of card theft and fraud. The randomly generated OTP also removes the need for users t remember PINs, serving as a temporary replacement.

Elkhodr, Shahrestani, & Kourouche (2013) In this study analyzes that while the mobile device emulator used for testing the software replicates all features of a real device, some issues may arise with actual devices. The study proposes a mobile application for financial institution clients that enables secure access to their accounts anytime and anywhere. It allows users to register their devices and provide the institution with a way to verify them.

Gyamfi, Mohammed, Nuamah-Gyambra, Katsriku, & Abdulah (2016) In this study identifies a model for modifying existing ATM system to incorporate fingerprint verification and blood group identification, outlining the benefits of using such a system. It is important to note that customer perceptions cannot be generalized, as they are significantly influenced by the users cultural or traditional background.

CHAPTER III

THEORETICAL FRAMEWORK

Information Technology is driving a changing out of traditional services to electronic ones. Various electronical channels, such as ATMs, debit and credit cards, mobile banking, and internet banking, are change the Indian banking sector. These channels have changed how services are delivered to customers. To produce in this competitive market, the Indian banking industry must hold these changes and provide high-quality services, as customers are the ultimate judges of service quality. It is essential for customers to be informed about the advantages and disadvantages of electronic banking services, especially regarding security and privacy, as they seek assurance in these areas. So, assessing consumer awareness of security and privacy issue related to electronic banking services is crucial. E-banking services, also known as electronic banking, involve using digital platforms to carry out banking transactions and access financial services. This current approach allows customers to complete various tasks, such as checking account balances, transferring money, paying bills, and applying for loans, all from their devices whether it's a computer, tablet, or smartphone.

The growth of e-banking has been filled by developments in Information Technology, which have changing traditional banking method. With the common availability of internet connectivity and mobile technology, customers can now access banking services anytime, anywhere, without needing to visit a physical branch. E-banking provides many advantages, including greater convenience, quicker transactions, lower operational costs for banks, and improved service delivery. However, it also raises important issues related to security and privacy, making it crucial for consumers to be aware of these concerns as they hold digital banking. E-banking services show a major change in how financial institutions interact with their customers, highlighting the need for continuous education and awareness in this fast-changing environment.

As e-banking services become more popular, security and privacy concerns are increasingly crucial for both consumers and financial institutions. While the ability to conduct transactions online offers convenience, it also poses risks such as data breaches, identity theft, and unauthorized access to sensitive financial information. With the growing prevalence of cyber threats, customers need to remain aware of the security measures designed to protect their personal and financial data. Additionally, privacy issue regarding the collection and use of customer information have emerged as significant concerns. As banks and financial services leverage advanced technologies to improve user experience and services efficiency, the risk of personal data misuse increases. It is vital for customers to understand how their personal information is managed and protected as they engage with digital banking. The importance of addressing security and privacy concerns in e- banking services, highlighting the need for strong protective measures and informed consumer practices to

build trust in digital banking. As the industry changes, protecting customer data will be essential for the ongoing success of e-banking services.

TYPES OF E-BANKING SERVICES

- **Online Banking:** Access banking services through a web browser on computers, enabling users to manage their accounts, transfer funds, and pay bills.
- **Mobile Banking:** Banking services available through specialized mobile apps on smartphones and tablets, allowing users to conduct banking activities while on the move.
- **ATM services:** Utilizing Automated Teller Machines for cash withdrawals, deposits, and account inquiries without the need for bank personnel
- **Telephone Banking:** Accessing banking services by phone, enabling customers to check their balances, make payments, and conduct transactions through automated systems or live operators.
- **Electronic Fund Transfer (EFT):** Digital transfer of funds between accounts, facilitating electronic payments, direct deposits, and various transactions.
- **Digital Wallets:** Services like PayPal, Apple Pay, and Google Pay that allow users to securely store payment information and make online transactions.
- **Online Bill Payment Services:** Features enabling customers to pay bills electronically through their bank's platform, shortening the payment process.

TYPES OF SECURITIES IN E-BANKING

- **Encryption:** Transforms data into a coded version to safeguard it from unauthorized access while being transmitted. It secures sensitive information such as passwords and personal data.
- **Two-Factor Authentication(2FA):** It necessitates two methods of verification to allow access, such as a password and a temporary code sent to a mobile device. It boosts security by providing an additional layer of protection.
- **Secure Socket Layer:** A protocol that creates a secure encrypted connection between a web server and a browser. It guarantees the privacy and integrity of all transmitted data.
- **Firewalls:** It is a security system that oversee and manage incoming and outgoing network traffic based on set security guidelines. It shields the e-banking system from unauthorized access and cyberattacks.

- **Digital signature:** Electronic signature that utilize cryptographic methods to verify the origin and integrity of a message.
- **Session Timeouts:** The automatic log-off that occurs after a period of inactivity. It protects accounts from unauthorized access when devices are left unattended.
- **Antivirus Software:** This application designed to identify and remove malicious software that can threaten security.

E- BANKING V/S TRADITIONAL BANKING

FEATURES	E-BANKING	TRADITIONAL BANKING
Accessibility	Available 24/7 from any location	Restricted to branch operating hours
Transaction speed	Immediate processing	Can take longer to complete
Fees	Typically, lower fees	Usually higher fees
Personal Interaction	Minimal in- person contact	Direct communication with bank personnel
Security	Vulnerable to cyber threats	Security provided by physical location
Complex services	Can be difficult for intricate needs	More straightforward for complex transactions
Budgeting Tools	Accessible online tools	Limited to services available in branches
Customer support	Mainly online via phone	Support available in person
Notifications	Immediate alerts for transactions	Notification may be slower

ADVANTAGES OF SECURITY IN E-BANKING

- **Safeguarding personnel Information:** It protects personal and financial data, including account numbers and passwords, from unauthorized access.
- **Fraud Prevention:** It strong security measures assist in identifying and stopping fraudulent activities, thereby lowering the risk of financial losses for both banks and their clients.

- **Building Trust:** Effective security and privacy measures promote trust among users, motivating more individuals to engage with e-banking services.
- **Improved Customer Experience:** Security features, like two-factor authentication, provide a smooth yet secure experience for users.
- **Data accuracy:** Ensures that information remains correct and unchanged during transmission, safeguarding against tampering and unauthorized modifications.
- **Lowered Identity Theft Risk:** Strong security protocols reduce the likelihood of personal information theft, protecting users from identity theft.
- **Assurance:** Customers can confidently use e-banking services, knowing their information is secured by advanced measures.

DISADVANTAGES OF SECURITY IN E-BANKING

- **Complexity of security protocols:** Implementing strong security measures can make accessing e- banking services more difficult, possibly confusing some customers.
- **User Inconvenience:** Advanced security features, such as two-factor authentication, may introduce additional step in the login process, which can be unsatisfying for users imperfect quick access.
- **Implementation Costs:** Maintaining high security standards can be expensive for banks, which may lead to increased fees for customers to offset these costs.
- **Technical Weaknesses:** Even with strong security measures, e-banking systems can still be vulnerable to advanced cyberattacks or emerging threats.
- **Concerns about Secrecy:** Improved monitoring and data collection can raise questions about how personal information is utilized and stored, potentially causing suspicion.
- **Inadequate Support services:** Online banking frequently lacks the modified assistance found in traditional banking, leaving users feeling unsupported when security issues arise.

TYPES OF FRAUDS IN E-BANKING

- **Phishing:** Scammers, send fraudulent emails or messages to deceive users into revealing sensitive information, such as passwords or account numbers.
- **Identity Theft:** Criminals gather personal information to impersonate individuals, enabling them to access existing accounts or open new ones in the victim's name.
- **Account Takeover:** Fraudsters snatch control of a user's account by acquiring their login credentials, allowing them to perform unauthorized transactions.

- **Keylogging:** Malicious software is used to track keystrokes on a user's device, taking sensitive data like passwords and credit card numbers.
- **SIM Swapping:** Fraudsters encourage a mobile carrier to switch a victim's phone number to a new SIM card, enabling them to receive two-factor authentication codes and access accounts.
- **Malware and Ransomware:** Malware can be installed on devices to steal data or encode files, demanding a ransom for their restoration.
- **Synthetic Identity Fraud:** Involves creating a new identity using both real and fictitious information, allowing fraudsters to open accounts and commit fraud without detection.
- **Online Auction Fraud:** Scammers take advantage of online marketplaces by selling non-existent goods or services, collecting payment without delivering the secure items.

ROLE OF AI IN FRAUD DETECTION IN E- BANKING

- **Pattern Recognition:** An algorithm can change through big volumes of transaction data to detect patterns that advise fake activity, including identifying rare performances that diverge from typical spending habits.
- **Machine learning Models:** This model is developed using historical transaction data to estimate and identify potentially fraudulent activities. It improves continuously as they are uncovered to new data.
- **Real- Time analysis:** AI system can evaluate transactions promptly, allowing quick detection and response to doubtful activities, which is crucial for minimizing possible losses.
- **Natural Language Processing (NLP):** NLP can observe communication patterns, including emails and chats to identify social engineering tactics or phishing attempts that could lead to fraud.
- **Improved Decision-Making:** AI system can allocate risk scores to transaction, assisting financial institutions in making informed decision regarding the approval or rejection of transactions based on associated risks.
- **Automatic Reporting:** AI can produce reports on suspicious activities helping compliance teams in detecting trends and improving regulatory reporting processes.

DO'S & DONT'S IN E- BANKING REGARDING SECURITY

DO'S	DONT'S
Use strong, unique passwords for each Account	Share your passwords with anyone
Enable two- factor authentication (2FA) whenever possible	Use easily guessable passwords E.g.:(123456)
Regularly monitor your account statements for unauthorized transaction	Ignore suspicious transactions or notification
Keep your banking app and devices updated with the latest security patches	Use outdated software or apps that may have vulnerabilities
Use secure, private networks for online banking (avoid public Wi-fi)	Access your bank account on public or unsecured Wi-Fi
Log out of your account after each session	Leave your banking session open on shared or public devices
Read and understand your bank's privacy policy	Assume that your data is safe without verifying security measures

CASE STUDIES RELATING SECURITY AND PRIVACY IN E- BANKING

1. **Zelle Fraud Cases (2020):** Users of Zelle, a widely used digital payment services reported an increase in fraud cases involving unauthorized fund transfer. This situation revealed weaknesses in user authentication process and the difficulties quickly resolving fraudulent transaction. Financial institutions faced increased pressure to improve consumer protection measure including improved verification processes and cleared fraud reporting mechanism.

2. **Capital One Data Breach (2019):** A weakness in Capital One's system was exploited by a past employee of a cloud service provider, resulting in the introduction of personal information for over 100 million customers. This occasion raised serious issues regarding

data security practices, risk associated with third-party vendors, and the necessity for proper cloud security arrangements. Capital, on faced regulatory scrutiny, concluding in an $80 million settlement. The breach highlighted the need for improved security measures and suggestion with data protection guidelines.

3. **Equifax Data Breach (2017):** While not completely related to e-banking, the Equifax breach exposed considerate information, including social security numbers, of 147 million individuals, affecting financial services. The event heightened awareness about the security of consumer data held by credit reporting agencies and its wider suggestions for financial services. Equifax met significant legal and financial consequences, prompting discussions about regulatory reforms for data protection.

RELATED GUIDELINE ON SAFETY AND SECRECY IN E-BANKING

- **General Data Protection Regulation (GDPR)**

  Area: European Union

  Outline: GDPR follows strict rules on data safety and privacy for individual within the EU and the European Economic Area (EEA). It highlights the importance of finding consent for data collection and allows individual rights over their personal data.

- **California Consumer Privacy Act (CCPA)**

  Area: California, USA

  Outline: CCPA improves privacy rights for California residents by providing them with the right to know what personal data is collected, the right to access that data, and the right to demand its decision.

- **Bank secrecy Act (BSA)**

  Area: USA

  Outline: BSA requires financial institutions to support government agencies in noticing and preventing money laundering. It includes provisions for customer identification and reporting doubtful activities.

FUTURE TRENDS IN E-BANKING SECURITY AND PRIVACY

- **Improved Biometric Authentication**

  The usage of biometric data (fingerprint, facial recognition, voice recognition) for confirmation is expected to grow, offering a more secure and appropriate way to access banking services.

- **Artificial Intelligence and Machine Learning**

  AI and machine learning will remain to evolve in fraud detection and risk assessment, examining huge amounts of transaction data in real-time to identify and prevent doubtful activities.

- **Zero Trust Security Models**

  Accepting a zero-trust approach where no one is important by default will become more dominant. This involves continuous verification of user identities and device health, irrespective of location.

- **Privacy- First Approaches**

  With increasing awareness of data privacy, banks will adopt privacy-first strategies, ensuring that customer agreement is prioritized and personal data is minimized in transactions.

- **Decentralized Finance (DeFi) Security**

  As decentralized investment grows, so will the focus on securing these platforms. New security protocols and frameworks will be developed to address the unique risks related with blockchain technology.

- **Addition Of Blockchain Technology**

  Financial organizations will invest more in cybersecurity training for employees and customers, developing awareness of potential threats like phishing and social engineering.

- **Real-Time Fraud Detection and Response**

  Technologies enabling real-time monitoring of transaction will become standard, allowing for immediate action against fake activities and minimizing potential losses

CHAPTER IV

DATA ANALYSIS AND INTERPRETATION

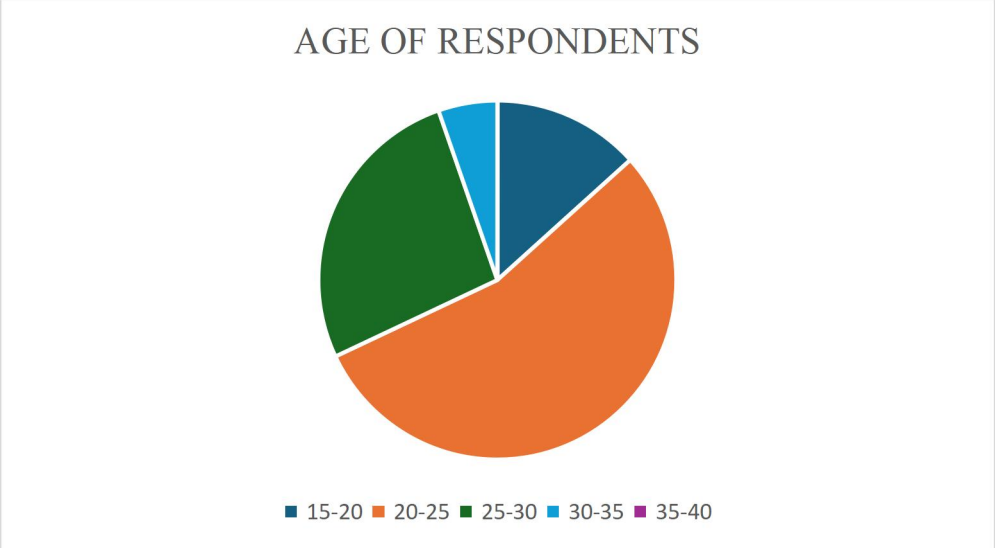
4.1 AGE WISE CLASSIFICATION OF RESPONDENTS

Table 4.1 Age-wise classification of respondents

ATTRIBUTES	RESPONSES	PERCENTAGE
15-20	20	13.3
20-25	82	54.7
25-30	40	26.7
30-35	8	5.3
35-40	0	0
TOTAL	150	100

(Source: Primary source)

Figure 4.1 Age-wise classification of respondents



INTERPRETATION

The data from Figure 4.1 shows that 54.7% of the respondents in the 20-25 age range, according to the age-wise classification of respondents. 26.7% of respondents comes in 25-30 age group, indicating an average level of presence. Otherwise, 13.3% of respondents included in 15-20 age category, while a smaller portion of 5.3% of respondents in 30-35 age -wise classification

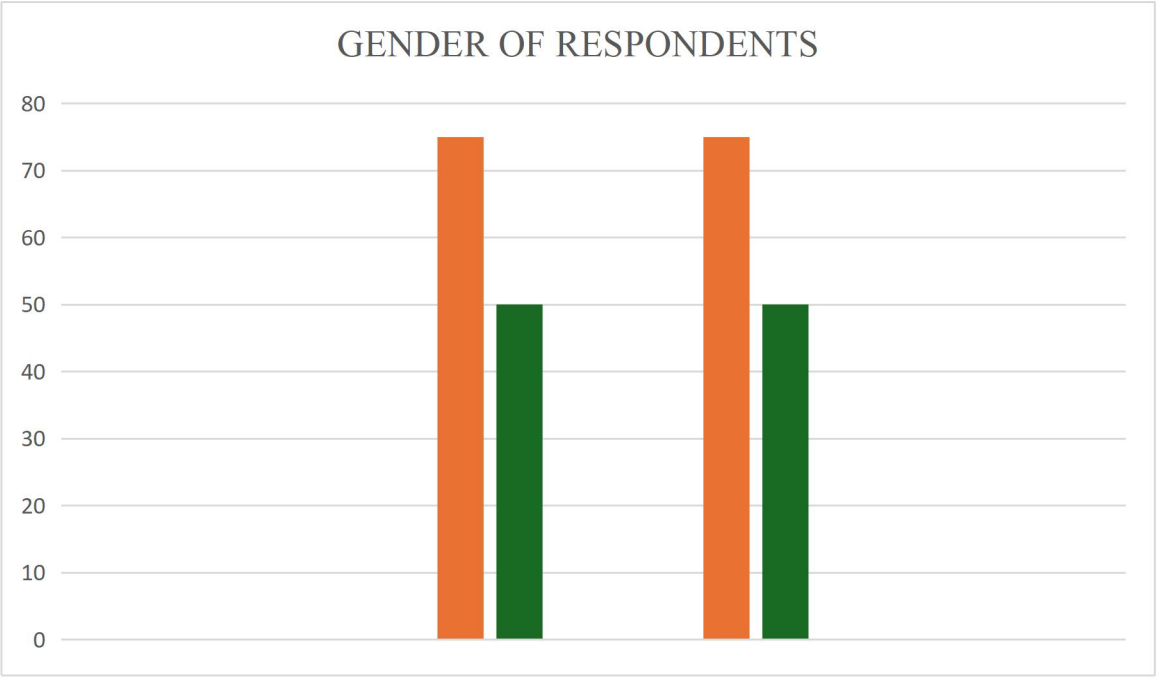
4.2 GENDER WISE CLASSIFICATION OF RESPONDENTS

Table 4.2 Gender wise classification of respondents

ATTRIBUTES	RESPONSES	PERCENTAGE
Male	75	50
Female	75	50
TOTAL	150	100

(Source: Primary source)

Figure 4.2 Gender wise classification of respondents



INTERPRETATION

The data from Figure 4.2 indicating that 50% of respondents are male, while 50% of respondents are Female

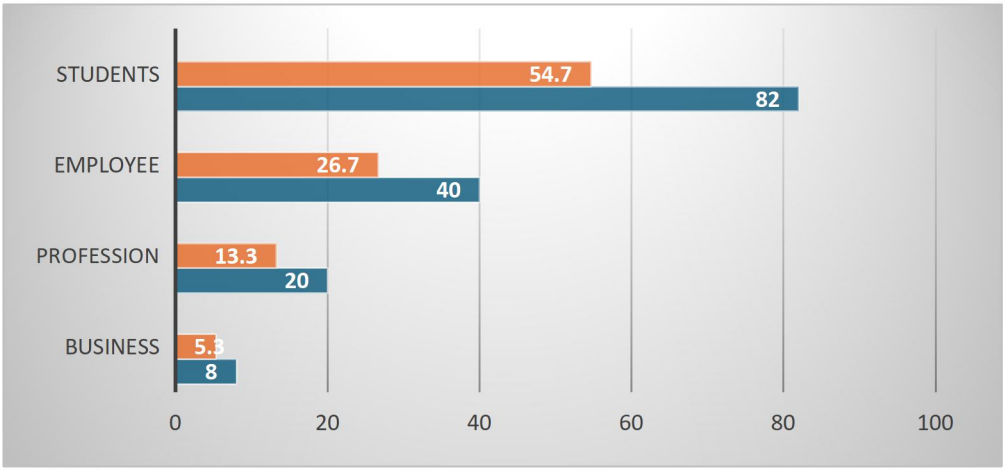
4.3 OCCUPATION OF RESPONDENTS

Table 4.3 Occupation of respondents

ATTRIBUTES	RESPONSES	PERCENTAGE
Business	8	5.3
Profession	20	13.3
Employee	40	26.7
Students	82	54.7
TOTAL	150	100

(Source: Primary source)

Figure 4.3 Occupation of respondents



INTERPRETATION

The data from Figure 4.3 shows that 54.7% of respondents are students, while 26.7% of respondents are employees. On the other hand, 26.7% of respondents are professionals, a smaller portion of 5.3 % of respondents are business category

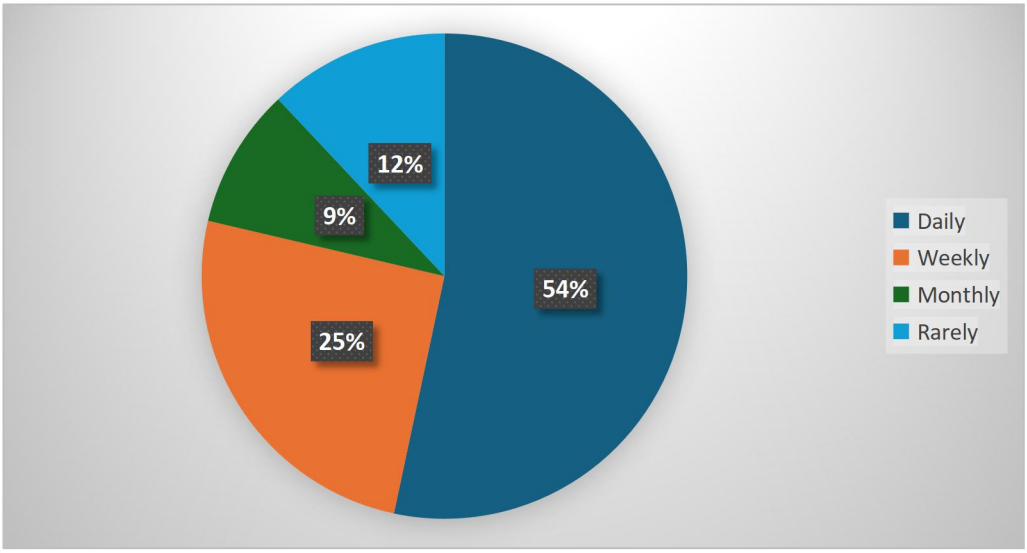
4.4 USAGE OF E-BANKING SERVICES

Table 4.4 Usage of E-banking services

ATTRIBUTES	RESPONSES	PERCENTAGE
Daily	80	53.3
Weekly	38	25.3
Monthly	14	9.3
Rarely	18	12
TOTAL	150	100

(Source: Primary source)

Figure 4.4 Usage of E-banking services



INTERPRETATION

The data from Figure 4.4 shows that 53.3 % of respondents uses E-banking services on daily basis, while 25.3% of respondents uses it weekly basis. Otherwise, 12% of respondents uses it monthly basis, a smaller portion of 9.3 % uses as rarely.

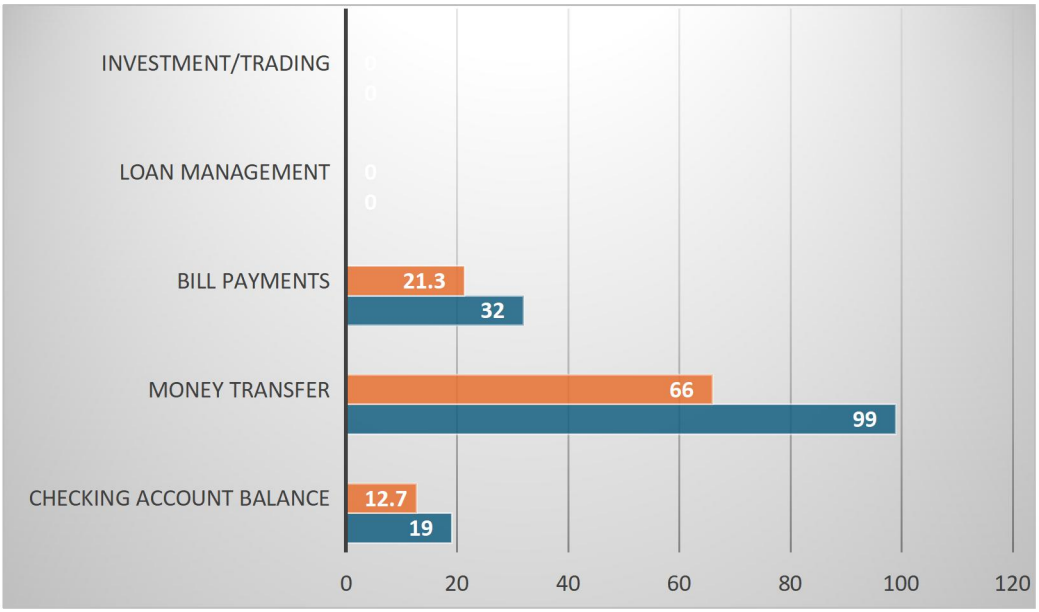
4.5 PRIMARILY USAGE OF E-BANKING SERVICES

Table 4.5 Primarily usage of E-banking services

ATTRIBUTES	RESPONSES	PERCENTAGE
Checking account balance	19	12.7
Money transfer	99	66
Bill payments	32	21.3
Loan management	0	0
Investment/Trading	0	0
TOTAL	150	100

(Source: Primary source)

Figure 4.5 Primarily usage of E-banking services



INTERPRETATION

The data from Figure 4.5 shows that 66% of respondents uses E-banking for transferring money, while 21.3% of respondents uses it for Bill payments. 12.7% of respondents indicates that E-banking services uses for checking account balance.

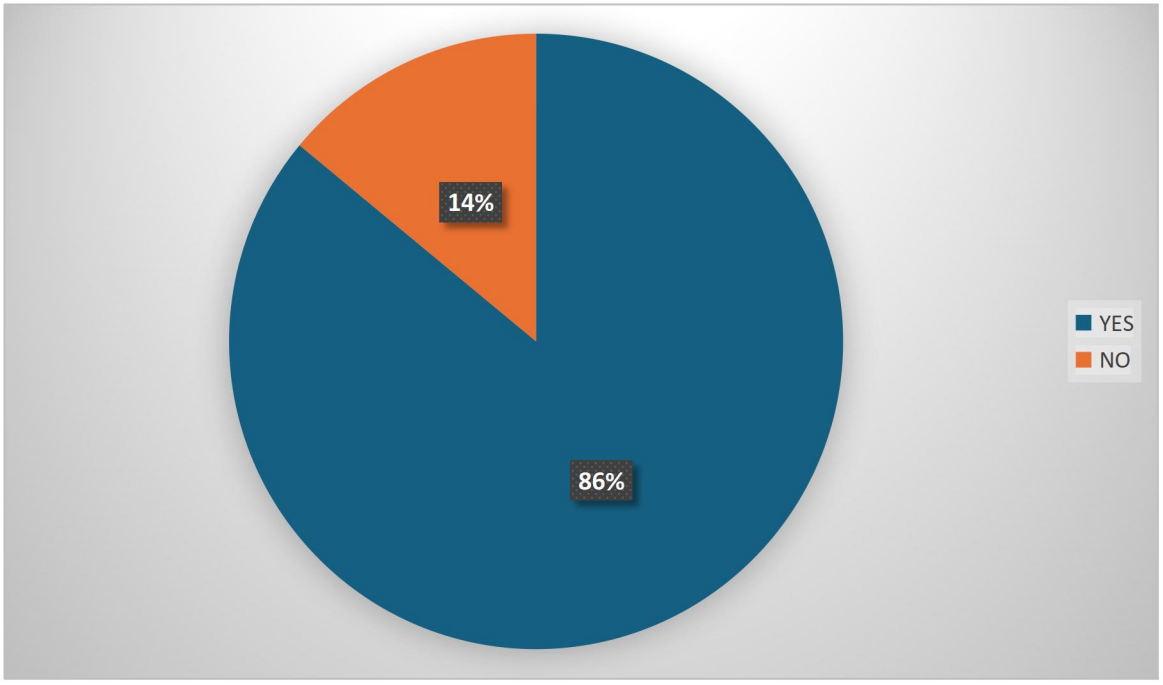
4.6 AWARENESS OF SECURITY MEASURES USED BY BANK FOR E-BANKING

Table 4.6 Awareness of security measures used by bank for E-banking

ATTRIBUTES	RESPONSES	PERCENTAGE
YES	129	86
NO	21	14
TOTAL	150	100

(Source: Primary source)

Figure 4.6 Awareness of security measures used by bank for E-banking



INTERPRETATION

The data from figure 4.6 shows that 86% of respondents are aware of security measures used by bank for E-banking. A smaller portion, 14% of respondents are not aware of security measures used by bank for E-banking services.

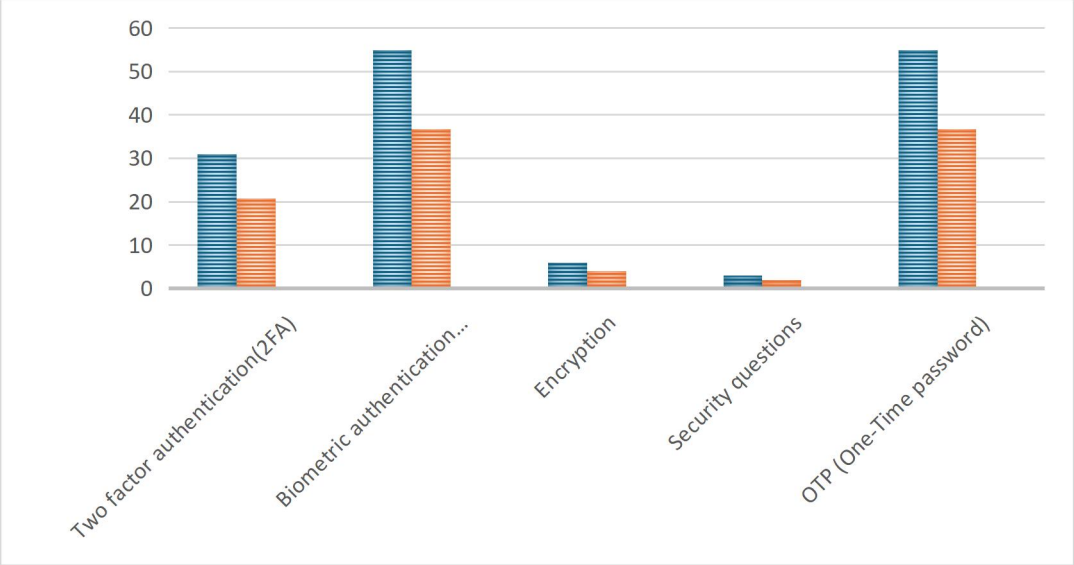
4.7 SECURITY FEATURES AWARENESS OF E-BANKING SERVICES

Table 4.7 Security features awareness of E-banking services

ATTRIBUTES	RESPONSES	PERCENTAGE
Two factor authentication (2FA)	31	20.7
Biometric authentication	55	36.7
Encryption	6	4
Security questions	3	2
OTP (One-Time password)	55	36.7
TOTAL	150	100

(Source: Primary source)

Figure 4.7 Security features awareness of E-banking services



INTERPRETATION

The data from Figure 4.7 indicating that 36.7 % of respondents uses either Biometric authentication and OTP feature, while 20.7% of respondents uses Two factor authentication. A smaller portion of 4% of respondents uses encryption and 2% uses security questions

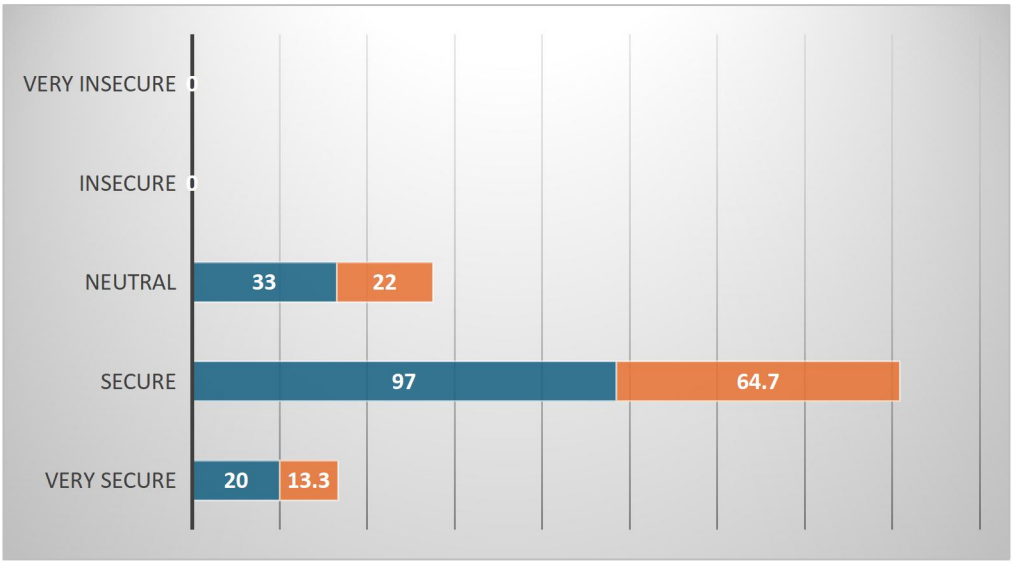
4.8 FEEL OF SECURE WHILE USING E-BANKING SERVICES

Table 4.8 Feel of secure while using E-banking services

ATTRIBUTES	RESPONSES	PERCENTAGE
Very secure	20	13.3
Secure	97	64.7
Neutral	33	22
Insecure	0	0
Very insecure	0	0
TOTAL	150	100

(Source: Primary source)

Figure 4.8 Feel of secure while using E-banking services



INTERPRETATION

The data from Figure 4.8 shows that 64.7 % of respondents feels secure while using E-banking services, while 22 % of respondents feel neutral while they using E-banking services A smaller portion, 13.3% of indicating respondents feels very secure about E-banking services. No respondents feel insecure while using E-banking services.

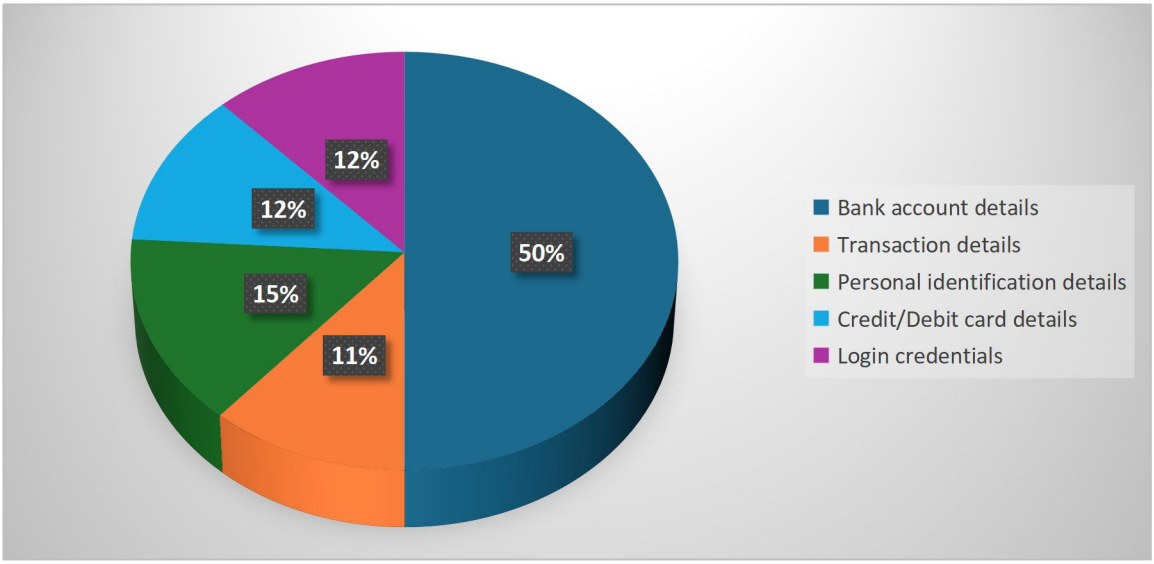
4.9 TYPES OF PERSONAL INFORMATION ARE MOST CONCERNED ABOUT BEING EXPOSED

Table 4.9 Type of personal information are most concerned about being exposed

ATTRIBUTES	RESPONSES	PERCENTAGE
Bank account details	75	50
Transaction details	17	11.3
Personal identification details	22	14.7
Credit/Debit card details	18	12
Login credentials	18	12
TOTAL	150	100

(Source: Primary source)

Figure 4.9 Types of personal information are most concerned about being exposed



INTERPRETATION

The data from Figure 4.9 indicating that 50% of respondents are concerned about exposing Bank account details, while 14.7% of respondents are concerned about Personal identification details. 12% of respondents are concerned about being exposing of their Credit/Debit card details and Login credentials. A smaller portion, 11.3 % of respondents are concerned about their Transaction details of E- banking services.

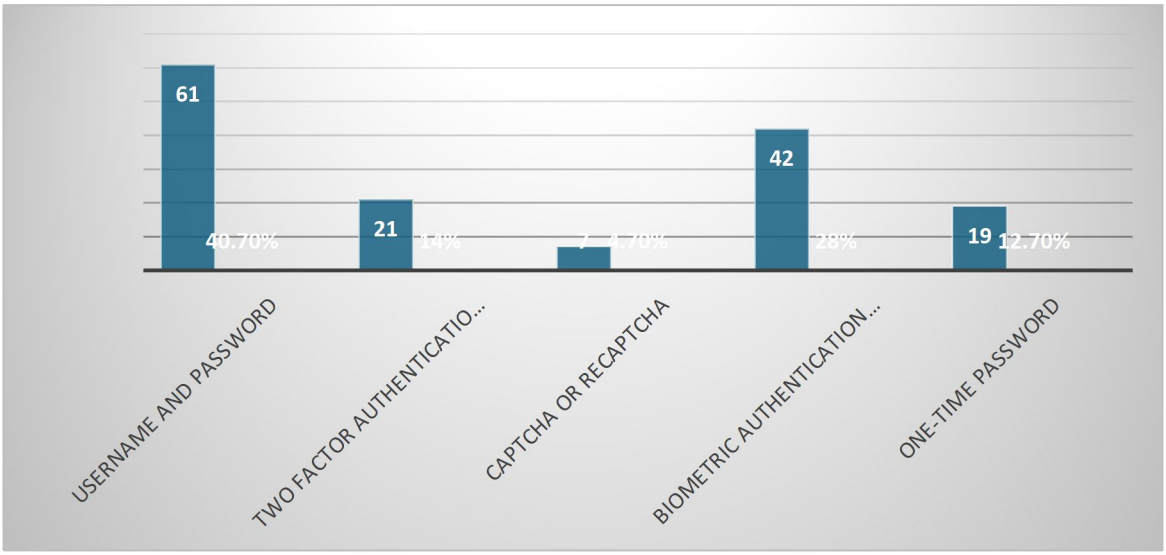
4.10 TYPES OF PRE- LOGIN SECURITY FEATURES WHEN ACCESSING E-BANKING ACCOUNTS

Table 4.10 Types of Pre-login security features when accessing E-banking accounts

ATTRIBUTES	REPSONSES	PERCENTAGE
Username and password	61	40.7%
Two factor authentication (SMS, E mail)	21	14%
CAPTCHA or reCAPTCHA	7	4.7%
Biometric authentication (fingerprint, face recognition)	42	28%
One-Time password	19	12.7%
TOTAL	150	100

(Source: Primary source)

Figure 4.10 Types of Pre-login security features when accessing E-banking accounts



INTERPRETATION

The data from Figure 4.10 show that 40.7% of respondents uses Username and password for accessing E-banking accounts, while 28% of respondents uses Biometric authentication for accessing E-banking accounts. Otherwise, 14% of respondents uses Two factor authentication, while 12.7% of uses One-Time password. A smaller portion 4.7% of respondents uses CAPTCHA or reCAPTCHA for accessing E-banking accounts

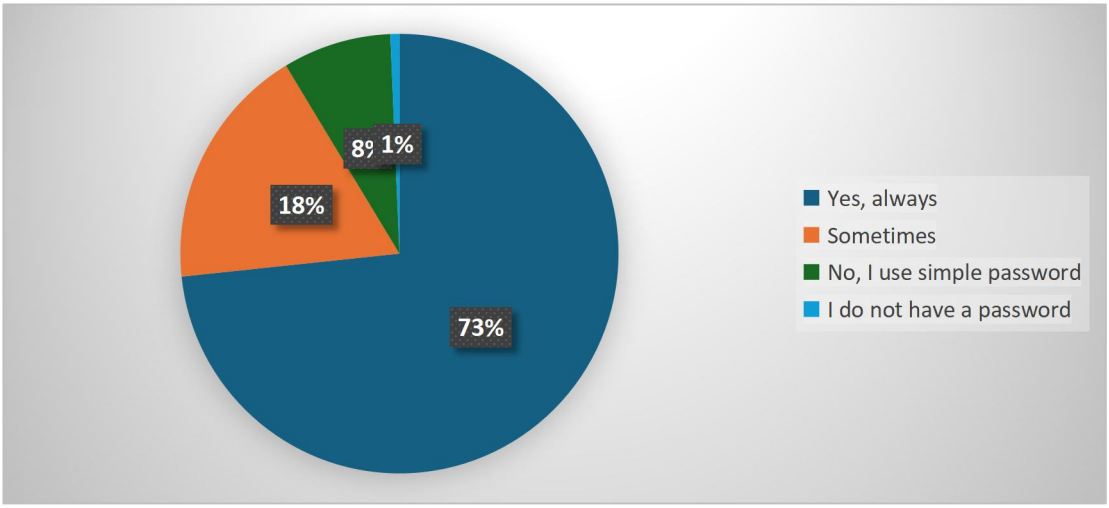
4.11 USAGE OF UNIQUE AND STRONG PASSWORD FOR E-BANKING LOGIN

Table 4.11 usage of unique and strong password for E-banking login

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes, always	110	73.3
Sometimes	27	18
No, I use simple password	12	8
I do not have a password	1	0.7
TOTAL	150	100

(Source: Primary source)

Figure 4.11 usage of unique and strong password for E-banking login



INTERPRETATION

From the above Figure 4.11 shows that majority of respondents 73.3% uses unique and strong password for E-banking login. However, 18% of uses unique and strong password sometimes only, while a small portion of 8% of respondents uses simple password for accessing E-banking login.

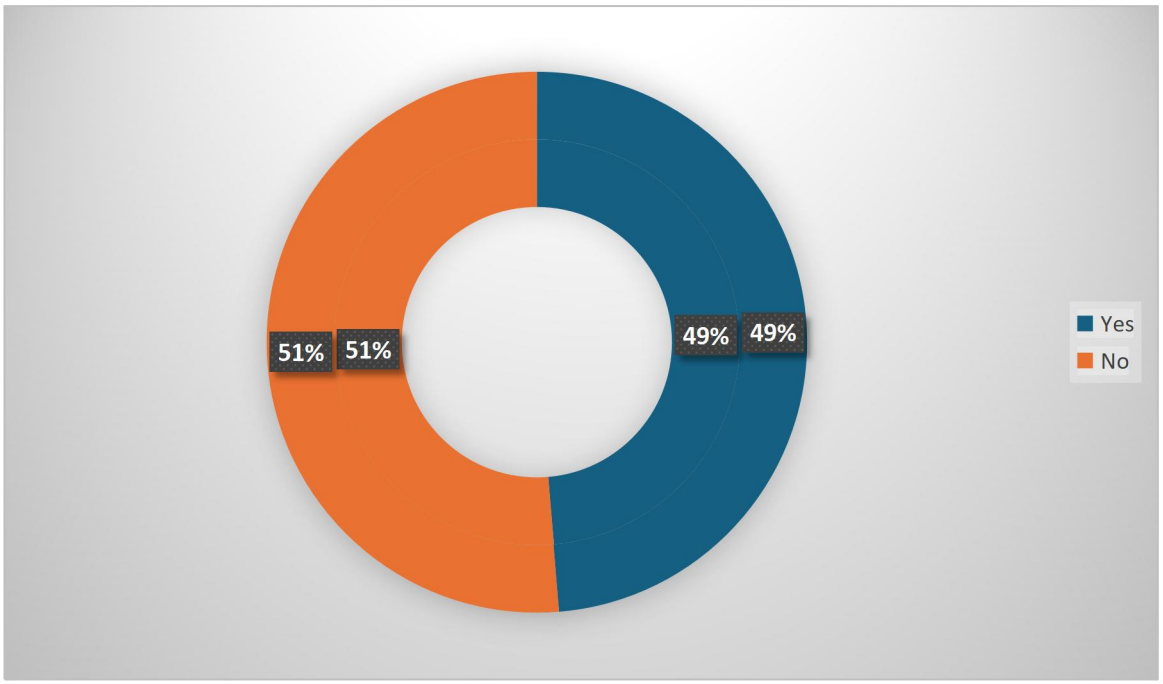
4.12 DIFFICULTY IN ACCESSING ACCOUNT DUE TO LOGIN SECURITY FEATURES

Table 4.12 Difficulty in accessing account due to login security features

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	73	48.7
No	77	51.3
TOTAL	150	100

(Source: Primary source)

Figure 4.12 Difficulty in accessing account due to login security features



INTERPRETATION

The data from Figure 4.12 shows that 51.3 % of respondents never experienced any difficulty in accessing their account due to login security features, while 48.7 % of respondents facing difficulty while accessing account due to login security features.

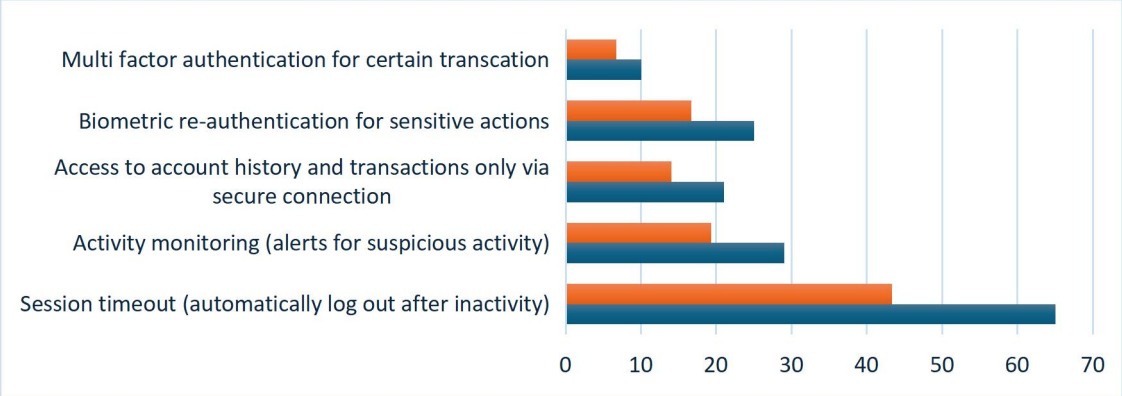
4.13 TYPES OF SECURITY FEATURES ARE ENABLED AFTER LOGGING INTO E-BANKING ACCOUNT

Table 4.13 Types of security features are enabled after logging into E-banking account

ATTRIBUTES	RESPONSES	PERCENTAGE
Session timeout (automatically log out after inactivity)	65	43.3
Activity monitoring (alerts for suspicious activity)	29	19.3
Access to account history and transactions only via secure connection	21	14
Biometric re-authentication for sensitive actions	25	16.7
Multi factor authentication for certain transaction	10	6.7
TOTAL	150	100

(Source: Primary source)

Figure 4.13 Types of security features are enabled after logging into E-banking account



INTERPRETATION

The data from Figure 4.13 indicating that 43.3% of respondents using session timeout after logging into E-banking account, while 19.3% of respondents uses activity monitoring feature after logging into E-banking account. On the other hand, 16.7% of respondents uses Biometric re-authentication for sensitive actions and 14% of uses access to account history and transaction only via secure connection feature after logging. A smaller portion 6.7% uses multi factor authentication for certain transaction security feature.

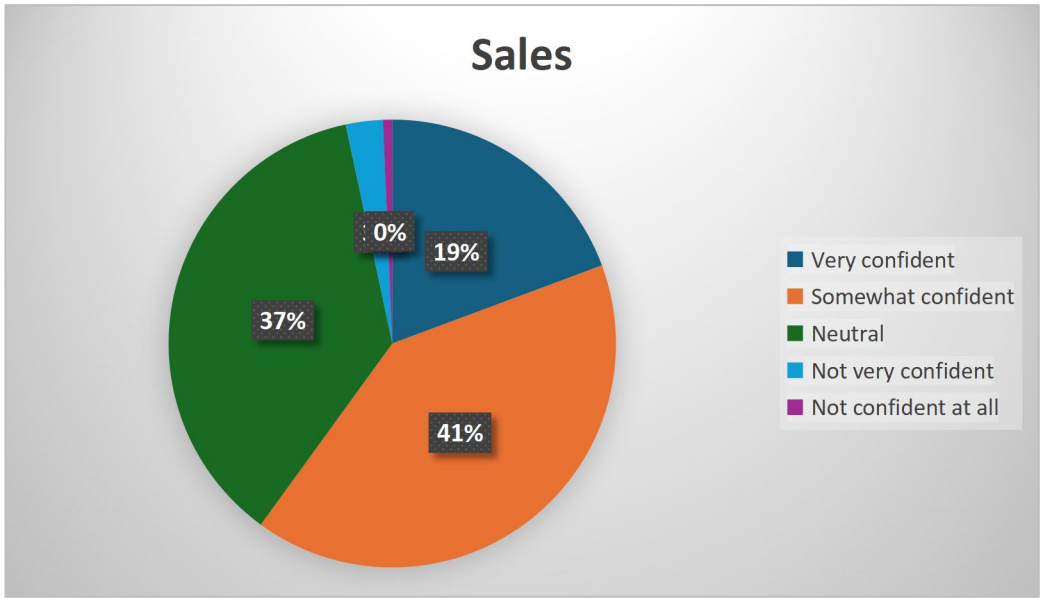
4.14 LEVEL OF CONFIDENT ABOUT E-BANKING ACCOUNT IS SECURE AFTER LOGGING IN

Table 4.14 Level of confident about E-banking account is secure after logging in

ATTRIBUTES	RESPONSES	PERCENTAGE
Very confident	29	19.3%
Somewhat confident	61	40.7%
Neutral	55	36.7%
Not very confident	4	2.7%
Not confident at all	1	0.7%
TOTAL	150	100

(Source: Primary source)

Figure 4.14 Level of confident about E-banking account is secure after logging in



INTERPRETATION

The data from Figure 4.14 show that majority of respondents 40.7% are somewhat confident in the security of their E-banking accounts, while 36.7% of respondents are neutral about secure after logging in. Otherwise, 19.3% of respondents are very confident about security, while a smaller portion are not very confident about E-banking account is secure after logging in.

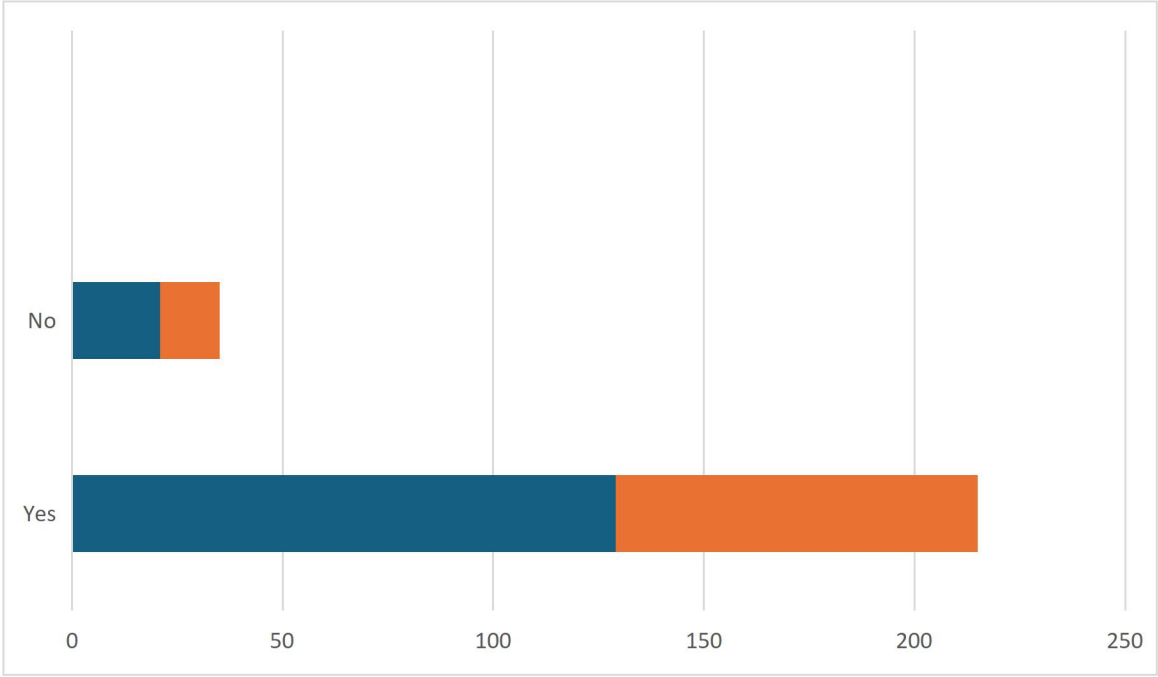
4.15 CONCERNED ABOUT THE PRIVACY OF ACCOUNT INFORMATION WHILE LOGGED IN

Table 4.15 Concerned about the privacy of account information while logged in

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	129	86
No	21	14
TOTAL	150	100

(Source: Primary source)

Figure 4.15 Concerned about the privacy of account information while logging in



INTERPRETATION

The data from Figure 4.15 indicating that 86% of respondents are concerned about the privacy of account information while logging in E-banking account, while 14% 0f respondents are not concerned about the privacy of account information while logging in E-banking accounts.

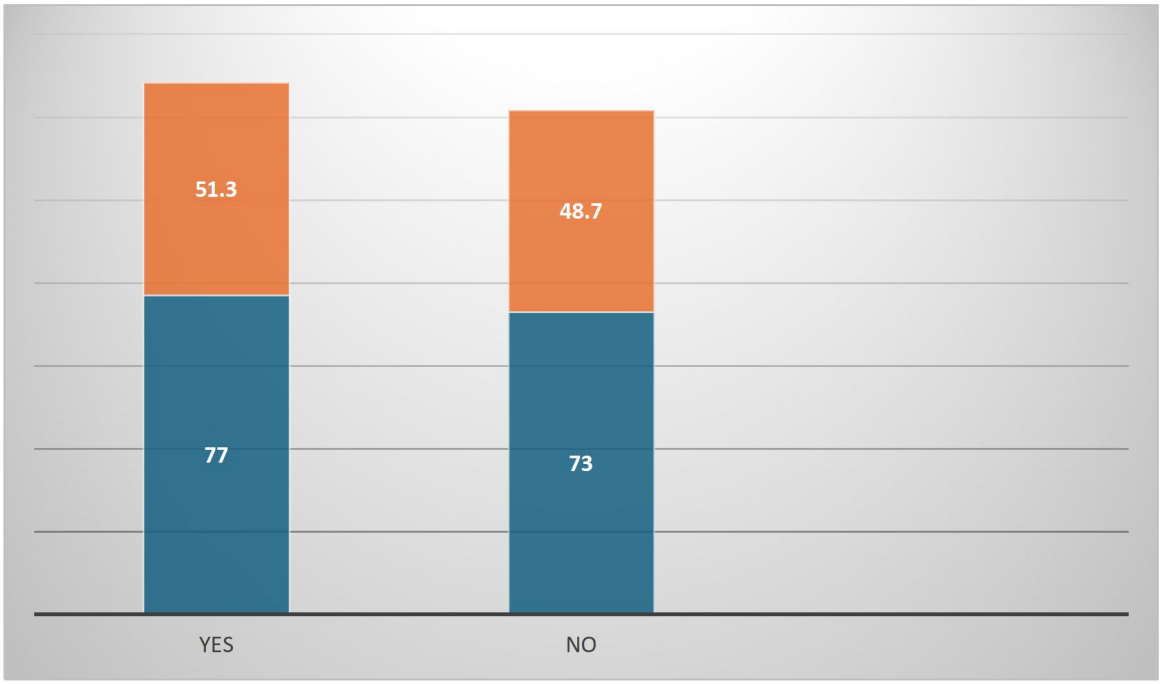
4.16 USAGE OF OPTION TO LOG OUT REMOTELY FROM ANOTHER SERVICES

Table 4.16 usage of option to log out remotely from another services

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	77	51.3
No	73	48.7
TOTAL	150	100

(Source: Primary source)

Figure 4.16 usage of option to log out remotely from another services



INTERPRETATION

The data from Figure 4.16 indicate that majority of users 51.3% using the option to log out remotely from another service, while 48.7% of respondents did not use the option to log out from another service.

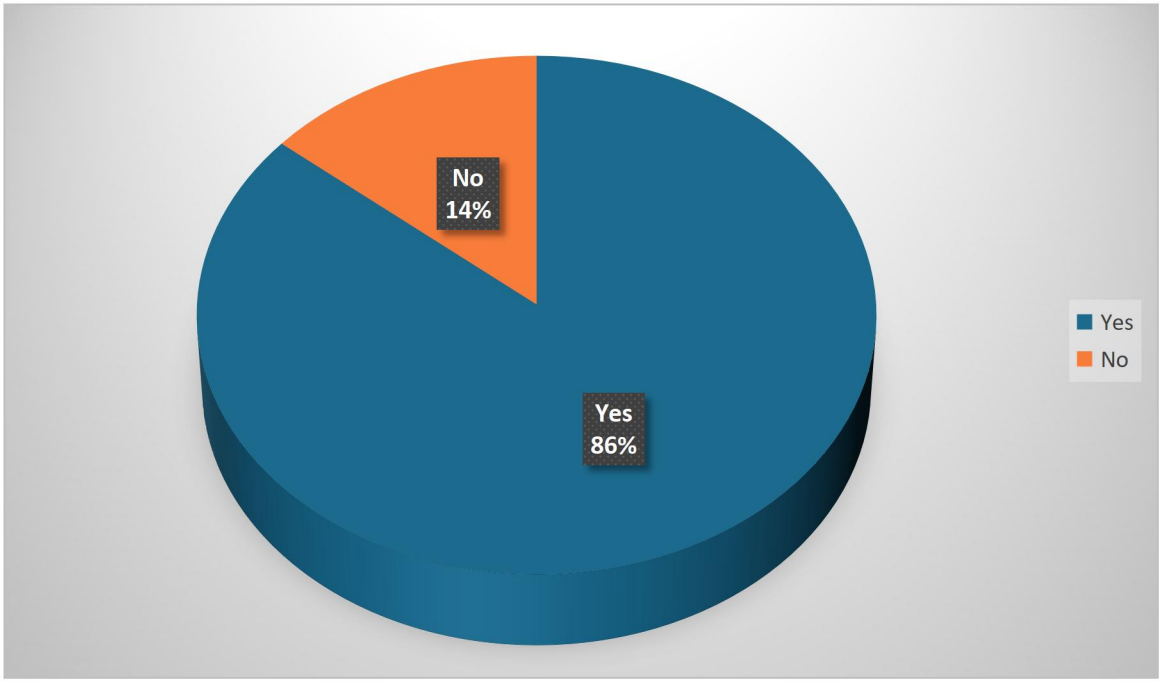
4.17 PRIVACY RELATED TO OPTION OR SETTING FOR POST LOGIN ACTIVITY

Table 4.17 Privacy related to option or setting for post login activity

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	129	86
No	21	14
TOTAL	150	100

(Source: Primary source)

Figure 4.17 Privacy related to option or settings for post login activity



INTERPRETATION

The data from Figure 4.17 shows that 86% of respondents thinks that bank provide more privacy related option or settings for post login activity, while 14% of respondents who thinks that bank does not provide more privacy related option for post login activity in E-banking services.

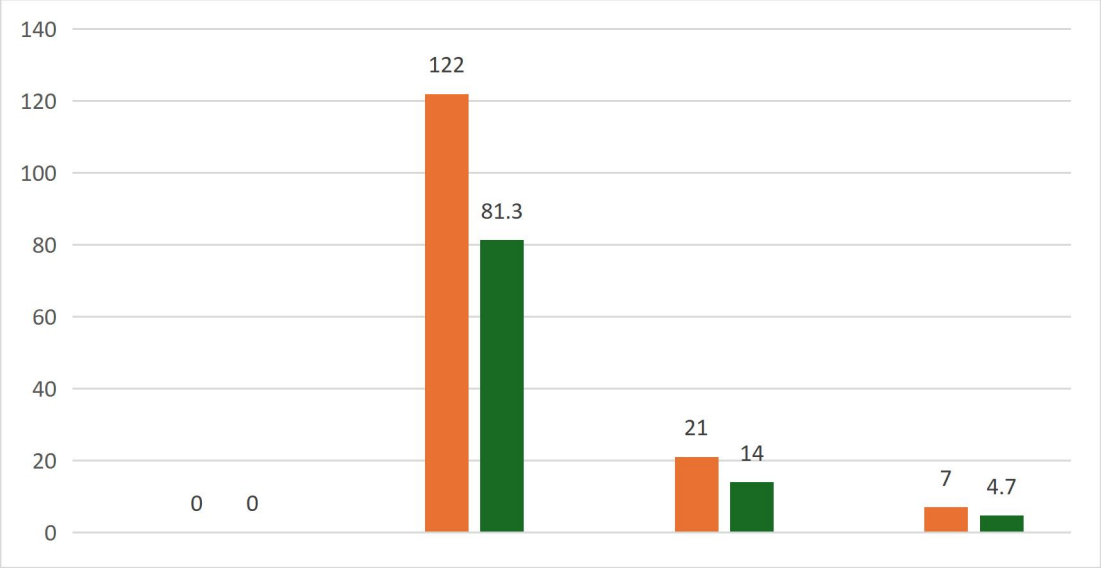
4.18 RECEIVING NOTIFICATIONS FOR TRANSACTIONS OR LOGIN ON WHILE USING E-BANKING ACCOUNT

Table 4.18 Receiving notifications for transactions or login on while using E-banking account

ATTRUBUTES	RESPONSES	PERCENTAGE
Yes, for all transactions	122	81.3
Yes, only for large transactions	21	14
No notifications	7	4.7
TOTAL	150	100

(Source: Primary source)

Figure 4.18 Receiving notifications for transactions or login on while using E-banking account



INTERPRETATION

The data from Figure 4.18 indicating that 81.3% of respondents receives notifications for all transactions on while using E-banking account, while 14% of respondents receives notifications only for large transactions. A smaller portion, 4.7 % of respondents didn't receives any notifications for transactions while using E-banking account.

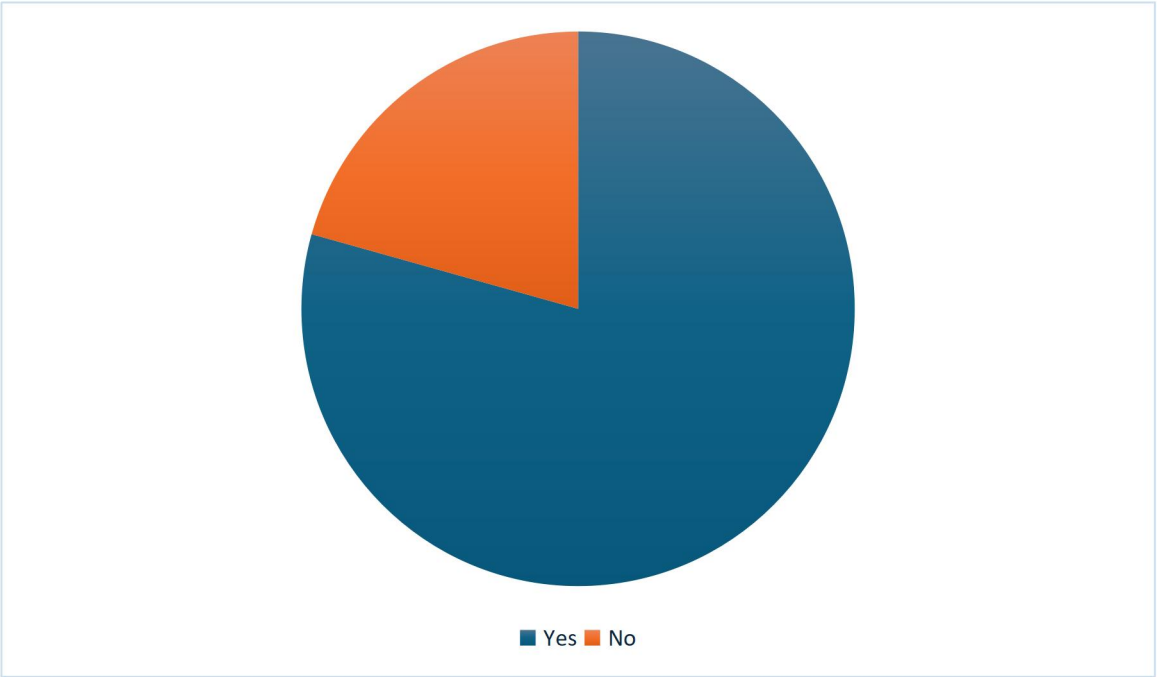
4.19 AWARENESS OF THE SECURITY MEASURES IMPLEMENTED BY BANK TO PROTECT THE TRANSACTION

Table 4.19 Awareness of the security measures implemented by bank to protect the transaction

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	119	79.3
No	31	20.7
TOTAL	150	100

(Source: Primary source)

Figure 4.19 Awareness of the security measures implemented by bank to protect the transaction



INTERPRETATION

The data from Figure 4.19 shows that 79.3% of respondents are aware of the security measures implemented by bank to protect the transactions, while 20.7% of respondents are unaware of the security measures implemented by bank to protect the transactions in E-banking services.

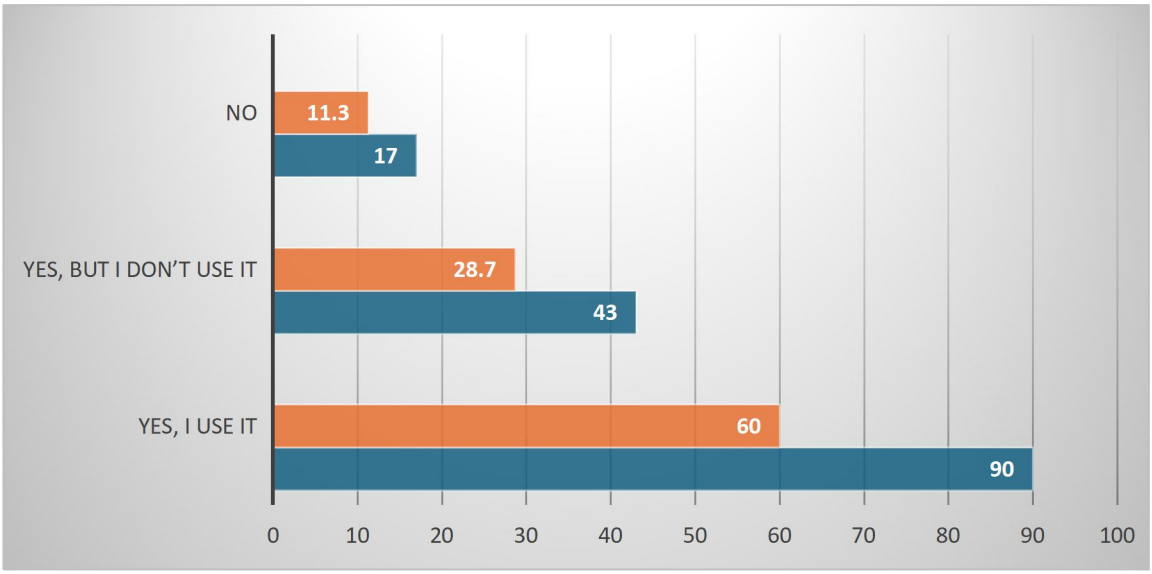
4.20 AWARENESS OF TWO FACTOR AUTHENTICATION AND WORKING OF IT IN E-BANKING SERVICES

Table 4.20 Awareness of Two factor authentication and working of it in E-banking services

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes, I use it	90	60
Yes, but I don't use it	43	28.7
No	17	11.3
TOTAL	150	100

(Source: Primary source)

Figure 4.20 Awareness of Two factor authentication and working of it in E-banking services



INTERPRETATION

The data from Figure 4.20 indicating that 60% of respondents know about Two factor authentication is and how it works, while 28.7% of respondents know about Two factor authentication but they didn't use it. A smaller portion 11.3% of respondents are not aware of Two factor authentication and working of it.

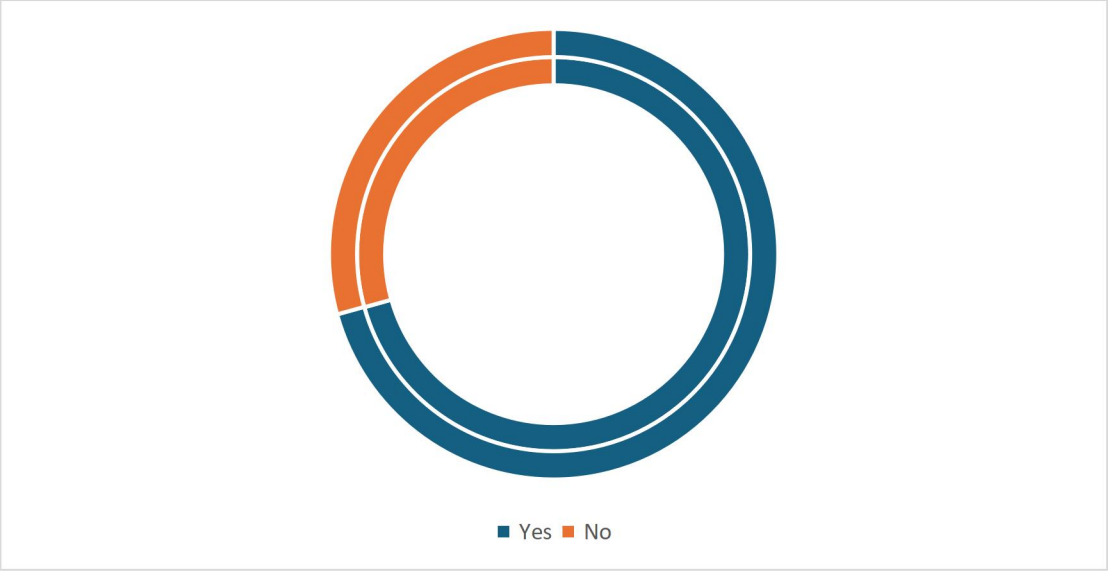
4.21 PROVIDING ADEQUATE EDUACTION AND ALERTS REGARDING SECURITY RISKS IN E-BANKING BY BANKS

Table 4.21 Providing adequate education and alerts regarding security risks in E-banking by banks

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	106	70.7
No	44	29.3
TOTAL	150	100

(Source: Primary source)

Figure 4.21 Providing adequate education and alerts regarding security risks in E-banking by banks



INTERPRETATION

The data from Figure 4.21 shows 70.7 % of respondents thinks that banks provide adequate education and alerts regarding security risks in E-banking, while 29.3 % of respondents didn't think that banks provide enough education and alerts regarding security risks in E-banking services.

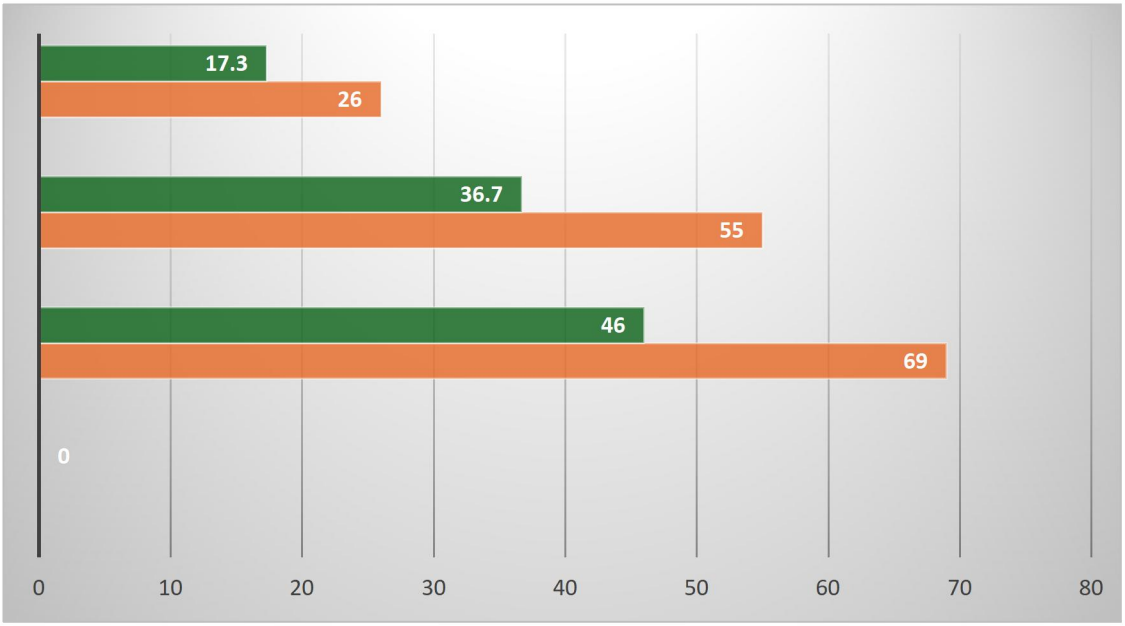
4.22 AWARE OF BANK PRIVACY POLICY AND HOW DATA IS USED

Table 4.22 Aware of bank privacy policy and how data is used

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes, I have read and understood it	69	46
Yes, but I haven't read it in details	55	36.7
No, I haven't read it	26	17.3
TOTAL	150	100

(Source: Primary source)

Figure 4.22 Aware of bank privacy policy and how data is used



INTERPRETATION

The data from Figure 4.22 shows that 46% of respondents are aware of their bank privacy policy and know how data is used, while 36.7% of respondents are aware of bank privacy policy but they didn't know how data is used. Otherwise, 17.3% of respondents are didn't know about the bank privacy policy and how their data is used.

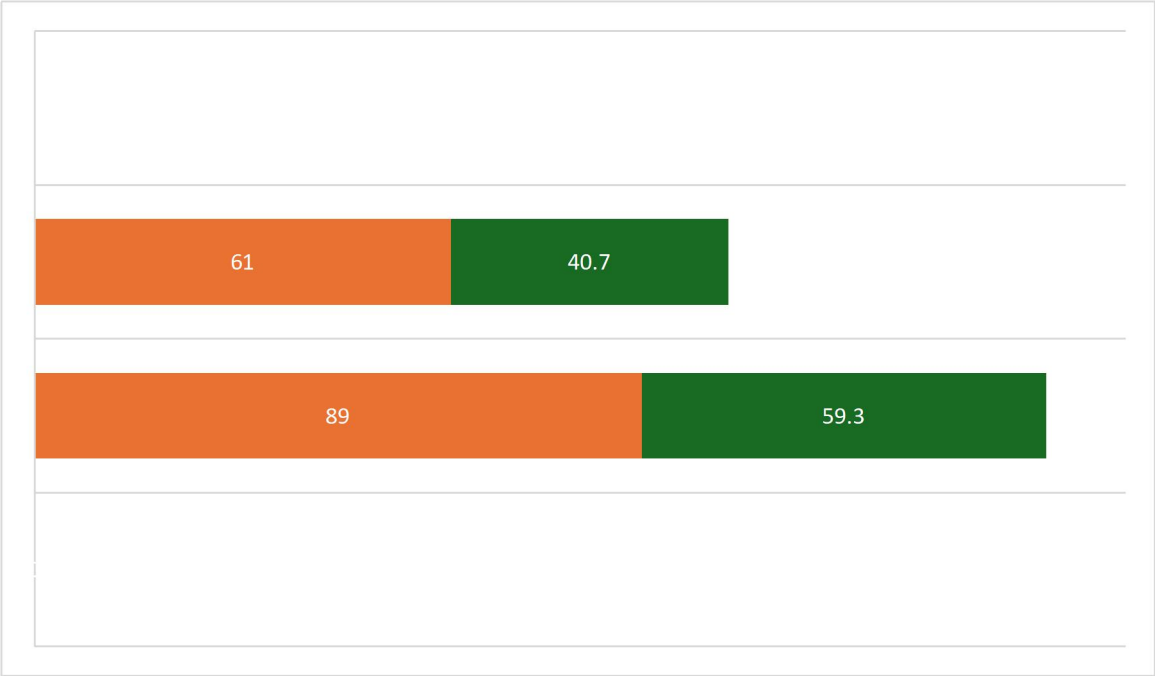
4.23 AWARENESS ABOUT PROTECTION OF PERSONAL DATA FROM UNAUTHORIZED ACCESS BY BANK

Table 4.23 Awareness about protection of personal data from unauthorized access by bank

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	89	59.3
No	61	40.7
TOTAL	150	100

(Source: Primary source)

Figure 4.23 Awareness about protection of personal data from unauthorized access by bank



INTERPRETATION

The data from Figure 4.23 majority of respondents 59.3 % are aware about protection of personal data from unauthorized access by bank in E-banking services, while 40.7% of respondents are unaware about the protection of personal data from unauthorized access by bank in E-banking

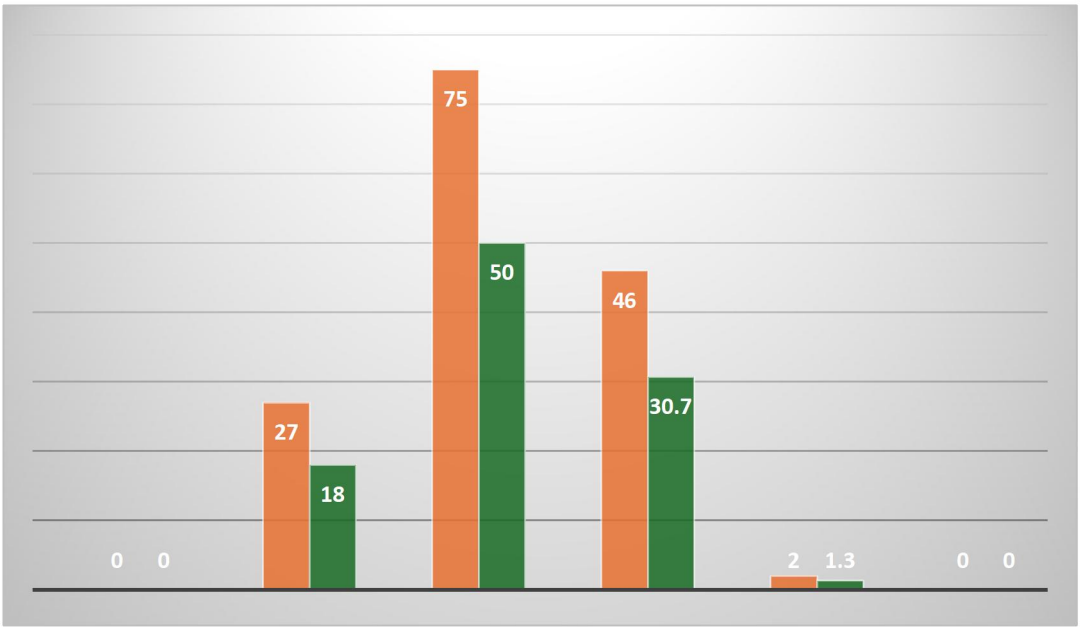
4.24 LEVEL OF SATISFACTION WITH THE SECURITY FEATURES OFFERED BY E-BANKING SERVICES

Table 4.24 Level of satisfaction with the security features offered by E-banking services

ATTRIBUTES	RESPONSES	PERCENTAGE
Very satisfied	27	18
Satisfied	75	50
Neutral	46	30.7
Dissatisfied	2	1.3
Very Dissatisfied	0	0
TOTAL	150	100

(Source: Primary source)

Figure 4.24 Level of satisfaction with the security features offered by E-banking services



INTERPRETATION

The data from Figure 4.24 implies that majority of respondents 50% are satisfied with security features, while 30.7% are either satisfied or dissatisfied with the security features offered by E-banking services. Otherwise, 18% of respondents are very satisfied with features by E-banking. A smaller portion of 1.3% are dissatisfied with the security features offered by E-banking services.

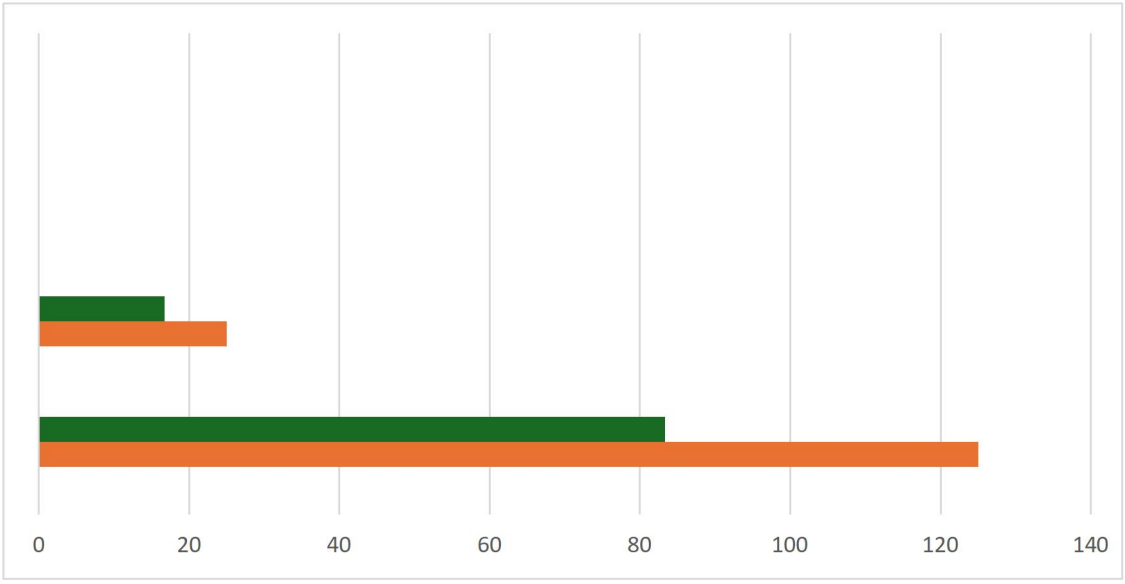
4.25 EFFECT OF SECURITY AND PRIVACY CONCERNS INFLUENCE THE SATISFACTION WITH E-BANKING SERVICES

Table 4.25 Impact of security and privacy concerns influence the satisfaction with E- banking services

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	125	83.3
No	25	16.7
TOTAL	150	100

(Source: Primary source)

Figure 4.25 Impact of security and privacy concerns influence the satisfaction with E-banking services



INTERPRETATION

The data from Figure 4.25 indicating that majority of respondents 83.3% are believe that their security and privacy concerns influence their satisfaction with the E- banking services, while 16.7% of respondents are not believe that security and privacy concerns influence their satisfaction with the E-banking services.

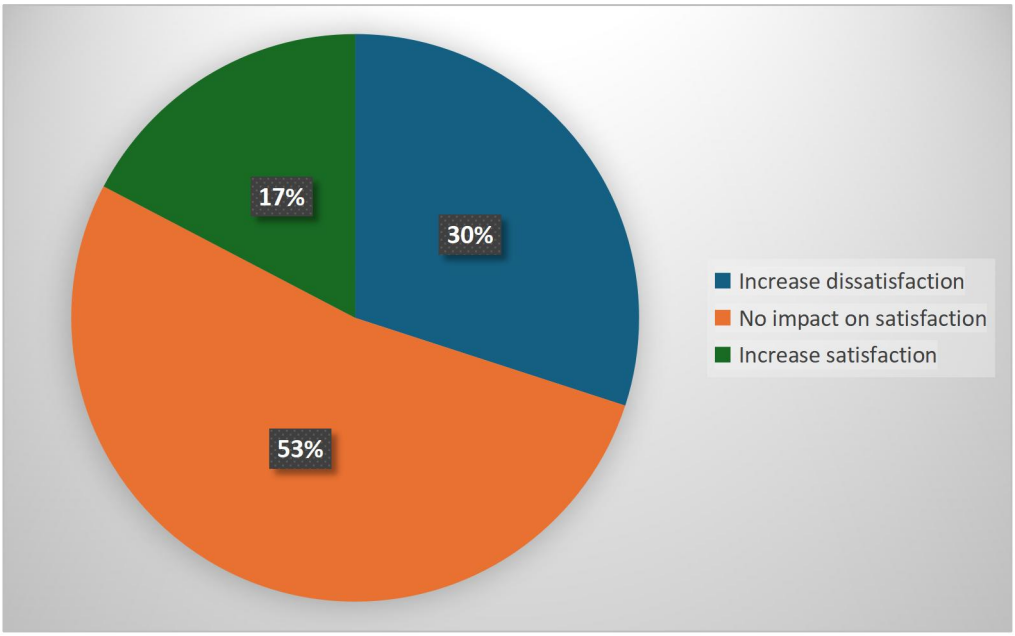
4.26 LEVEL OF SATISFACTION WITH E-BANKING SERVICES WHILE EXPERIENCED HIGHER CONCERNS ABOUT SECURITY AND PRIVACY

Table 4.26 Level of satisfaction with E-banking services while experienced high concerns about security and privacy

ATTRIBUTES	RESPONSES	PERCENTAGE
Increase dissatisfaction	45	30
No impact on satisfaction	79	52.7
Increase satisfaction	26	17.3
TOTAL	150	100

(Source: Primary source)

Figure 4.26 Level of satisfaction with E-banking services while experienced high concerns about security and privacy



INTERPRETATION

The data from Figure 4.26 shows that 52.7% of respondents have no impact on satisfaction while experiencing high concerns about security and privacy, while 30% of respondents have increase their dissatisfaction while experiencing high concerns about privacy and security in E- banking services. A smaller portion of 17.3% of respondents have increase satisfaction with E-banking services while experiencing with high concerns about security and privacy

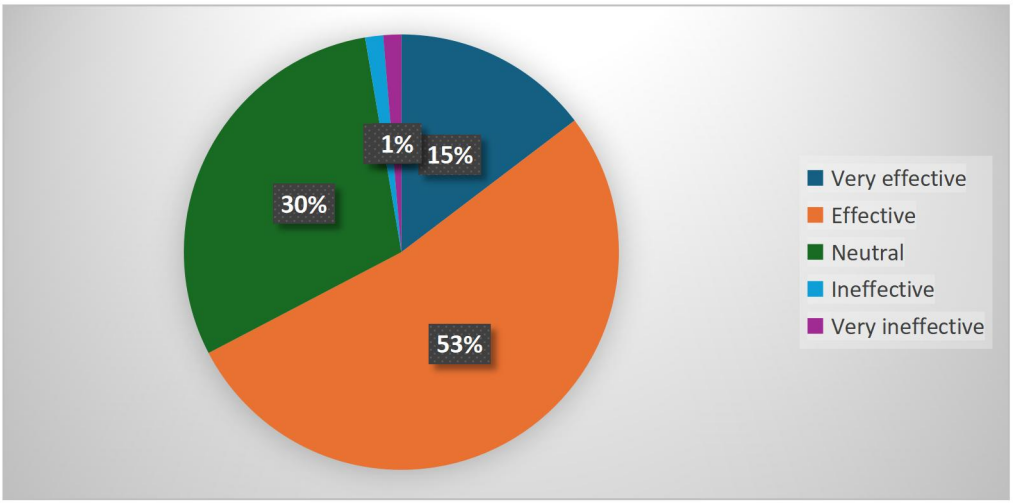
4.27 OVERALL EFFECTIVENESS OF THE PRIVACY PROTECTION MEASURES IMPLEMENTED BY E-BANKING PROVIDER

Table 4.27 Overall effectiveness of the privacy protection measures implemented by E-banking provider

ATTRIBUTES	RESPONSES	PERCENTAGE
Very effective	22	14.7
Effective	79	52.7
Neutral	45	30
Ineffective	2	1.3
Very ineffective	2	1.3
TOTAL	150	100

(Source: Primary source)

Figure 4.27 Overall effectiveness of the privacy protection measures implemented by E-banking provider



INTERPRETATION

The data from Figure 4.27 indicating that 52.7% of respondents are effective with the overall protection measures implemented by E-banking services, while 30% of respondents either effective or ineffective with protection measures. Otherwise, 14.7% of respondents are very effective with the protection measures implemented by E-banking. A smaller portion 1.3% either ineffective or very ineffective with the privacy measures implemented by E-banking services

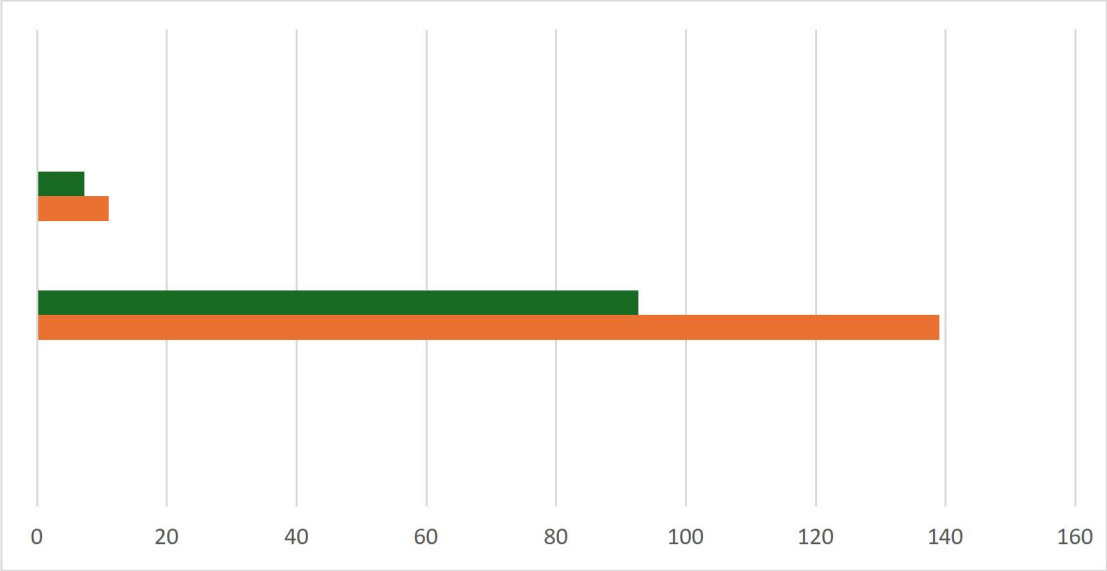
4.28 ADDRESSING SECURITY AND PRIVACY CONCERNS IN E-BANKING LEAD TO GREATER SATISFACTION AND TRUST IN SERVICES

Table 4.28 Addressing security and privacy concerns in E-banking lead to greater satisfaction and trust in services

ATTRIBUTES	RESPONSES	PERCENTAGE
Yes	139	92.7
No	11	7.3
TOTAL	150	100

(Source: Primary source)

Figure 4.28 Addressing security and privacy concerns in E-banking lead to greater satisfaction and trust in services



INTERPRETATION

The data from Figure 4.28 shows that 92.7% of respondents believe that addressing security and privacy concerns in E-banking would lead to greater user satisfaction and trust in the services, while 7.3% of respondents didn't believe that addressing security and privacy concerns in E-banking would lead to greater user satisfaction and trust in services

CHAPTER V

FINDINGS, RECOMMENDATIONS AND CONCLUSION

5.1 FINDINGS

- Majority of respondents are within the age between 20-25 category using E-banking services
- Data are equally collected from male and female category
- Most of the respondents are Students
- Majority of respondents uses E-banking services Daily
- Majority of respondents primarily uses E-banking services for Money transfer
- Most of the respondents are aware of the security measures used by bank for E-banking
- Majority of respondents are equally aware of Two factor authentication and OTP security features in E-banking
- Majority of respondents feel secure when using E-banking services
- Most of the respondents are concerned about exposing of their Bank account details when using E-banking
- Majority of respondents uses Username and password security feature for pre-login when accessing E-banking accounts
- Majority of respondents uses unique and strong password for E-banking login
- Most of the respondents never experienced difficulty in accessing account due to login security features
- Most of the respondents uses Session timeout security feature after logging into their E-banking account
- Majority of respondents are somewhat confident about their E-banking account is secure after logging in
- Majority of respondents are concerned about the privacy of their account information while logged in
- Most of the respondents uses the option to logout remotely from another services
- Most of the respondents thinks that bank provide more privacy related option or settings for post login activity
- Majority of respondents receives notifications for all transactions or logins on using E-banking account
- Majority of respondents are aware of the security measures implemented by bank to protect their transactions
- Most of the respondents uses Two factor authentication and know the working of it

- Most of the respondents thinks their bank provides adequate education and alerts regarding security risks in E-banking
- Majority of respondents are aware of bank privacy policy and understood how their data is used
- Majority of respondents know how their bank protects their personal data from unauthorized access
- Most of the respondents are satisfied with the security features offered by E-banking services
- Majority of respondents believe that their security and privacy concerns influence their satisfaction with the E-banking services
- Most of the respondents have no impact on satisfaction while experiencing higher concerns about security and privacy in E-banking services
- Most of the respondents rate the privacy protection measures implemented by E-banking as Effective
- Majority of respondents believe that addressing security and privacy concerns in E-banking would lead to greater satisfaction and trust in the services

5.2 RECOMMENDATIONS

- Introduce continuous educational initiatives to help users understand security features like Two-Factor Authentication (2FA), OTP, and other relevant measures to maintain and increase user trust.
- Improve security options by introducing biometric authentication or advanced encryption and effectively communicate these features to users to strengthen their confidence in the safety of their personal data.
- Allow users more control over their privacy settings after logging in, such as hiding balances or setting customized session timeouts, addressing their concerns about post-login security.
- Enhance privacy protection through measures like data masking, session locking, or regular security audits to ensure users feel their data is secure.
- Promote the use of 2FA by making it the default setting, offering incentives, and simplifying the activation process to encourage broader adoption and improve overall account security.
- Continue sending transaction alerts and login notifications, and introduce notifications for other activities such as login attempts from unknown devices or changes to account settings.
- Offer educational content after login to emphasize the importance of security features like session timeouts and logging out remotely, increasing users' confidence in the system.
- Ensure transparency about how users' data is collected and utilized, regularly updating and clearly communicating privacy policies to help users understand how their personal information is being protected.

5.3 CONCLUSION

According to the findings and recommendations, it is clear that E-banking services are commonly used, particularly among younger users, with a significant number of persons actively engaging with the platform on a daily basis for tasks like money transfers. Respondents are generally aware of the security measures in E-banking, such as Two-Factor Authentication (2FA) and OTP, and feel secure using these services. However, concerns about privacy, mostly regarding the revealing of account details and the protection of personal information, continue dominant.

Users actively accept security features, including strong passwords, session timeouts, and pre-login measures, contributing to a sense of safety while using E-banking. Notifications related to transactions and logins are well-received, and many users' rapid satisfaction with the security measures implemented by their banks. Despite this, there is a clear need for greater privacy controls and more education on security risks.

To address these concerns, recommendations focus on improving user education, introducing more advanced security options like biometric authentication, and providing users with greater control over privacy settings after logging in. Encouraging the use of 2FA as a default, safeguarding transparency about data usage, and contributing post-login security measures will more strengthen user trust. By applying these recommendations, banks can improve the security and privacy of E-banking services, leading to higher user satisfaction, increased trust, and a more secure overall experience. This will not only address existing concerns but also ensure that users feel confident and protected while using E-banking services.

BIBLIOGRAPHY

BOOKS

- Miller, M (2015) Digital Banking: A Guide to the New World of Online Payments and E-commerce Pearson.
- Nash, L (2019) Banking and Financial Institutions Security: A Guide to Protecting Digital Assets
- Parker, M.J & Mc Daniel, LL (2018): The security and privacy of Online financial Transactions
- Goodwin, P (2016): The privacy and security in E banking protecting consumer information in a Digital World

JOURNALS

- Chong, A.Y.L & Chan F.T.S(2012): A model of consumer adoption of electronic banking services, journal of financial services marketing
- Liu Y, & Zhang J (2017): The influence of privacy concerns on the intention to use e banking services, international journal of information management
- Tufail, M.N &Gohar, S.F (2021): Privacy and security concerns in e-banking, A systematic review, journal of Internet commerce

WEBSITES

https://www.bankingtech.com

https://www.cisa.gov

https://www.nist.gov

https://www.bankofengland.co.uk

APPENDIX

1. How often do you use e-banking services?
    - Daily
    - Weekly
    - Monthly
    - Rarely
2. What e-banking services do you primarily use?
    - Checking account Balance
    - Money transfers
    - Bill payments
    - Loan management
    - No Investment¥Trading
3. Are you aware of the security measures used by your bank for e-banking?
    - Yes
    - No
4. Which of the following security features are you aware of in your bank's e-banking service?
    - Two factor authentication (2FA)
    - Biometric authentication (Fingerprint, face recognition)
    - Encryption
    - Security Questions
    - OTP (one-Time password)
5. How secure do you feel when using e-banking services?
    - Very secure
    - Secure
    - Neutral
    - Insecure
    - Very insecure
6. What type of personal information are you most concerned about being exposed?
    - Bank account details
    - Transaction history
    - Personal identification details
    - Credit¥Debit card details

7. Do you use any of the following pre-login security features when accessing your e-banking account?
    - Username and password
    - Two-factor authentication (SMS, E-mail)
    - CAPTCHA or reCAPTCHA
    - Biometric authentication (fingerprint, face recognition)
    - One-Time Password
8. Do you use unique and strong password for your e-banking login?
    - Yes, always
    - Sometimes
    - No, I use simple passwords
    - I do not have a password
9. Have you ever experienced difficulty accessing your account due to login security features? (e.g.: 2FA, CAPTCHA)
    - Yes
    - No
10. After logging into your e-banking account, which of the following security features are enabled?
    - Session timeout (automatically log out after inactivity)
    - Activity monitoring (alerts for suspicious activity)
    - Access to account history and transactions only via secure connection
    - Biometric re-authentication for sensitive actions
    - Multi-factor authentication for certain transactions
11. Do you feel confident that your e-banking account is secure after logging in?
    - Very confident
    - Somewhat confident
    - Neutral
    - Not very confident
    - Not confident at all
12. Are you concerned about the privacy of your account information while logged in?
    - Yes
    - No

- Not sure

13. Have you ever used the option to log out remotely from another devices (eg: through your bank's website or app)?
    - Yes
    - No
14. Do you think your bank should provide more privacy related option or settings for pots-login activity?
    - Yes
    - No
15. Do you receive notifications for transactions or logins on your e-banking account?
    - Yes, for all transactions
    - Yes, only for large transactions
    - No notification
16. Are you aware of the security measures implemented by your bank to protect your transactions?
    - Yes
    - No
17. Do you know what two-factor authentication (2FA) is and how it works?
    - Yes, I use it
    - Yes, but I don't use it
    - No
    - Not sure
18. Do you think your bank provides adequate education and alerts regarding security risks in e-banking?
    - Yes
    - No
    - Not sure
19. Are you aware of your bank's privacy policy and how your data is used?
    - Yes, I have read and understood it
    - Yes, but I haven't read it in detail
    - No, I haven't read it
    - Not sure
20. Do you know how your bank protects your personal data from unauthorized access?

- Yes
- No
- Not sure

21. How satisfied are you with the security features offered by your e-banking services?
    - Very satisfied
    - Satisfied
    - Neutral
    - Dissatisfied
    - Very dissatisfied
22. Do you believe that your security and privacy concerns influence your satisfaction with the e-banking services?
    - Yes
    - No
    - Not sure
23. When you experience higher concerns about security or privacy, how does it affect your satisfaction with the e-banking services?
    - Increases dissatisfaction
    - No impact on satisfaction
    - Increases satisfaction
    - Not sure
24. How would you rate the overall effectiveness of the privacy protection measures implemented by your e-banking provider?
    - Very effective
    - Effective
    - Neutral
    - Ineffective
    - Very ineffective
25. Do you believe that addressing security and privacy concerns in e-banking would lead to greater user satisfaction and trust in the services?
    - Yes
    - No
    - Unsure