GALGOTIAS UNIVERSITY

A RESEARCH REPORT

ON

‘STUDY OF DIGITAL BANKING FACILTIY IN NCR’

UNDER THE SUPERVISION OF

MS. VAISHALI JOSHI

(ASST. PROFESSOR, SFC, GU)

SUBMITTED BY:

AMAN JHA

B.COM(HONS)

Supervisor's Certificate

This is to certify that **Aman Jha** a student of **B.com (Honors)** in Banking & Finance of School of Finance & Commerce under the Galgotias University has worked under my supervision and guidance for his project work and prepared a project Report with the title **"DIGITAL BANKING IN FACILITIES IN DELHI NCR".**

The project Report, Which she is submitting, in her genuine and original work to the Best of my knowledge.

Place: Greater Noida
Date:

Supervised by:
Asst. Prof. Vaishali joshi
Galgotias University

Signature:

STUDENT DECLARATION

I hereby declared that the project work which the title of ***"Online Banking in India"*** *submitted by me for the partial fulfilment of the degree of B.Com (Honours) in Banking and Finance under the Galgotias University is my own original work and has not been submitted earlier to any other university for the fulfilment of therequirement for any other degree.*

I do hereby also declare that no chapter of this manuscripts in whole or in part has been incorporated in this Report from any earlier books or work done by other or by me. However extract of any literature which has been used for this Report has been duly acknowledged providing detail of such literature in this reference.

Place: Greater Noida

Signature:
Name: Aman Jha
Admission no: 17gsfc101035
Enrolment No: 1708101010

ACKNOWLEDGEMENT

While conducting the Industry Online Banking Oriented Project, innumerable people have given me various suggestions and opinions while conducting the Online Banking Oriented Project. I have tried to incorporate all those suggestions which are really relevant in preparing my final report. I think it is essential to thank all those who have contributed and helped me throughout the duration of the project.

I pay my immense gratitude to Prof. "Vaishali joshi", Faculty of "Galgotias University, Greater Noida for her continuous and deliberate discussion on the topic and indeterminable burden taken by her in helping me throughout conducting the project.

I would also like to thank my friends who rendered their wholehearted co-operation in the successful completion of the project work.

Finally, I am thankful to all the people who willingly responded to the questionnaire and their contribution has been invaluable. This project would not have been completed without their participation.

I am pleased to state that the whole report is just the presentation of the facts that have been found during the project through different sources and its each sentenceis an exact representation of the information obtained and the analysis thereof. I hope that I have manifested my sincere attempts to represent all the information and other things to the best of my ability

AMAN JHA

BATCH (2019-2020)

ADMISSION NO: - 17GSFC101035

CHAPTER 1

INTRODUCTION

Electronic banking, or e-banking, is the term that describes all transactions that take place among companies, organizations, and individuals and their banking institutions. First conceptualized in the mid-1970s, some banks offered customers electronic banking in 1985. However, the lack of Internet users, and costs associated with using online banking, stunted growth. The Internet explosion in the late-1990s made people more comfortable with making transactions over the web. Despite the dot- com crash, e-banking grew alongside the Internet.

- *Online banking (or internet banking or E-banking) allows customers of a financial institution to conduct financial transactions on a secure website operated by the institution, which can be a retail or virtual bank, credit union or building society.*
- *Online banking is the practice of making bank transactions or paying bills via the Internet. Thanks to technology, and the Internet in particular, people no longer have to leave the house to shop, communicate, or even do their banking. Online banking allows a customer to make deposits, withdrawals, and pay bills all with the click of a mouse.*

1.2. HISTORY

While financial institutions took steps to implement e-banking services in the mid-1990s, many consumers were hesitant to conduct monetary transactions over the web. It took widespread adoption of electronic commerce, based on trailblazing companies such as America Online, Amazon.com and eBay, to make the idea of paying for items online widespread. By 2000, 80 percent of U.S. banks offered e-banking. Customer use grew slowly. At Bank of America, for example, it took 10 years to acquire 2 million e-banking customers. However, a significant cultural change took place after the Y2K scare ended. In 2001, Bank of America became the first bank to top 3 million online banking customers, more than 20 percent of its customer base. In comparison, larger national institutions, such as Citigroup claimed 2.2 million online relationships globally, while J.P. Morgan Chase estimated it had more than 750,000 online banking customers. Wells Fargo had 2.5 million online banking customers, including small businesses. Online customers proved more loyal and profitable than regular customers. In October 2001, Bank of America customers executed a record

3.1 million electronic bill payments, totaling more than $1 billion. In 2009, a report by Gartner Group estimated that 47 percent of U.S. adults and 30 percent in the United Kingdom bank online.

OBJECTIVES OF THE STUDY

The main objectives of the study are_

- To understand the genesis and concept of Online-Banking.
- To analyze the importance, functions, advantages and limitations of Online-Banking.
- To explain the different form of Online-Banking and to analyze the rules & regulation regarding Online-Banking guided by RBI.
- To highlighting on the security problems of Online-Banking and how to reduce the security issues with the help of security control tools.
- To analyze the trend of Online-Banking with the help of primary data.
- To analyze the present e-banking scenario concerned with ATM, Internet banking, Mobile banking, credit card-debit card, fund transfer and other e-banking services.
- To examine the impact of ATM, Internet banking, Mobile banking and Credit cards on customer satisfaction by analyzing the problems faced by the customers.

1.3. REVIEW OF LITERATURE

- **An Introduction to E-Commerce**: - written by Ramit Kumar Roy & Debasri Dey and published by the Elegant Publications.
- **E-Commerce**: - written by Prof.(Dr.) Dilip Kumar Chakraborty & Prof. Debdulal Chatterjee and published by B.B. Kundu Grandsons.
- **Introduction to Information Technology & its Business Application:** - written by A.K. Mukhopadhyay & A. Das and published by Kalimata Pustakalaya.

1.4. DATABASE AND METHODOLOGY

- *Data Collection:*

Primary Source: The study is based on both of primary and secondary data. For the purpose of case study primary data have been collected from the people of GHAZIABAD through phone calls, social network and direct interview from them.

Secondary Source: The secondary data have been collected from different articles & website resources such as www.wikipedia.com, www.google.co.in and so many others. We have used simple pictures, tables, & graphs to analysis & present the data. Apart from this I also followed my supervisor's instructions to finish the project.

- ***Sampling Methodology:*** The Primary data have been collected through a survey with a pre-tasted structured QUESTIONNAIRE on a sample of randomly selected 114 people of GHAZIABAD in which some are college students, business persons, service holders, working women and some people who belong to 20-60 age group. From 114 respondents 100 respondents use online banking and the data collected from those people are used to analysis the trend of Net-Banking.

1.5. LIMITATION OF THE STUDY

The major limitations of the study are:

- A small sample size of 114 respondents are taken to primary data analysis. So I cannot draw proper inferences about the respondents from this sample size.
- I have not used modern statistical tools to analysis the data.
- Due to shortage of time I have not been able to make a depth study
- I could not collect data from out site of UTTARPARA.
- This study is based on the prevailing respondents' satisfaction. But their satisfaction may change according to time, fashion, need etc.

1.6. CHAPTER PLANNING

The study is divided into six chapters with reference:

- Introduction
- Online Banking- An Overview
- Different Types of Online Banking
- Online Banking in India-Guidelines of RBI
- Growth of online banking in India
- Findings, Conclusions & Recommendations
- References
- Bibliography.

CHAPTER-2

ONLINE BANKING- AN OVERVIEW

2.1. DEFINITION

- **Online banking** is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual bank, credit union or building society. Online banking is also referred as **internet banking**, **e-banking**, **virtual banking** and by other terms.
- Online banking or E-banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution.
- Online banking is the practice of making bank transactions or paying bills via the Internet. Thanks to technology, and the Internet in particular, people no longer have to leave the house to shop, communicate, or even do their banking.

2.1. HOW ONLINE BANKING EVOLVED INTO A MAINSTREAM FINANCIAL TOOL

In today's highly technical world, it's hard to imagine there was once a time when all banking was conducted at an actual brick-and-mortar financial institution. Even simple account transfers required a trip into the bank.

While today's online banking is filled with amazing innovations, it hasn't always been this easy – in fact it took a long time to get this far.

➢ *HISTORICAL DEVOLOPMENT:*

- The precursor for the modern home online banking services were the distance banking services over electronic media from the early 1980s. The term 'Online' became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line. 'Home banking' can also refer to the use of a numeric keypad to send tones down a phone line with instructions to the bank. Online services started in New York in 1981 when four of the city's major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services using the videotex system. Because of the commercial failure of videotex these banking services never became popular except in France where the use of videotex (Minitel) was subsidised by the telecom provider and the UK, where the Prestel system was used.
- While financial institutions took steps to implement in e-banking services in the mid-1990s, many consumers were hesitant to conduct monetary transactions over the web. It took widespread adoption of electronic commerce, based on trailblazing companies such as America Online, Amazon.com and eBay, to make the idea of paying for items online widespread. By 2000, 80 percent of U.S. banks offered e-banking. Customer use grew slowly. At Bank of America, for example, it took 10 years to acquire 2 million e-banking customers. However, a significant cultural change took place after the Y2K scare ended. In 2001, Bank of America became the first bank to top 3 million online banking customers, more than 20 percent of its customer base. In comparison, larger national institutions, such as Citigroup claimed 2.2 million online relationships globally, while J.P. Morgan Chase estimated it had more than 750,000 online banking customers. Wells Fargo had 2.5 million online banking customers, including small businesses. Online customers proved more loyal and profitable than regular customers. In October 2001, Bank of America customers executed a record 3.1 million electronic bill payments, totalling more than $1 billion. In 2009, a report by Gartner Group estimated that 47 percent of U.S. adults and 30 percent in the United Kingdom are using bank online.

- Today, many banks are internet only banks. Unlike their predecessors, these internet only banks do not maintain brick and mortar bank branches. Instead, they typically differentiate themselves by offering better interest rates and more extensive online banking features.

❖ *First Online Banking Services in the United States:*

According to "Banking and Finance on the Internet," edited by Mary J. Cronin, online banking was first introduced in the early 1980s in New York. Four major banks—Citibank, Chase Manhattan, Chemical and Manufacturers Hanover—offered home banking services. Chemical introduced its Pronto services for individuals and small businesses in 1983. It allowed individual and small-business clients to maintain electronic chequebook registers, see account balances, and transfer funds between checking and savings accounts. Pronto failed to attract enough customers to break even and was abandoned in 1989. Other banks had a similar experience.

❖ *First Online Banking Services in the U.K.:*

Almost simultaneously with the United states, online banking arrived in the United Kingdom. The UK's first home online banking services known as Home link was nset up by Bank of Scotland for customers of the Nottinghamin 1983. The system used was based on the UK's Prestel view link system and used a computer, such as the BBC Micro, or keyboard (Tandata

Td1400) connected to the telephone system and television set. The system allowed on-line viewing of statements, bank transfers and bill payments. In order to make bank transfers and bill payments, a written instruction giving details of the intended recipient had to be sent to the NBS who set the details up on the Home link system.

Stanford Federal Credit Union was the first financial institution to offer online internet banking services to all of its members in October 1994.

Banks and the World Wide Web:

In the 1990s, banks realized that the rising popularity of the World Wide Web gave them an added opportunity to advertise their services. Initially, they used the Web as another brochure, without interaction with the customer. Early sites featured pictures of the bank's officers or buildings, and provided customers with maps of branches and ATM locations, phone numbers to call for further information and simple listings of products.At the beginning of 2004, some 33 million U.S. households (31% of the market) were using one form or another of online banking. Five years later, 47% of Americans were banking online, according to a survey by Gartner Group. Meanwhile, in the UK e-banking grew its reach from 63% to 70% of Internet users between 2011 and 2012.

First Online Banking in India:

ICICI bank is the first one to have introduced Online-Banking in 1994 for a limited range of services such as access to account information, correspondence and, recently, funds transfer between its branches. ICICI is also getting into e-trading, thus offering a broader range of integrated services to the customer.

2.2 FEATURES OF ONLINE BANKING:

Online banking facilities offered by various financial institutions have many features and capabilities in common, but also have some that are application specific.

- *The common features fall broadly into several categories:*

A bank customer can perform non-transactional tasks through online banking, including

I. Viewing account balances.
II. Viewing recent transactions.
III. Downloading bank statements, for example in PDF format.
IV. Viewing images of paid cheques.
V. Ordering cheque books.
VI. Download periodic account statements.
VII. Downloading applications for M-banking, E-banking etc

(B). Bank customers can transact banking tasks through online banking, including –

Funds transfers between the customer's linked accounts.

I. Paying third parties, including bill payments (see, e.g., BPAY) and third-party fund transfers (see, e.g., FAST).
II. Investment purchase or sale.
III. Loan applications and transactions, such as repayments of enrolments.
IV. Credit card applications.
V. Register utility billers and make bill payments.
VI. Financial institution administration.
VII. Management of multiple users having varying levels of authority.
VIII. Transaction approval process.

2.2. THE DISADVANTAGES OF INTERNET BANKING:

Internet banking seems like an obvious choice to leave the hassles of traditional money management behind in exchange for it. However, there are potential problems associated with banking over the internet of which customers may not be aware. Consumers need to weigh the advantages as well as the disadvantages of internet banking before signing up. Some of the disadvantages of internet banking include:

- Bank relationship

A traditional bank provides the opportunity to develop a personal relationship with that bank. Getting to know the people at your local branch can be an advantage when a customer needs a loan or a special service that is not normally offered to the public. A bank manager usually has some discretion in changing the terms of customer's account if the customer's personal circumstances change. They can help customers solve problems such as reversing an undeserved fee. The banker also will get to know the customer and his unique needs. If the customer has a business account,

this personal relationship may help if the customer needs capital to expand. It's easier to get the bank's support if there is someone who understands customer's business and vouch for his operating plan.

- Transaction issues

Sometimes a face-to-face meeting is required to complete complex transactions and address complicated problems. A traditional bank can host meetings and call in experts to solve a

specific issue. Moreover, international transactions may be more difficult (or impossible) with some direct banks. If a customer deposits cash on a regular basis, a traditional bank with a drive-through window may be more practical and efficient.

- Service issues

Some direct banks may not offer all the comprehensive financial services such as insurance and brokerage accounts that traditional banks offer. Traditional banks sometimes offer special services to loyal customers such as preferred rates and investment advice at no extra charge. In addition, routine services such as notarization and bank signature guaranteed are not available online. These services are required for many financial and legal transactions.

- **Security**

Direct banks are subject to the same laws and regulations as traditional banks and accounts are protected by the FDIC. Sophisticated encryption software is designed to protect your account information but no system is perfect. Accounts may be subject to phishing, hacker attacks, malware and other unauthorized activity. Most banks now make scanned copies of cleared checks available online which helps to avoid and identify check fraud. It enables verification that all checks are signed by the customer and that dollar or euro amounts have not been changed. The timely discovery of discrepancies can be reported and investigated immediately.

- Connectivity

Another issue is that sometimes it becomes difficult to note whether your transaction was successful or not. It may be due to the loss of net connectivity in between, or due to a slow connection, or the bank's server is down.

CHAPTER-3

1.1.1 DIFFERENT TYPES OF ONLINE BANKING

3.1 CORE BANKING SOLUTION or CBS:

Core Banking is a banking service provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices. Core banking is often associated with retail banking and many banks treat the retail customers as their core banking customers. Businesses are usually managed via the Corporate banking division of the institution. Core banking covers basic depositing and lending of money.

Normal Core Banking functions will include transaction accounts, loans, mortgages and payments. Banks make these services available across multiple channels like ATMs, Internet banking, mobile banking and branches.

The core banking services rely heavily on computer and network technology to allow a bank to centralize its record keeping and allow access from any location. It has been the development of banking software that has allowed core banking solutions to be developed.

HISTORY

Core banking became possible with the advent of computer and telecommunication technology that allowed information to be shared between bank branches quickly and efficiently.

Before the 1970s it used to take at least a day for a transaction to reflect in the account because each branch had their local servers, and the data from the server in each branch was sent in a batch to the servers in the data center only at the end of the day (Edom).

Over the following 30 years most banks moved to core banking applications to support their operations where CORE Banking may stand for "**centralized online real-time exchange**". This basically meant that all the bank's branches could access applications from centralized data centers. This meant that the deposits made were reflected immediately on the bank's servers and the customer could withdraw the deposited money from any of the bank's branches.

ADVANTAGES:

1. Centralized Accounting:

i) All the transactions of the bank directly impact the General Ledger and Profit and Loss Account. This provides a real time total picture about the financial position and situation of the bank

ii) This helps for timely effective decision making for financial management, a very critical and dynamic function in today's banking.

2. Centralized Product Control & Monitoring:

i) Centralization helps in better product analysis, monitoring and rollout.

ii) Aspects like interest rate modifications, product modification and interest application can be done centrally from one place for all the branches.

iii) Bank can quickly respond to market scenario and customer needs. This gives competitive edge to the bank.

3. Introduction of Technology Based Services:

i) Service channels such as ATM, either on-site or offsite, can be started.

ii) Cheque Deposit Machines (CDM) can be installed. Such machine in WAN connectivity can allow any customer to deposit the cheque for collection at any branch.

iii) Cheque book printing machine can be installed at central location to give personalized cheque books. Such machine in WAN connectivity can receive command from any branch.

4. Centralized Customer Account Management:

i) Any customer becomes the customer of the bank rather than of a branch.

ii) With unique ID / Account Number the accounts of the customers can be viewed centrally by the bank. As such, customer profile, details of products and services availed by him and customer behavior about business of the bank can be well understood.

iii) Such customer view gives the bank opportunity to decide directions for business development and marketing strategies.

5. Advantages to Head Office:

i) Consolidation of MIS / statements / reporting at one place reducing duplication of tasks at branches and it is of real time.

ii) Supervision of branches on risk perceptions possible as ongoing process.

iii) Frequent audits and timely control measures can be initiated.

iv) Faster and practically real time reconciliation of accounts.

v) Centralized marking and movement monitoring of NPA accounts.

vi) Better ALM, especially for short term assets and liabilities possible.

vii) Audit on operational aspects of the accounts can be done at a single location as entire data is available at one place.

viii) By installing mailing solution on the intra net of the bank, written communication in the form of letters, between H. O. and branches and vice versa, can be eliminated.

6. Advantages to Branch:

i) With reduced work at the branches they can focus on development of business, customer service and attendance and meaningful liaison with customer for getting new business.

ii) Since customer needs are known with proper analysis they can be well attended even before their demands that boosts the image of bank.

State Bank of India, World's Largest Centralized Core Processing Implementation:

The story began in 2000. With its growth curve heading northward, State Bank of India (SBI), the country's largest bank with the largest branch network, realized the need for a core banking solution. An expression of interest was invited in July 2000, and the actual implementation was started in August 2003 when the first branch of the bank was put on TCS' BαNCS core banking solution.

The planning stage lasted three years, while the BαNCS implementation took another five years (till July 2008) to complete. The entire project of implementing the core banking solution was handled by TCS as the systems integrator, while other major technology partners in the project were HP, Data craft, Cisco and Microsoft. The core banking solution implemented at SBI and its associate banks currently execute an average of 42 million transactions per day with a peak of 1,900 transactions per second through a massive network of about 17,700 branches and over 20,000 ATMs servicing nearly 243 million customers. The CBS at SBI executes an average of 42 million transactions per day with a peak of 1,900 transactions per second through a network of about 17,700 branches.

Further, SBI had more than 2 lac employees, and many of them had little familiarity with Web-based technology before the core banking solution's implementation. "SBI and TCS had to ensure that the bank employees were well-acquainted with the use of the solution, Indeed, at one point of time, SBI had 58 training centers.

3.1. ATM BANKING:

Full-service banking, 24 hours a day

Make banking more convenient with ATMs and debit card.

- **Convenient Self Service**
  - Deposits – Cash and check deposits can be made at most BBVA Compass ATMs.
  - Withdraw Funds – The cash you need when you need it. *
  - Transfer funds – Move funds between checking accounts and savings accounts that are linked to your debit card.
- **Account Management**
  - Check Balance – View your account balance before you make a withdrawal.
  - Mini Statement – Receive a print out of your transaction history and account balances. *
- **Customizable**
  - Fast Cash – Set standard ATM withdrawal amounts.
  - Receipt Options – Set whether or not you will receive a receipt when you make transactions.
  - Preferred Language – Choose between English or Spanish.

CREDIT vs. DEBIT

Debit Cards vs. Credit Cards

	Debit Cards	Credit Cards
Payments	Buy now, **pay now.**	Buy now, **pay later.**
Interest Charges	**No charges apply** as funds are automatically debited from your checking account.	**Charges will apply** if you carry a balance or your card offers no grace period (time to repay without incurring interest charges).
Fees	• **Fees** on certain transactions (e.g., an ATM fee charged for withdrawing funds from an ATM not operated by the financial institution that issued your card). • Potentially costly fees if you try to spend more money than you have available in your account.	• **Fees and penalties** can be imposed if payments are not timely. • **Some cards also have annual fees.** • **Not all cards offer grace periods** (time to repay without incurring interest charges).
Other Potential Benefits	• **Easier and faster** than writing a check. • **No risk** of losing cash that you cannot replace. • Some cards may offer **freebies or rebates.** • As long as you do not overdraw your account, debit cards are a good way to pay for purchases without borrowing money and paying interest.	• **Freebies** sometimes offered (e.g., cash rebates, bonus points, or travel deals). • You can **withhold payment** on charges in dispute. • **Purchase protections** offered by some cards for faulty goods. • If you are careful about how you manage your credit card, especially by paying your bill on time, **your credit score may go up** and you may qualify for lower interest rates on loans.
Other Potential Concerns	• Usually there are **no protections** against faulty goods and services. • You need another way to pay for unexpected emergencies (e.g., a car repair) if you do not have enough money in your bank accounts.	• **Over-spending** can occur, since the credit limit may be higher than you can afford. • If you do not pay your card balance in full each month, or your card does not have an interest-free grace period, **you will pay interest.** This can be costly, especially if you only pay at or near the minimum amount due each month.

DIGITAL WALLET:

Nowadays, we find ourselves carrying cold hard cash less and less because you can just as easily make your purchase with payment cards, and track your spending online. Plus, it's **more secure** than carrying $350 to buy the latest iPad (MINI). Certain payment or loyalty cards also let you **earn rewards** or **entries to contests**, but they do add up. They make your wallet unnecessarily thick and heavy. Perhaps it is time to swap the system again; this time, for something that you have always been carrying around: your smartphone

Digital wallets can help take you there. They are smartphone apps that hold your payment and loyalty card information. **Google Wallet** and **Apple's Passbook** are two of the more popular ones we often hear about, but if they are not your fancy, **there are plenty of other digital wallets that carry perks and benefits** that you may prefer.

1. Google Wallet

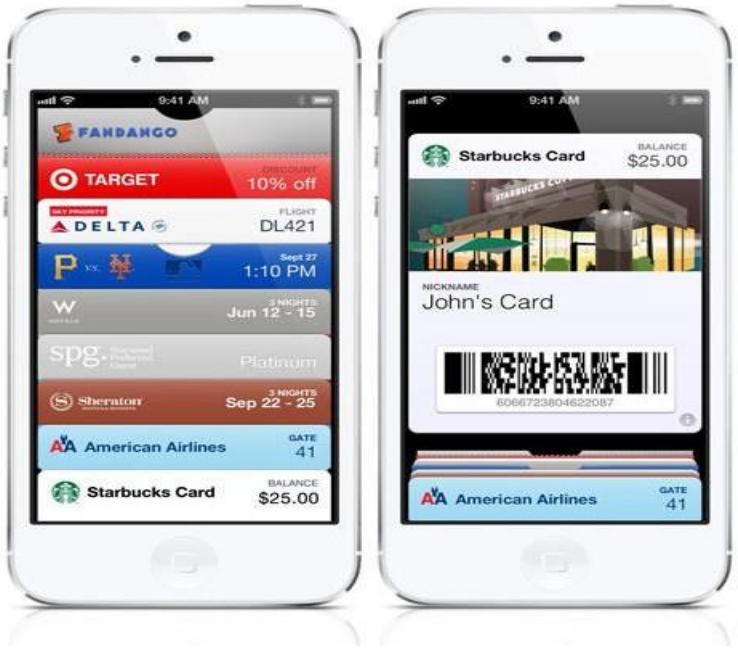
Instead of tapping your credit card on the NFC machine at the checkout counter, all you have to do is **wave your smartphone** or tap it on the machine to make your payments. It'll be able to identify the credit card information linked on your Google account. For this to work, Google Wallet requires **Near Field Communication (NFC) technology** available, which unfortunately is only available on certain smartphones and tablets.

You **link your debit or credit card** to your Google account and you can leave your wallet at home – but at the moment, it only works with phones and credit cards from the US and **only in the US**. Currently, it supports 20+ merchants on the ground and online, promising more merchants to come.

2. Apple's Passbook

Apple's Passbook was introduced in iOS 6 and relies on scanning 2D barcodes to help you manage your movie, concert and airline tickets as well as **loyalty cards and coupons** for selected merchants.

The result: you get **location and time-based notifications** when you're near a cafe where you can use your loyalty card or when your airline, movie or concert ticket is nearing its due date.

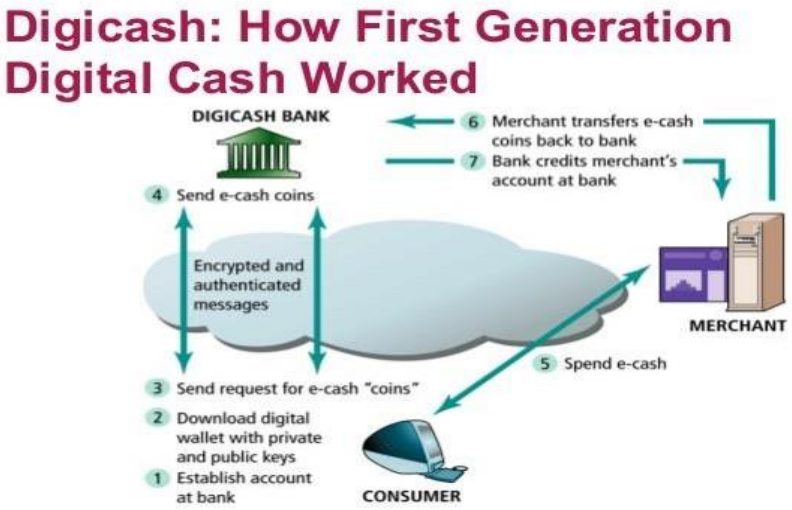


You add passes through apps that support Passbook (link opens iTunes). So instead of bringing your grocery coupons and stack of loyalty cards wherever you go, you can store it in Passbook. Unlike Google Wallet, you cannot use your debit or credit card for purchases in-store, however you can use Bill Guard to **view your bank balance** and other related information on your iPhone.

DIGITAL CASH:

Digital Cash acts much like real cash, except that it's not on paper. Money in your bank account is converted to a digital code. This digital code may then be stored on a microchip, a pocket card (like a smart card), or on the hard drive of your computer.

The concept of privacy is the driving force behind digital cash. The user of digital cash is assured an anonymous transaction by any vendor who accepts it. Your special bank account code can be used over the internet or at any participating merchant to purchase an item. Everybody involved in the transaction, from the bank to the user to the vendor, agree to recognize the worth of the transaction.



3.2. ***KIOSK BANKING:*** This is the latest development on the remote baking front, also known as 'Touch-screen' banking. A kiosk is a self- service banking terminal that can be operated with both credit & debit cards. The Debit/credit card can be swiped at against the card reader at the kiosk and account accessed post entering the ATM PIN. Currently, very few banks like Citibank offer this facility to their customers at select ATM centers across the country.

3.3. NEFT:

National Electronic Funds Transfer (NEFT) NEFT is electronic funds transfer system, which facilitates transfer of funds to other bank accounts in over 63000 bank branches across the country. This is a simple, secure, safe, fastest and cost-effective way to transfer funds especially for Retail remittances.

FEATURES & BENEFITS

Customers can remit any amount using NEFT Customer intending to remit money through NEFT has to furnish the following particulars:

- IFSC (Indian Financial System Code) of the beneficiary Bank/Branch
- Full account number of the beneficiary
- Name of the beneficiary.

The facility is also available through online mode for all internet banking and mobile banking customers.

For corporate customers, bulk upload facility is also available at branches

TIMINGS

Customers can use this facility between 8 AM and 7 PM on all weekdays and between 8 AM and 1 PM on Saturday. There are twelve hourly settlements between 8 AM and 7 PM on all weekdays and six hourly settlements between 8 AM and 1 PM on Saturdays.

The money will be credited to the beneficiary's account on the same day or at the most next day in case the message is sent during the last batch of settlement. Union Bank offers NEFT facility to its customers through all its branches.

CHARGES

Rs. 5/ per transaction if the transaction amount is less than Rs. 1 lakh

Rs. 25/- per transaction if the transaction amount is more than Rs. 1 lakh

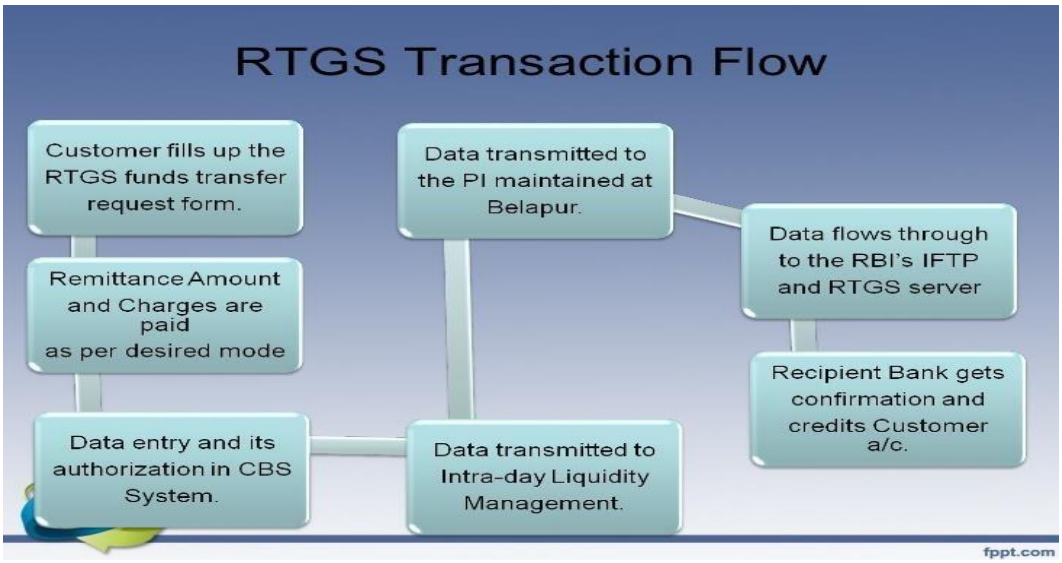
NOTE: Charges are waived for customers availing services at our branches in North Eastern States

3.4. RTGS:

Real Time Gross Settlement (RTGS) is an electronic form of funds transfer where the ransmissions akes place on a real time basis.

In India, transfer of funds with RTGS is done for high value transactions, the minimum amount being Rs 2 lakh. The beneficiary account receives the funds transferred, on a real time basis. The main difference between RTGS and National Electronic Funds Transfer (NEFT) is that while transfer via NEFT takes place in batches (with settlements and transactions being netted off), in the case of RTGS, the transactions are executed individually and on gross basis.

The customer initiating the funds transfer through RTGS has to have the Indian Financial System Code (IFSC) of the beneficiary's bank, along with the name of the beneficiary, account number and name of the bank. The bank branches, both at the initiating and receiving end, have to be RTGS- enabled for the transaction to be processed. Customers with Internet banking accounts can do RTGS transactions on their own.



IMPS:

Using IMPS, a relatively newer service, users can transfer money immediately from one account to the other account, within the same bank or accounts across other banks. Similar to NEFT, there is no minimum amount for transactions, but the maximum* amount possible is Rs 5 lakhs.Users can carry out Person to Person (P2P), Person to Account (P2A) and Person to Merchant (P2M) transactions from their mobile, Internet or ATM. One of the advantages of IMPS transaction is that it is available 24X7 and even on holidays. This can be payments for utility bills, mobile or DTH recharge, credit card bills, grocery bills, travel ticketing, online shopping and even educational institutes fee payments through this channel.

Transaction Timings	NEFT	RTGS	IMPS
Monday to Friday	8:00 AM to 6:30 PM	9:15 AM to 4:15 PM	24x7
Saturdays	8:00 AM to 12:30 PM	9:15 AM to 1:45 PM	24x7
Transaction Limits	**NEFT**	**RTGS**	**IMPS**
Minimum	No limit	Rs 2 lacs	No limit
Maximum	Rs 5 lacs	Rs 5 lacs	Rs 5 lacs

3.10. SMART CARD/STORE VALUE CARD:

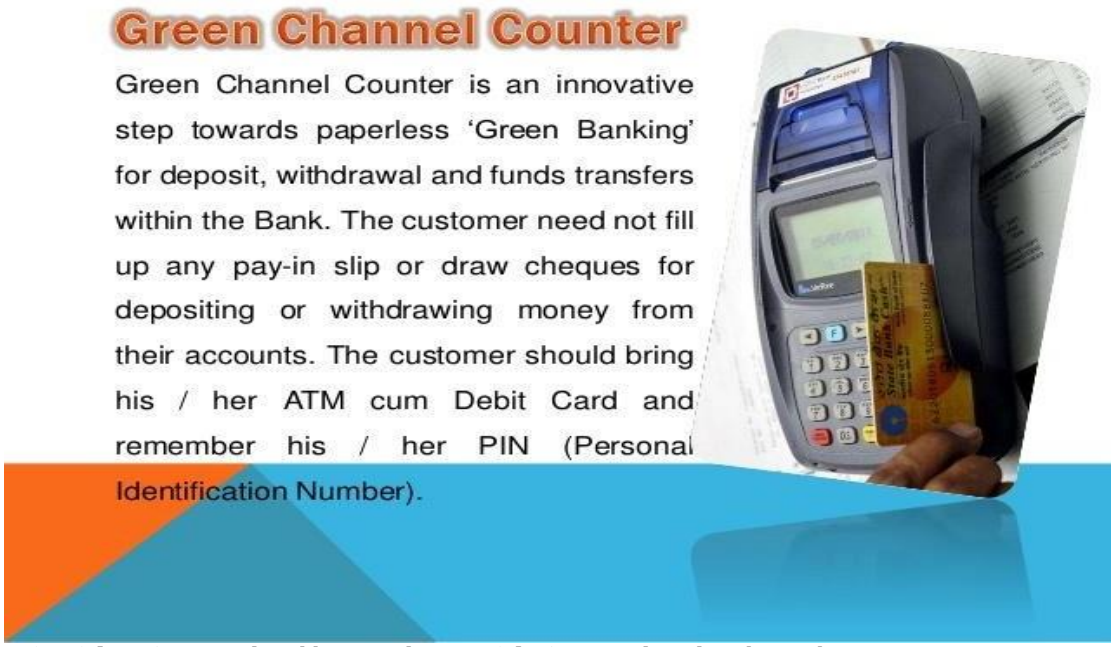
A smart card, typically a type of chip card, is a plastic card that contains an embedded computer chip–either a memory or **micro-processor** type–that stores and transacts data. This data is usually associated with either value, information, or

both and is stored and processed within the card's chip. The card data is transacted via a reader that is part of a computing system. Systems that are enhanced with smart cards are in use today throughout several key applications, including healthcare, banking, entertainment, and transportation. All applications can benefit from the added features and security that smart cards provide. According to Euro smart, worldwide smart card shipments will grow 10% in 2010 to 5.455 billion cards. Markets that have been traditionally served by other machine-readable card technologies, such as barcode and magnetic stripe, are converting to smart cards as the calculated return on investment is revisited by each card issuer year after year.

3.11. GREEN CHANNEL COUNTER:

E-TICKETING:

An



electronic ticket (commonly abbreviated as **e-ticket**) is a digital ticket. The term is most commonly associated with airline issued tickets. Electronic ticketing for urban or rail

public transport is usually referred to as travel card or transit pass. It is also used in ticketing in the entertainment industry.

An electronic ticket system is a more efficient method of ticket entry, processing and marketing for companies in the railways, flight and other transport and entertainment industries.

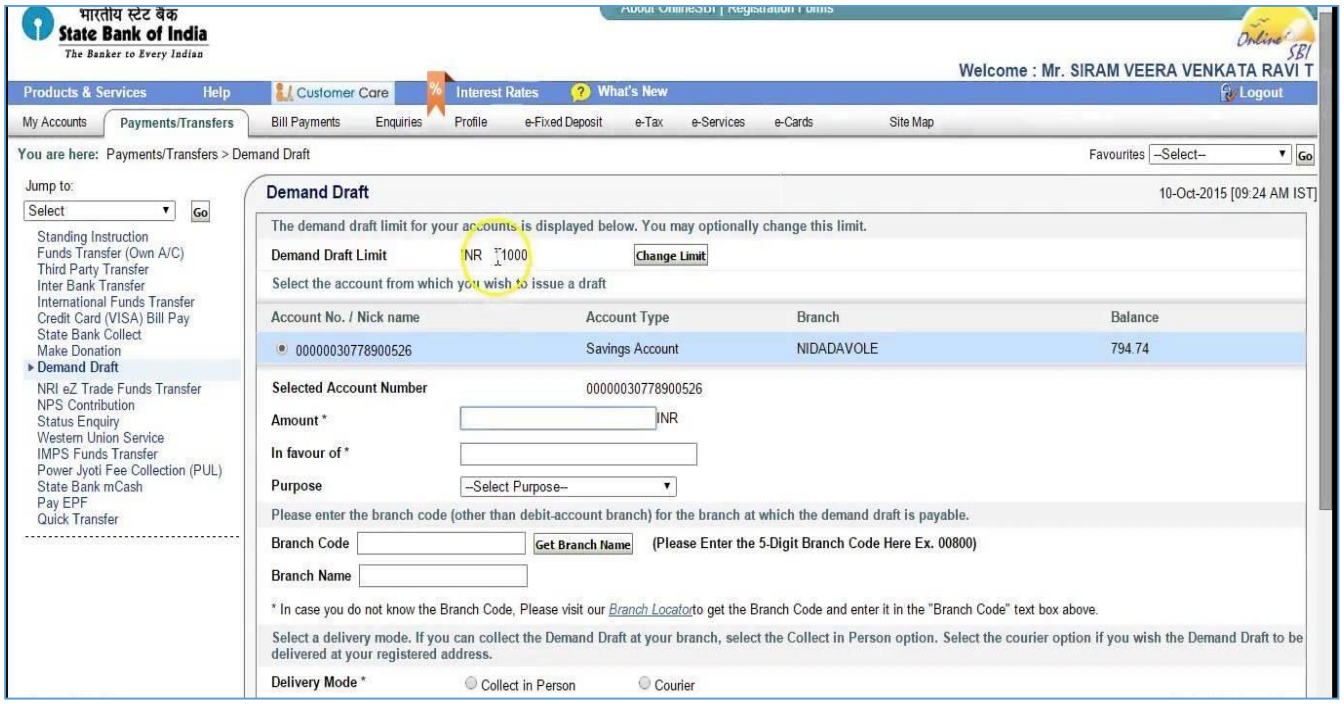
On 1 June 2008, the industry moved to 100% electronic ticketing and the paper ticket became a thing of the past. Apart from substantial cost savings for the industry of up to US$3bilion per year, ET is also more convenient for passengers who no longer have to worry about losing tickets and can make changes to itineraries more easily.

United Airlines was the first airline to issue electronic tickets, back in 1994. A decade later however, only 20% of all airline tickets were electronic. The industry was missing out on an opportunity to save costs and make travel for passengers easier. In June 2004, IATA set an industry target of 100% ET in four years. At the time, many believed this was an unrealistic goal. Evolving standards, uncertainty about the return on investment and skepticism about the customer acceptance of paper in parts of the world were some of the reasons why e-ticketing hadn't taken off.

3.12. ONLINE DEMAND DRAFT:

A **demand draft** is a negotiable instrument similar to a bill of exchange. A bank issues a demand draft to a client (drawer), directing another bank (drawee) or one of its own branches to pay a certain sum to the specified party (payee).

A demand draft can also be compared to a cheque. However, demand drafts are difficult to countermand. Demand drafts can only be made payable to a specified party, also known as pay to order. But cheques can also be made payable to the bearer. Demand drafts are orders of payment by a bank to another bank, whereas cheques are orders of payment from an account holder to the bank.



CHAPTER-4

SECURITY ISSUES OF NET BANKING

5.1. INTRODUCTION:

The Internet has made banking, shopping, and conducting other financial transactions online quite convenient. But when it comes to your money, you want to make sure your transactions are safe.

Security of a customer's financial information is very important, without which online banking could not operate.

Presently, Internet banking customers only need a computer with access to the Internet to use Internet banking services. Customers can access their banking accounts from anywhere in the world. Each customer is provided a login ID and a password to access the service. It is indeed easy and convenient for customers.

However, the use of password does not provide adequate protection against Internet fraud such as phishing. The problem with password is

that when it has been compromised, the fraudsters can easily take full control of online transactions. In such cases, the password is no longer works as an authentication token because we cannot be sure who is behind the keyboard typing that password in.

However, easy access and convenience should not be at the expense and mercy of the security of information. This is important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by the fraudsters.

In this lesson, we will review strategies you should employ when dealing with money and the Internet. You will learn how to make sure a **website is secure**, including checking the **SSL certificate**. In addition, you'll learn the steps you need to take to make **shopping online** a safe and enjoyable experience.

5.2. TYPES OF FRAUDS:

Nowadays, the nature of attacks is more active rather than passive. Previously, the threats were all passive such as password guessing, dumpster diving and shoulder surfing. Here are some of the techniques used by the attackers today:

- **Trojan Attack.** The attacker installed a Trojan, such as key logger program, on a user's computer. This happens when users visited certain websites and downloaded programs. As they are doing this, key logger program is also installed on their computer without their knowledge. When users log into their bank's website, the information keyed in during that session will be captured and sent to the attacker. Here, the attacker uses the Trojan as an agent to piggyback information from the user's computer to his backyard and make any fraudulent transactions whenever he wants.

- **Man-in-the-Middle Attack.** Here, the attacker creates a fake website and catches the attention of users to that website. Normally, the attacker was able to trick the users by disguising

their identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website, users do not realize that they actually go to the fraudster's website. The information keyed in during that session will be captured and the fraudsters can make their own transactions at the same time.

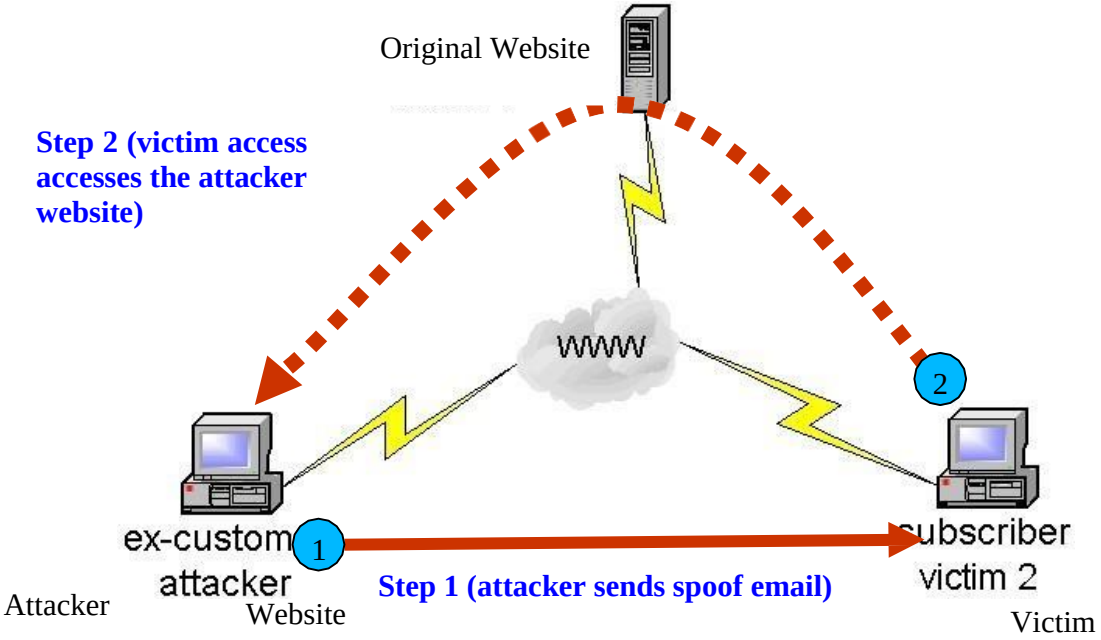


Diagram on how information is being compromised

- **Phishing**. One of the primary methods a hacker gains access to account information is through phishing, or tricking the victim into giving up the information voluntarily. A hacker might send an e-mail or even call, pretending to be a representative of the bank and informing you about some irregularities with your account. All you need to do to sort things out is to provide your password or other account information to verify your identity. If you ever receive a communication that appears to be from your bank and requests this type of information, contact your bank by phone immediately. Do not give out account information to a caller, and do not click any links provided in any e-mails that claim to be from your bank. You should also ensure that any employees with access to the company's accounts follow the same procedures.

- **Keyloggers.** Keyloggers are malware programs that record keystrokes and other data, allowing a hacker to capture your password as you enter it. Maintaining up-to-date antivirus suites on your company computers can prevent these malicious programs from gaining a foothold, and setting up your network's firewall to monitor outgoing traffic can help you determine when an nfection occurs. man ivebloggers and viruses use email to travel from computer to computer, so adding anti-virus protection to your company's email server can help filter out these attacks.
- **Spyware**. Spyware is the number one way that online banking credentials are stolen

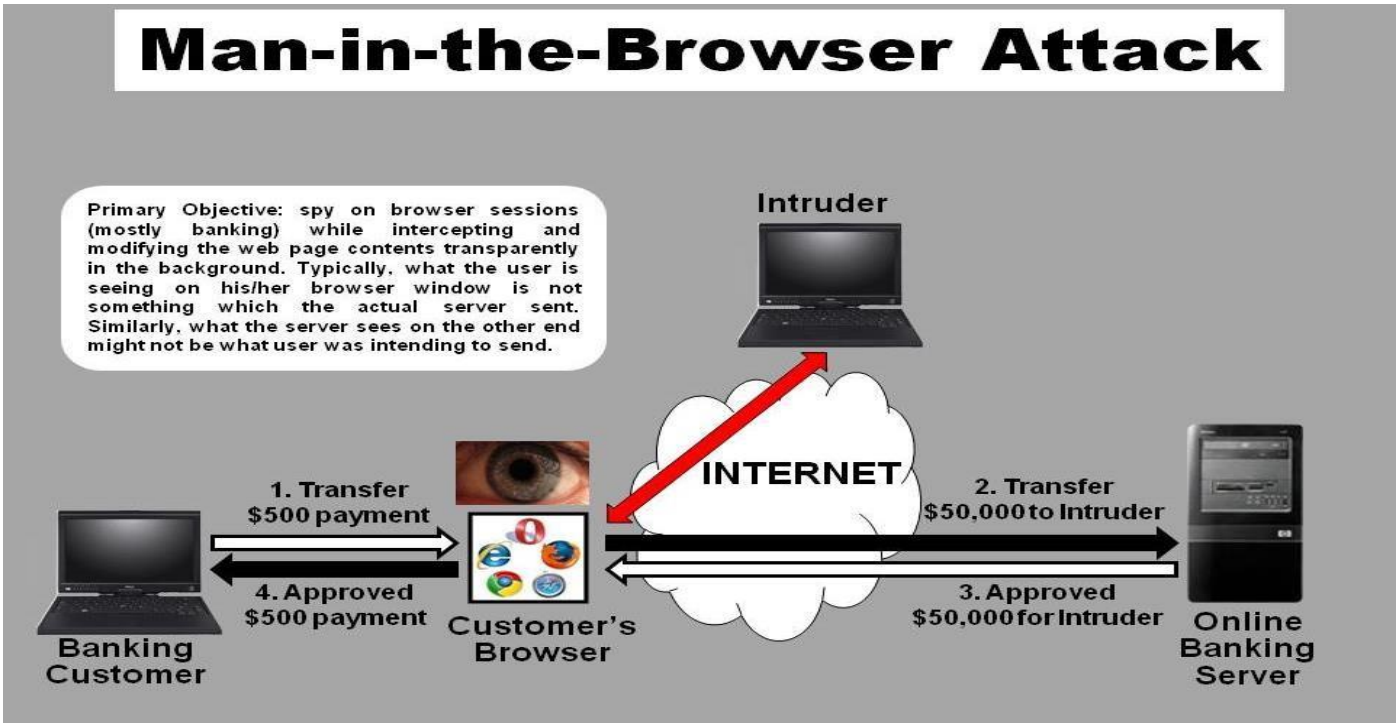
and used for fraudulent activities. Spyware works by capturing information either on your computer, or while it is transmitted between your computer and websites. Often times, it is installed through fake "pop up ads asking you to download software.

Industry standard Antivirus products detect and remove software of this type, usually by blocking the download and installation before it can infect your computer.

- **VIRUSES**. Viruses are designed to compromise your computer systems, and allow others to gain access to your files, etc. This is different than spyware in that a virus may search for information considered to be of value, where spyware will wait for input or action from whomever is using the computer. A system that is compromised may be used to attack other systems, denying people legitimate access to services. An example would be the recent activities of the group called

  "Anonymous." This group took over computer systems around the world, and used them to launch attacks on websites. These types of attacks are called "denial of service" attacks.

- **Hacking.** Hacking works similarly to viruses. A "hacker" uses software to probe for vulnerabilities, and then uses programming techniques, software utilities, or system commands to exploit the vulnerability. The primary objective is to gain access to your system. Once this access is obtained, you can think of it like a burglary – they search for anything of value and often times leave damage behind. More threatening are those hackers who simply take control of your system and wait, to see what information becomes available or what other systems they can gain access to.



- **Identity Theft** – Identity theft refers to all types of crime in which someone illicitly obtains and uses another person's personal data through deception or fraud, typically for monetary gain. With enough personal information about an individual, a criminal can assume that individual's identity to carry out a wide range of crimes. Identity theft occurs through a wide range of methods—from very low-tech means, such as check forgery and mail theft to more high-tech schemes, such as computer spyware and social

network data mining. The following table[1] illustrates well-known social Web sites that have been attacked.

- **Spam:** Spam is an electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.
- **Nigerian Scam:** Nigerian or Frauds 409 or 419 are basically the lottery scam in which some overseas persons are involved to cheat innocent persons or organizations by promising to give a good amount of money at nominal fee charges. Their intention is to steal money in the form of fee against the lottery prize.

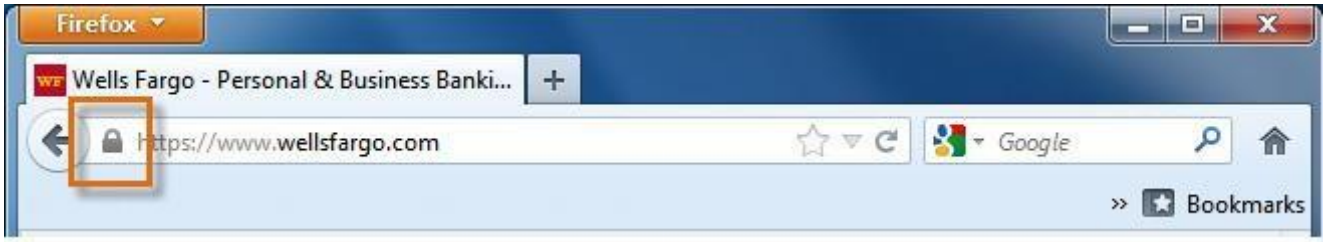
5.3. STEPS TO SECURE ONLINE BANKING:

5.3.1. When is a website secure for financial transactions?

Before sending any sensitive or financial information online, you want to know that you are communicating with a **secure site**. Secure sites make sure all information you send is **encrypted**—or protected—as it travels across the Web. The **https** address heading and your browser's **security symbol** are two signs indicating you are on a secure site.

- Web addresses either begin with **http** or **https**. If the address is **https**, the information you send to it is **encrypted** and will look like gibberish if intercepted by cybercriminals.

Your browser will use a **security symbol** or **lock** to indicate that the **browser verifies** that the website is a **secure site**. As seen in the examples below, the look of each browser's symbol can be slightly different, and it is usually located in the address bar.



5.3.2. Security alerts and the SSL certificate

Secure sites have an **SSL certificate**. An **SSL certificate does two things**. First, it acts like a **virtual passport** or **driver's license**. It means, **I am who I say I am**. Second, it

enables **encryption**. If a site does not have an SSL certificate, the address will begin with http instead of https, and your browser will not show a lock symbol. If it has an SSL certificate, you can **access it by clicking your browser's lock**.

CHAPTER-5

1.1.1.1 ONLINE BANKING IN INDIA-GUIDELINES BY RBI

6.1. Guidelines by RBI on Internet Banking facility to Customers of Regional Rural banks (RRBs):

6.1.1. Technology and Security Standards:

a. RRBs should have appropriate Information Security policy duly approved by the Board of Directors. There should be clear segregation of duties between the Information Technology (IT) Division and the Information Security (IS) Division. The Information Technology Division will actually implement the computer systems. There should be a separate Information Security Officer dealing exclusively with Information Systems security. Further, an Information Systems Auditor will audit the Information Systems.

b. The bank should designate a Network and Database Administrator with clearly defined roles as per the IS Audit policy duly approved by their Board.

c. Logical access controls to data, Systems, Application software, utilities, telecommunication lines, libraries, System software, etc. should be in place.

d. The bank should ensure that there is no direct connection between the Internet and the bank's system.

e. All unnecessary services on the Application Server such as File Transfer Protocol (FTP), Telnet should be disabled. The Application Server should be isolated from the e-mail server.

f. The Information Security officer and the Information System auditor should conduct periodic penetration tests of the system, which should include:

1. Attempting to guess passwords using password-cracking tools.
2. Search for back door traps in the programs.
3. Attempt to overload the System using Distributed Denial of Service (DDoS) & Denial of Service (DoS) attacks.

4. Check if commonly known holes in the software, especially the browser and the email software exist.
5. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers').

g. Physical access controls should be strictly enforced. Physical security should cover all the Information Systems and sites where they are housed, both against internal and external threats.

h. The bank should have proper infrastructure and schedules for backing up data.

i. Security infrastructure should be properly tested before using the Systems and Applications for normal operations. Banks should periodically upgrade the Systems to newer versions which give better security and control.

6.1.2. Legal Issues:

a. Banks may provide Internet Banking facility to a customer only at his/her option based on specific written or authenticated electronic requisition along with a positive acknowledgement.
b. Considering the prevailing legal position, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about the integrity and reputation of the customer opting for internet banking. Therefore, even though request for opening an account may be accepted over Internet, accounts should be opened only after verification of the identity of the customer and adherence to **KYC** guidelines.

6.2. Authentication practices for internet banking:

Single Factor Authentication:

An authentication mechanism that utilizes any one of the factors is called single factor authentication. This is the basic authentication method. (For example, a User id and password comes under this category).

Two Factor Authentication:

An authentication mechanism that utilizes a combination of two factors i.e. (User knows, User possesses). This method is used by various banks for authentication for online banking.

E.g. User using a password as the first factor (User knows) and a One-Time Password (OTP) as the second factor (User possesses) to perform say, a funds transfer transaction.

Multi Factor Authentication:

An authentication mechanism where two or more factors are used in which one of the factors is necessarily pertaining to 'the user is'.

(For example, a large value transaction authorized in a bank by using a combination of the person's user id, a smart card and his biometric authentication factor).

6.2.1. Implementation of authentication and other security measures for internet banking:

a. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems.

b. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer.

c. Changes in mobile phone number may be done through request from a branch only.

d. Virtual keyboard should be implemented.

e. Customers should be advised to adopt various good security precautions and practices in protecting their personal computer and to avoid conducting financial transactions from public or internet café computers.

f. Risk-based transaction monitoring or surveillance process needs to be considered as an adjunct.

g. An online session would need to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained.

h. As an integral part of the two-factor authentication architecture, banks should also implement appropriate measures to minimize exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack.

(i) **Specific OTPs for adding new payees**: Each new payee should be authorized by the customer based on an OTP from a second channel which also shows payee details or the customer's handwritten signature from a manual procedure which is verified by the bank.

(ii) **Individual OTPs for value transactions (payments and fund transfers)**: Each value transaction or an approved list of value transactions above a certain monetary threshold determined by the customer should require a new OTP.

(iii) **OTP time window:** It is recommended that banks should not allow the OTP time window to exceed 100 seconds on either side of the server time since the smaller the time window, the lower the risk of OTP misuse.

(iv) **SSL server certificate warning:** Internet banking customers should be made aware of and shown how to react to SSL or EV-SSL certificate warning.

CHAPTER-7

A CASE STUDY ON ONLINE-BANKING

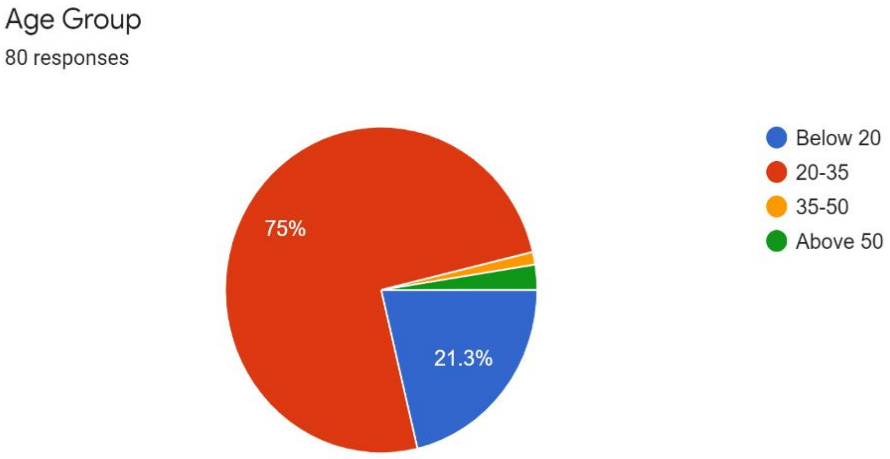
For case study a survey was conducted from FOR 1 MONTHS for the project "digital Banking services in Delhi NCR". This survey was done on the basis of 50 respondents from various sectors.

Mainly the objective of the research is to understand online banking users' behaviors, opinions, preferences and expectations. The questions were designed in such a way to cover all the relating fields. The fieldwork and data analysis were conducted by me after consulting with my supervisor and with the help of my friend. I am very much grateful to them.

Duration of survey	***1 MONTH***
Target population	***Local people of GHAZIABAD AND STUDENTS OF GU***
Survey method	***Direct interview, phone call and social media***
Effective response rate	***97% (77 OUT OF 80)***

7.1. DATA ANALYSIS AND INTERPRETATION:

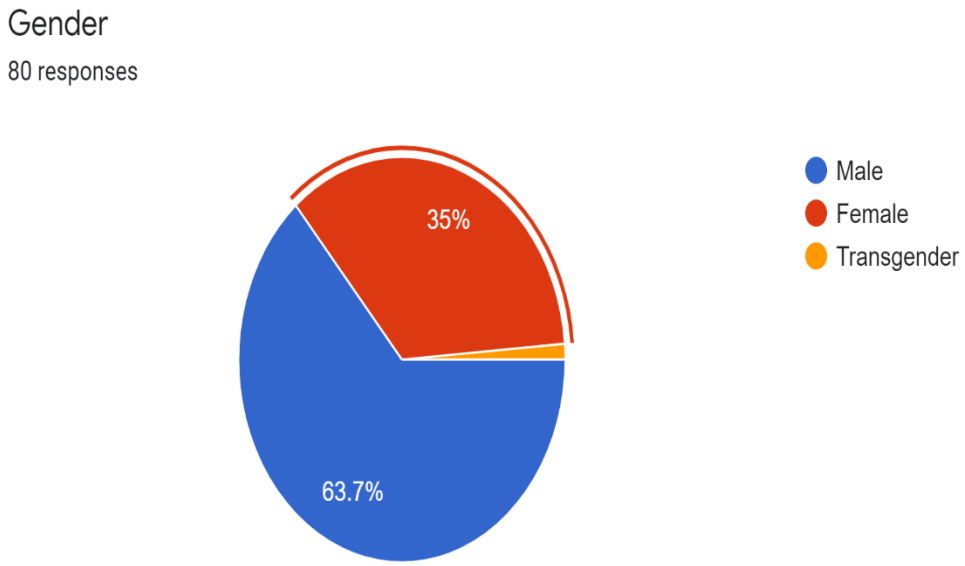
AGE GROUP ANALYSIS



PARTICULARS	*FREQUENCY*	*PERCENTAGE*
BELOW 20	17	21.3%
20-35	60	75%
35-50	1	1.2%
ABOVE 50	2	2.5%

INTERPRETATION: ***Out of 80 respondents 17 respondents are in below 20 age group, 60 respondents in 20-35 age group, 1 respondent in 35-50 age group and 2 respondents in above 50 age group. This shows with the help of a Pie-Chart.***

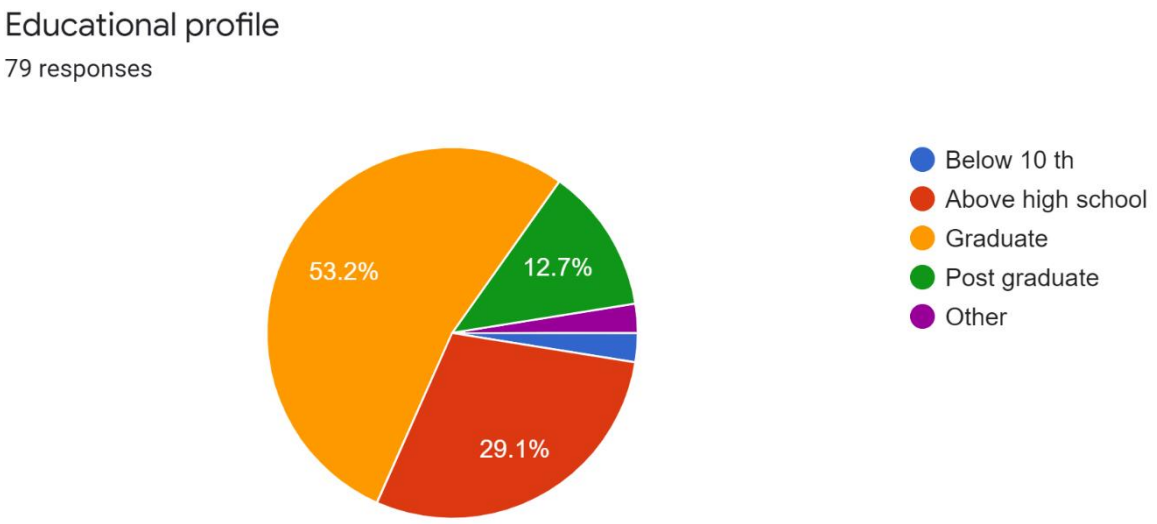
GENDER BASIS ANALYSIS:



GENDER	*FREQUENCY*	*PERCENTAGE*
MALE	*51*	*63.7%*
FEMALE	*28*	*35%*
TRANSGENDER	**1**	**1.2%**

INTERPRETATION: ***Data collected from 80 respondents, all respondents perform online banking and this is represented by a pie chart with male and female basis analysis. It is good for the banks as most of the respondents are aware of the internet banking and all the services have enjoyed them being offered by banks***

EDUCATIONAL PROFILE ANALYSIS:

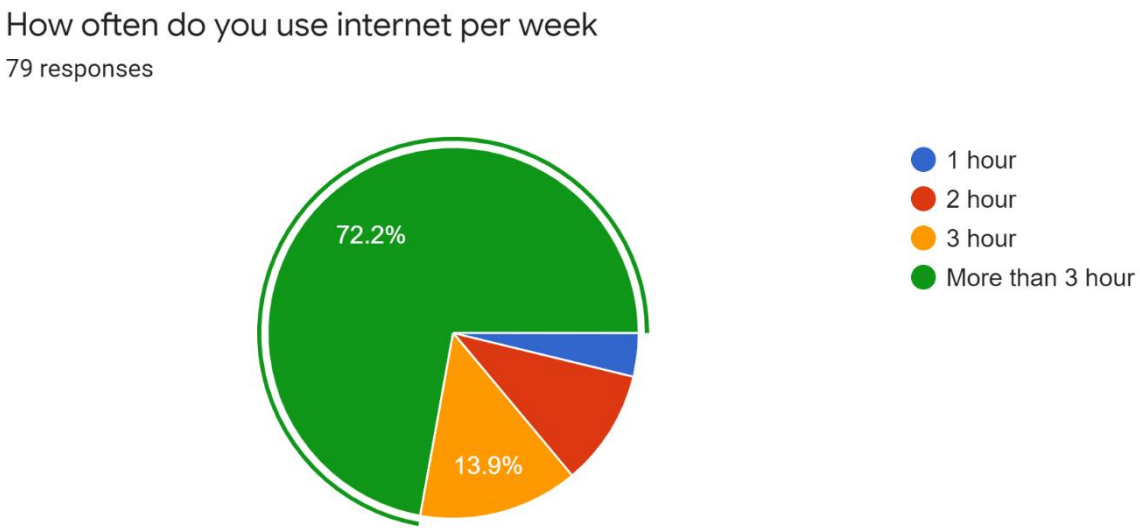


EDUCATION PROFILE	***FREQUENCY***	***PERCENTAGE***	***COMULATIVE FREQUENCY***
BELOW 10TH	2	2.5%	2
HIGH SCHOOL&ABOVE	23	29.1%	25
GRADUATE	42	53.2%	68
POST GRADUATE	10	12.7%	77
OTHER	2	2.5%	80

INTERPRETATION:

Among 80 respondents 2.5% are BELOW HS pass, HIGH SCHOOL&ABOVE ARE 29.1%, 53.2% are graduate, 12.7% are Post-Graduate and 2.5% are others.

INTERNET USES BASIS ANALYSIS:

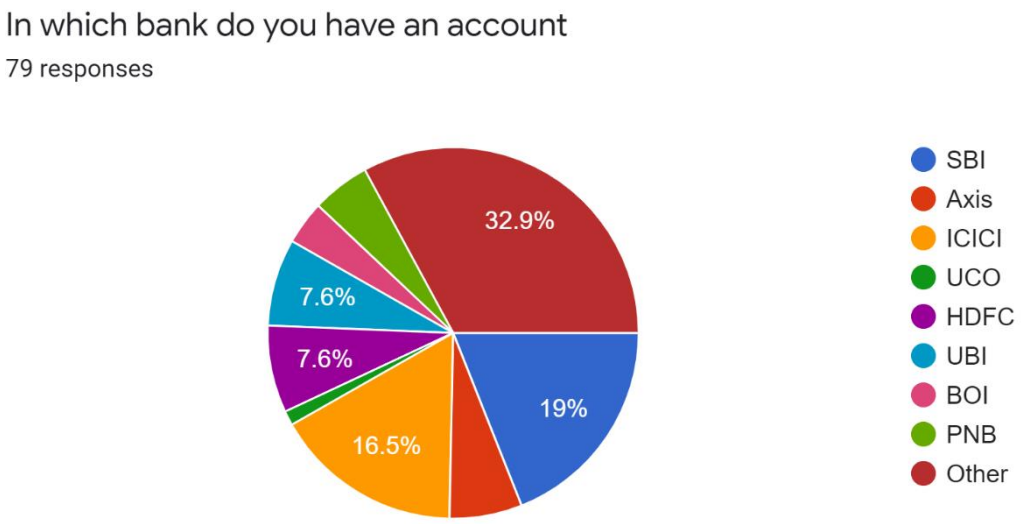


INTERNET USES	*FREQUENCY*	*PERCENTAGE*	*COMULATIVE FREQUENCY*
ONE HOUR	*3*	*3.8%*	*3*
TWO HOURS	*8*	*10.1%*	*12*
THREE HOURS	*11*	*13.9%*	*22*
MORE THAN THREE HOURS	*57*	*72.2%*	*80*

INTERPRETATION:

Among 79 respondents 72.2% use internet more than three hours per week, 13.9% use internet three hours per week, 10.1% use internet two hours per week and 3.8% use internet one hour in a week.

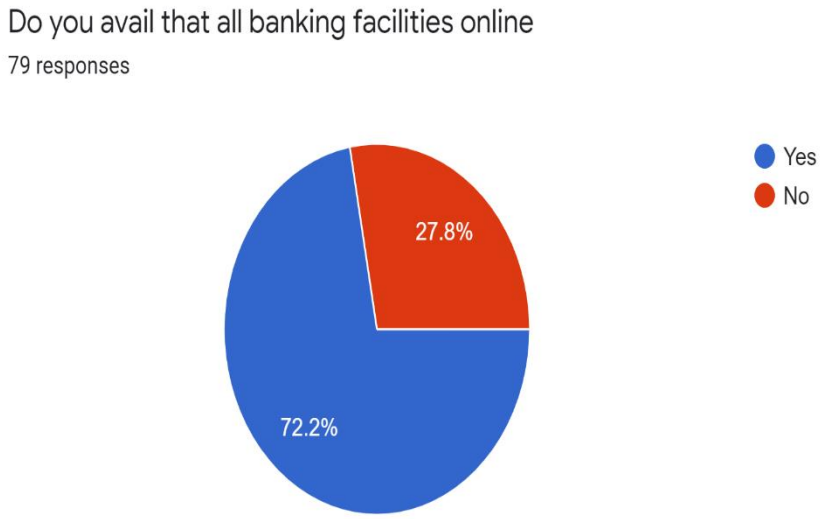
1. BANK ACCOUNT:



BANK ACCOUNT	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
SBI	*15*	*19%*	*15*
AXIS	*5*	*6.3%*	*20*
ICICI	*13*	*16.5%*	*33*
UCO	*4*	*5.1%*	*37*
HDFC	*6*	*7.6%*	*43*
UBI	*6*	*7.6%*	*49*
BOI	*3*	*3.8%*	*52*
PNB	*4*	*5.1%*	*56*
OTHER	*26*	*32.9%*	*79*

INTERPRETATION: Among 79 respondents, 15 respondents have SBI bank a/c, 5 have AXIS bank a/c, 13 have ICICI bank a/c, 4 have UCO bank a/c, 6 have HDFC bank a/c, 6 have UBI bank a/c, 3 have BOI bank a/c, 4 have PNB bank a/c, 26 have other' bank a/c.

2. DO YOU AVAIL OF ALL BANKING FACILITIES ONLINE?

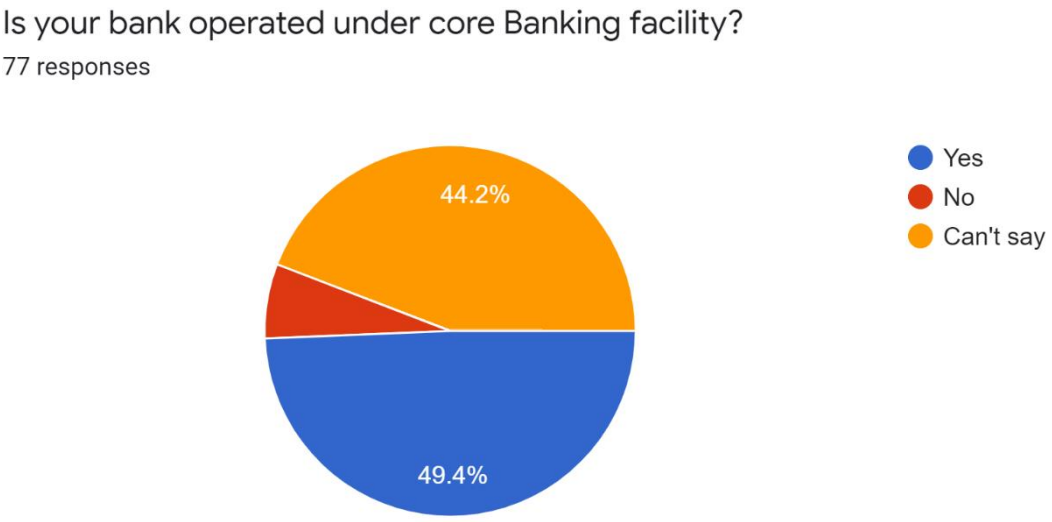


BANKING FACILITIES	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
YES	*57*	*72.2%*	*57*
NO	*22*	*27.8%*	*79*

INTERPRETATION:

Most of the respondents prefer online banking services. About 72.2% respondents support online banking services and only 27.8% respondent support offline banking services.

3. BANK OPERATED UNDER CORE BANKING FACILITY?

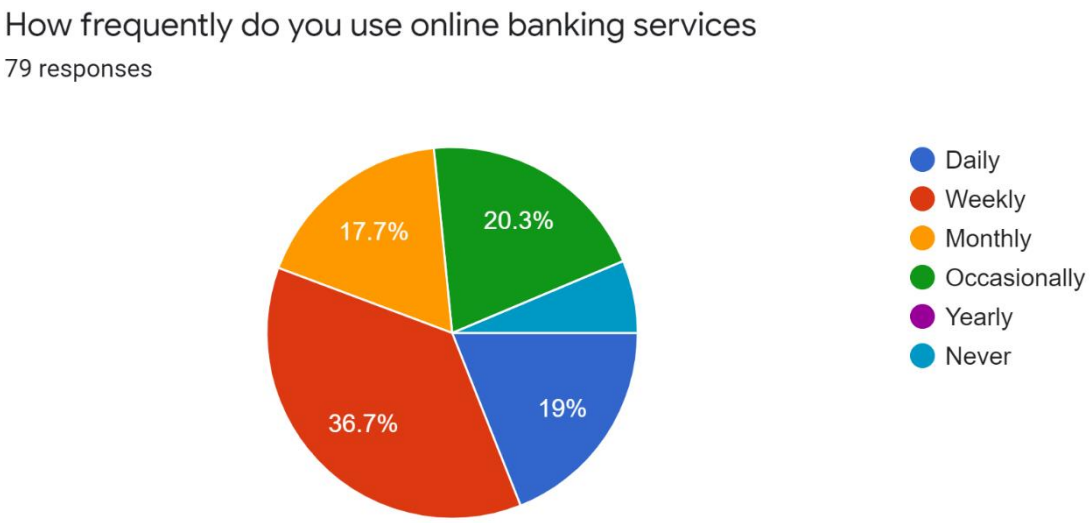


BANKING UNDER CORE BANKING	*FREQUENCY*	*PERCENTAGE*	*COMULATIVE FREQUENCY*
YES	*38*	*49.4%*	
NO	*5*	*6.5%*	
CAN'T SAY	*34*	*44.2%*	*77*

INTERPRETATION:

Among 100 respondents 49.4% say that their bank run under core banking system but 44.2% have no clear concept about this and they choose "CAN'T SAY" option.

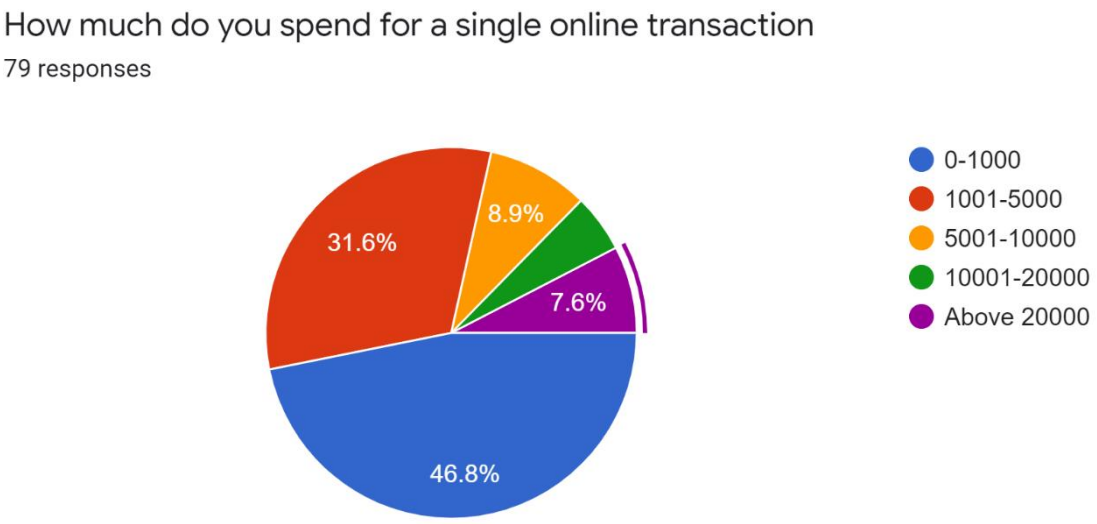
4. HOW FREQUENTLY DO YOU USE ONLINE BANKING FACILITIES?



ONLINE BANK SERVICES	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
DAILY	*15*	*19%*	*15*
WEEKLY	*29*	*36.7%*	*34*
MONTHLY	*14*	*17.7%*	*48*
OCASSIONALLY	*16*	*20.3%*	*74*
YEARLY	*0*	*0%*	*64*
NEVER	*5*	*6.3%*	*79*

INTERPRETATION:

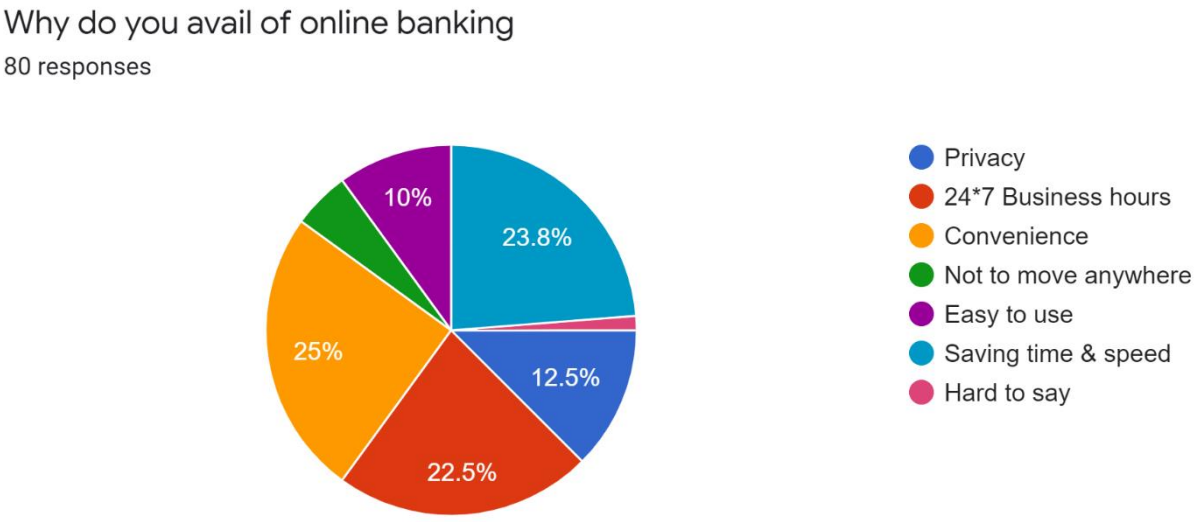
Most of the people do not need the services of banks regularly. They may transact with banks on occasionally basis, yearly or never. This chart shows the habits of people in case of use of online banking.



SINGLE ONLINE TRANSACTION	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
0-1000	*37*	*46.8%*	*37*
1000-5000	*25*	*31.6%*	*62*
5000-10000	*7*	*8.9%*	*69*
10000-20000	*4*	*5.1%*	*73*
ABOVE 20000	*6*	*7.6%*	*79*

INTERPRETATION:

Most of the online banking users have a tendency to spend Rs.1000 or below this amount in a single transaction.

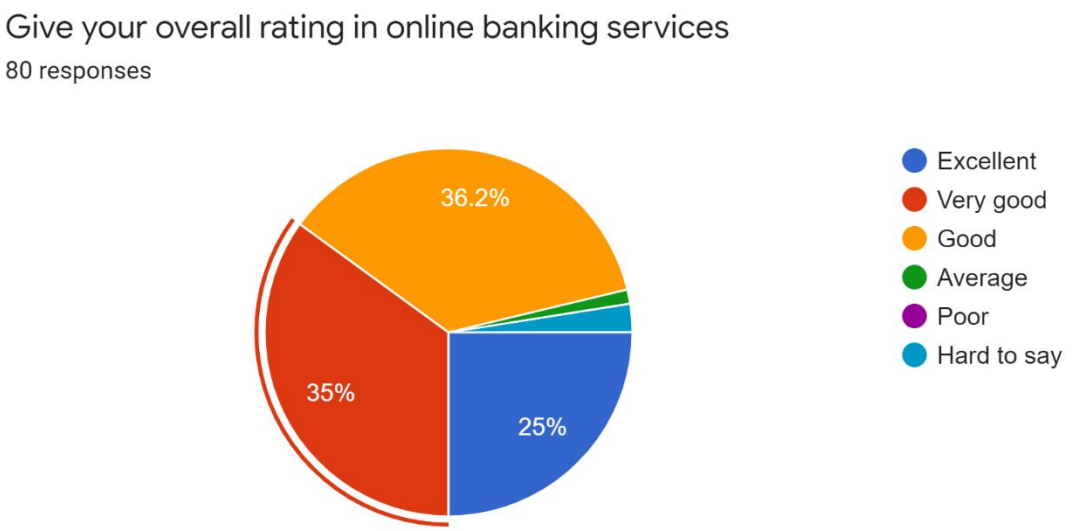


B

AVAIL OF ONLINE BANKING	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
PRIVACY	*10*	*12.5%*	*10*
*24*7*	*18*	*22.5%*	*28*
CONVENIENCE	*20*	*25%*	*48*
NOT TO MOVE ANYWHERE	*4*	*5%*	*52*
EASY TO USE	*8*	*10%*	*60*
SAVING TIMES & SPEED	*19*	*12.5%*	*79*
HARD TO SAY	*1*	*1.2%*	*80*
OTHERS	*0*	*0%*	*80*

INTERPRETATION:

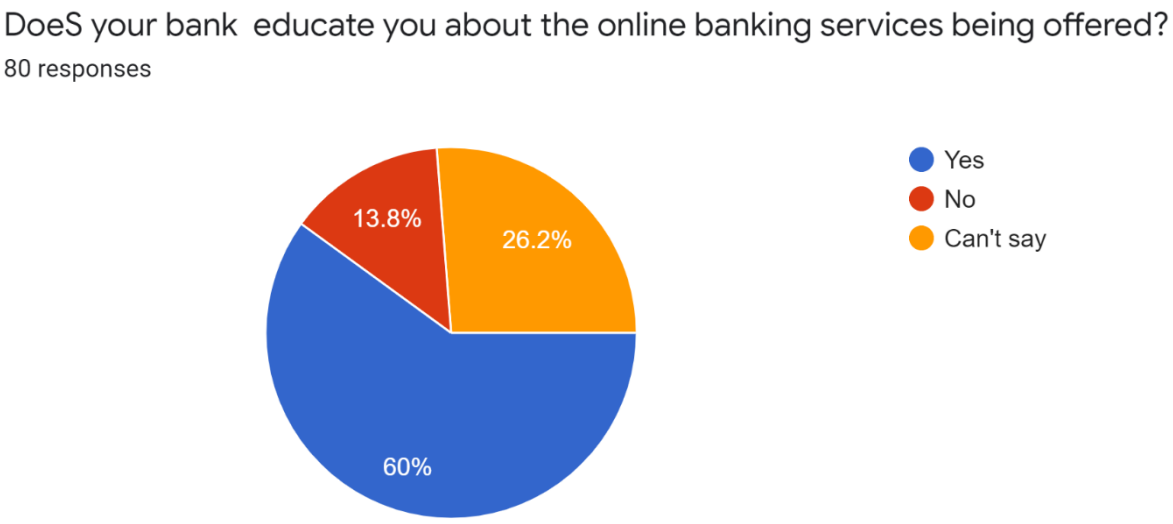
Most of the respondents felt that the "24*7 BUSINESS HOURS" provided by the internet banking is the highest motivating factor for an individual to use internet banking and rest prefer "PRIVACY"," CONVENIENCE", "NOT TO MOVE" etc.



Rating	*Frequency*	*Percentage*	*Cumulative Frequency*
EXCELLENT	*20*	*25%*	*20*
VERY GOOD	*28*	*35%*	*48*
GOOD	*29*	*36.2%*	*77*
AVERAGE	*1*	*1.2%*	*78*
POOR	*0*	*0%*	*78*
HARD SAY	*2*	*2.5%*	*80*

INTERPRETATION:

It is interesting to see that most of the respondents give "good" rating to ATM Banking, Balance Enquiry, Pay Fund Transfer, Online-Shopping and Online Recharge



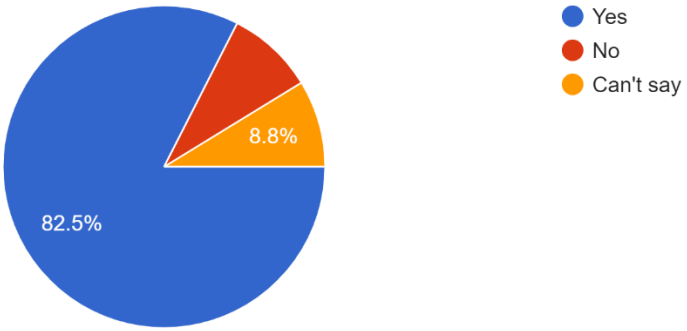
EDUCATE ABOUT ONLINE BANKING SERVICES	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
YES	***51***	***60%***	***51***
NO	***9***	***13.8%***	***60***
CAN'T SAY	***20***	***26.2%***	***80***

INTERPRETATION:

Among 80 respondents 51 people said that their bank educated them about the several online banking services and on the other hand 9 people said that their bank did not educate them about their net banking services.

Are you aware of the security threats and frauds in online banking and familiar with the method of secured online transaction?

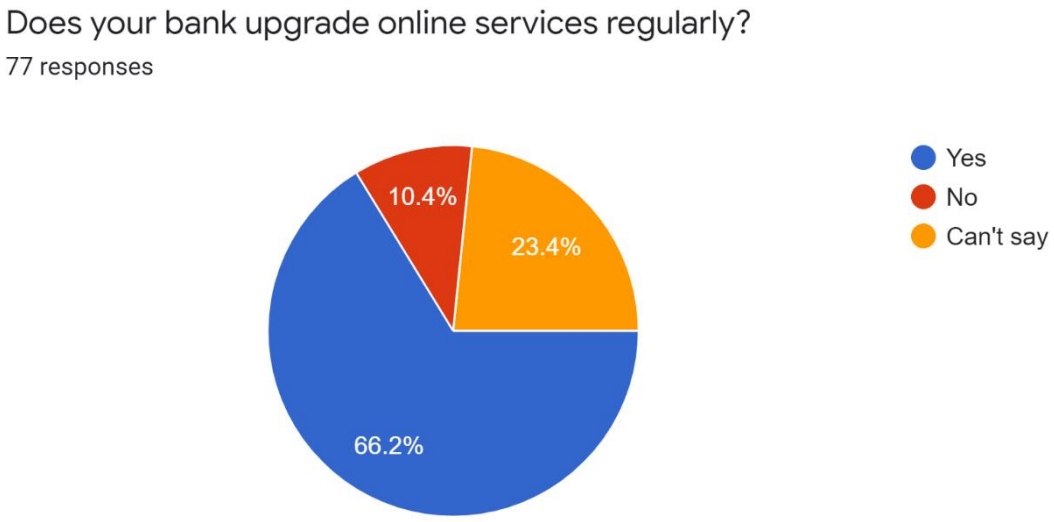
80 responses



SECURITIES & THREATS IN ONLINE BANKING	*FREQUENCY*	*PERCANTAGE*	*COMULATIVE FREQUENCY*
YES	*66*	*82.5%*	*66*
NO	*7*	*%*	*73*
CAN'T SAY	*7*	*8.8%*	*80*

INTERPRETATION:

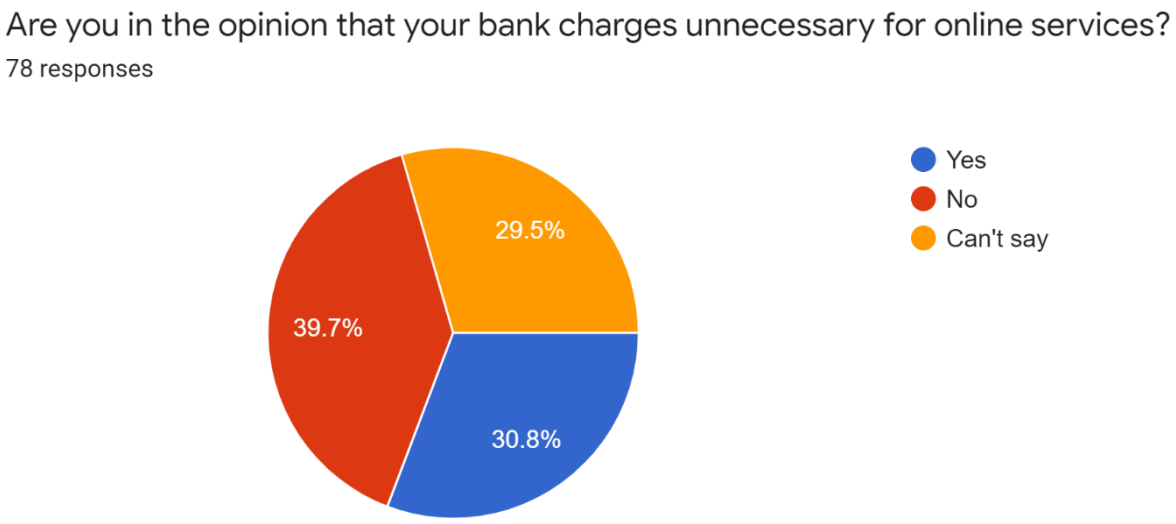
It is good to see that most of the users have knowledge about frauds and security issues of net banking but even with the increasingly knowledge of internet banking some respondents are unaware the methods taken up by the bank to secure each and every transaction.



UPDATE ONLINE SERVICES REGULARLY	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
YES	*51*	*66.2%*	*51*
NO	*8*	*10.4%*	**59**
CAN'T SAY	**18**	**23.4%**	**77**

INTERPRETATION:

This is very interesting to see that most of the online banking users think that their banks upgrade their services regularly. But some people did not think so and some few did not come to a conclusion.



5.

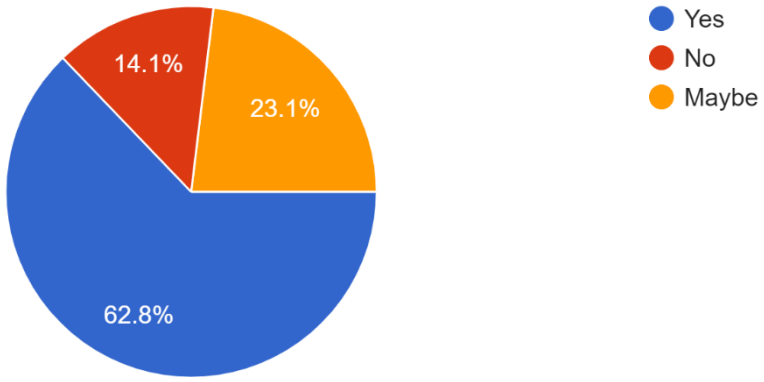
UNNECESSARY CHARGES BY BANK	***FREQUENCY***	***PERCENTAGE***	***CUMULATIVE FREQUENCY***
YES	***24***	***30.8%***	***24***
NO	***31***	***39.7%***	***55***
CAN'T SAY	***23***	***29.5%***	***78***

INTERPRETATION:

30.8% users think that their banks charge unnecessary for online services. While 39.7% people think that their banks don't do such and 29.5% people are unable to answer this question.

Do you think online banking is better substitute of traditional banking system

78 responses



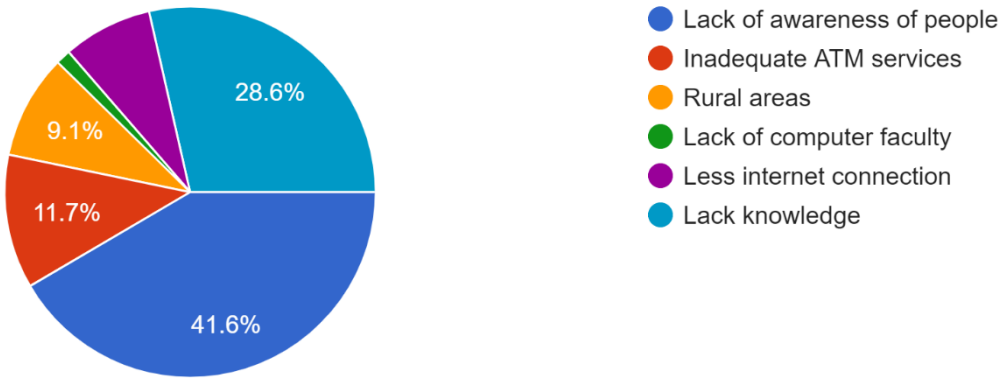
ONLINE BANKING BETTER SUBSTITUTE	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
YES	*49*	*62.8%*	*49*
NO	*11*	*14.1%*	*50*
MAY BE	*18*	*23.1%*	*78*

INTERPRETATION:

It was witnessed that most of the respondents preferred using Internet Banking over there traditional banking system. Thus, Internet Banking has a bright future ahead.

Which factor do you think responsible for non-accessebility of online banking by majority of people in your area?

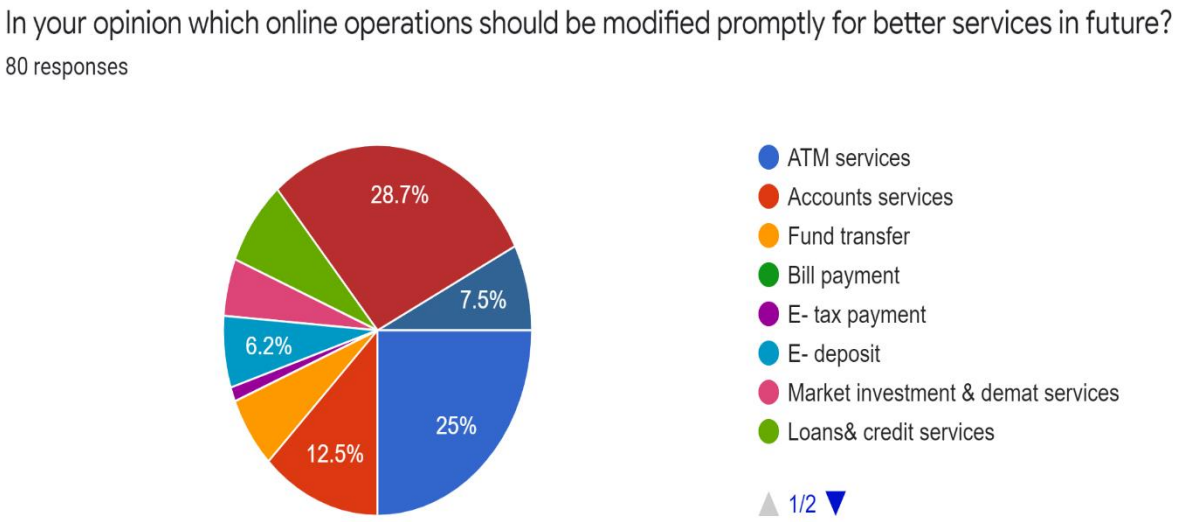
77 responses



FACTORS FOR NON-ACCESSEBILITY OF ONLINE BANKING	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
LACK OF AWARENESS OF PEOPLE	*32*	*41.6%*	*32*
INADEQUATE ATM SERVICES	*9*	*11.7%*	*41*
RURAL AREA	*7*	*9.1%*	*47*
LACK OF COMPUTER FACILITY	*1*	*1.3%*	*48*
LESS INTERNET CONNECTION	*6*	*7.8%*	*54*
LACK KNOWLEDGE	*22*	*28.6%*	*77*
OTHER	*0*	*0%*	*77*

INTERPRETATION:

Among 80 respondents 32 choose "LACK OF AWARNESS", 9 choose "INADEQUATE ATM SERVICE", 7 choose "RURAL AREA", 1 choose "LACK OF COMPUTER FACILITY", 6 choose LESS INTERNET CONNECTION" and 22choose "LACK OF KNOWLEDGE" option.



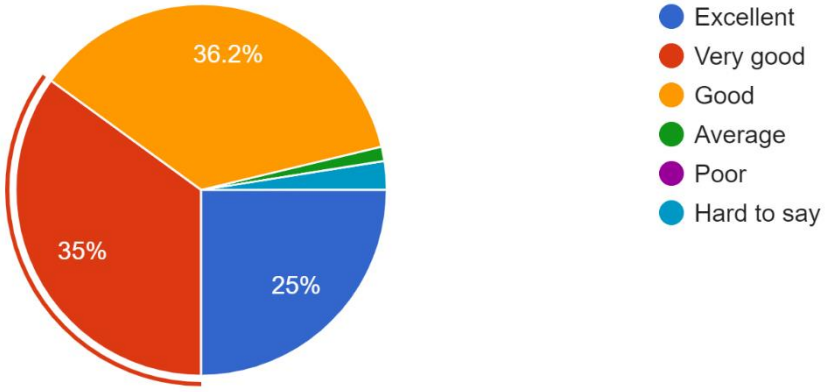
ONLINE SERVICES NEED TO BE MODIFIED	FREQUENCY	PERCENTAGE	CUMULATIVE FREQUENCY
ATM SERVICES	20	25%	20
ACCOUNT SERVICES	10	12.5%	30
FUND TRANSFER	5	6.3%	35
BILL PAYMENT	0	0%	35
E-TAX PAYMENT	1	1.3%	36
E-DEPOSITE	6	6.2%	41
MARKET INVESTMENT	4	5%	45
LOANS & CREDIT	6	7.5%	51
INTERNET SECURITY SERVICES	23	28.7%	74
OTHERS	6	7.5%	80

INTERPRETATION:

This chart shows that "ATM SERVICES", "ACCOUNT SERVICES" and "Internet security services" should be modified in near future.

Give your overall rating in online banking services

80 responses



OVERALL RATING	*FREQUENCY*	*PERCENTAGE*	*CUMULATIVE FREQUENCY*
EXCELLENT	*20*	*25%*	*17*
VERY GOOD	*28*	*35%*	*45*
GOOD	*29*	*36.2%*	*75*
AVERAGE	*1*	*1.2%*	*76*
POOR	*0*	*0%*	*78*
HARD TO SAY	*2*	*2.5%*	*80*

INTERPRETATION:

The satisfaction level of people with the online banking services of their banks has a mixed Review. This may due to multiple reasons. Moreover 36% people choose "VERY GOOD" option.

CHAPTER-7

FINDINGS, RECOMMENDATIONS & CONCLUSIONS

7.1. THE MAJOR FINDINGS OF THE PRIMARY SURVEY ARE:

- 80 people respond to this study. But out of which 57 people claim that they perform online banking service.
- 57 respondents use internet more than three hours in a week.
- Out of 80 people are 51 male and 28 female a 1 transgender. That's mean the male have more knowledge about the transactions and having more knowledge about the services provided by the banks. Only working ladies and school-college students having knowledge about that service.
- Most of the respondents who lies under below 20-35 are using E-Banking services.
- Most of the respondents are either H.S pass or Graduate.
- It is very interesting to see that 27 people have accounts in SBI, AXIS and ICICI banks. But SBI BANK has more customers than others.
- Among 80 respondents 38 said that their banks run under CORE BANKING SOLUSION and this is very good for Indian economy.
- Saving time & speed and convenience is the main benefit which online banking users have seen among other options.
- Most of the online banking users have a tendency to spend Rs.1000 or below this amount in a single transaction.
- Users got excellent services from ATM BANKING, BALANCE ENQUARY, BILLS PAYMENT, ONLINE SHOPPING and ONLINE RECHARGE etc. and other services have not excellent performance like that.
- Among 80 respondents 51 people said that their bank educated them about the several online banking services and on the other hand 9 people said that their bank did not educate them about their net banking services. So, it is very controversial matter.
- Most of the users have no requirement for daily or monthly base transactions, they prefer weekly base transactions.
- This study revealed that most of the users claim that they aware of security threats and they took recommend steps to secure the net banking.
- Maximum number of respondents claim that their banks do not charge extra charges for net banking facilities.
- Out of 80 respondents 59 people told that they will continue online banking activities in future.
- Most of the respondents claim that LACK OF AWARENESS, LESS COMPUTER FACILITIES and LESS INTERNET CONNECTION are the main causes for non-accessibility of online banking by majority of people in their area.
- People also claim that ATM SERVICE, BILL PAYMENT SERVICE and INTERNET SECURITY SERVICE should be modified in near future. Some people also vote for CUSTOMER FEEDBACK service.

___CONCLUSION AND LIMITATION:

In a country like India, there is need for providing better and customized services to the customers. Banks must be concerned about the attitudes of customers with regard to acceptance of internet banking. The importance of security and privacy for acceptance of internet banking has been noted in many earlier studies and it was found that people claim that they have knowledge about security issues but they have no clear idea about all kind frauds. The present study shows that customers are more reluctant to accept new technologies or methods that might contain little risk. Hence, banks should design the website to address security and trust issues.

The survey was conducted with 50 people of Noida and Greater Noida. So, we can't say that this is the real trends of net banking of whole the country.

People are not confident enough to whether to rely completely on online banking. There is hesitancy in their minds with regards to preference. So, they use both the online and offline banking.

At the time of survey when I give questionnaires to people, they very casually fill it without think of the depth of the study.

Another point is people are not disclosing their personal data truly.

Due to shortage of time data can't be collected form all types of people.

The study was conducted with the help of students, service holders and business men etc.

The study reveals that ATM BANKING, BILL PAYMENT, ONLINE SHOPPING and ONLINE RECHARGE etc. are performed by so many respondents but it does not reflect that NEFT, RTGS or DMAT services are not performed by the people.

7.2.RECOMMENDATIONS:

We can see the time is changing and we are now accepting technology but there is still a lot of perceptual blocking which hampers the growth its normal tendency of technology, that why the growth of internet banking is very primitive in nature.

- ***Recommendations to banks:***

  - Banks should obey the RBI norms and provide facilities as per the norms. But this are not completely followed by the banks. Some of our respondents complained that their bank does not give feedback of online transaction in proper times. If customers do not get proper feedback then their interest in online services will be reduced. So, bank should take proper steps to build their feedback services.
  - Internet banking facilities must be made available in all banks as well as in all branches.
  - There are some co-operative banks in this area and this type of banks still do not have core-banking facilities. For this reason, this type of bank loses their customers. So co-operative banks should be covered under core-banking system.
  - Link failure is a big problem especially in UCO bank and for this reason the important business deals have been hampered. So, banks should modify their software immediately.

- Now some banks install automated balance update machine to avoid customer harassment but all banks should except this system very quickly.
- Banks should develop their services not only in town areas but also in village areas. Banks should install more and more ATMs in both urban and rural areas.
- There is another problem I faced at the time of conducting this survey that the respondents complained that there are so many ATM machines in this locality but most of the ATMs have normally no cash at all. So, bank should extend this service with regular cash filling.
- Fair dealing with the customers is more preferable. The stuff should be co- operative, friendly and must be capable to understand the problems of the customers.
- Banks should give proper training to customers to use net banking.
- Banks should always update their security systems and create a trust in the mind of customers towards security of their accounts.
- Banks should make their sites more user friendly. Customers should be motivated to use internet banking facilities more.
- Banks are now using two factor authentications i.e. password and OTP but they should improve that and using three factor authentications because hackers sometimes break the two-factor authentication system.

Recommendations to users:

- Use anti-virus and maintain the integrity of your computer by scanning regularly for computer viruses.
- If using the same computer or mobile for online banking, e-mail and web browsing, always LOG OFF banking sessions before checking e-mail or web browsing. computer viruses today are capable of installing themselves through e- mail links as well as web sites where just passively moving your mouse over an image could be enough to install a script that grabs your cached online banking credentials (user ID and password) and allows a criminal to steal money from your account. Always keep your anti-virus software up-to-date.
- Always use original operating system with original commercial anti-virus which could be better than crack version or free sample.
- If you are using computer with multiple operating system (e.g., Ubuntu, Dos or Windows) you must separately install anti-viruses for each O.S.
- Do not respond to e-mails requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information.
- Do not use e-mail (or e-mail-based fax systems like Facey's) to send sensitive information.
- Install a dedicated, actively managed network firewall to limit the potential for unauthorized access to your network or computer. Consider installing a spyware detection program.
- Clear the browser cache before starting an online banking session to eliminate copies of web pages that have been stored on the hard disk.
- Verify the secure session (https or not https) in the browser.
- Avoid using automatic login features that save your personal details.
- Create a strong password but that will be easy to remember without writing it down anywhere.

- Frequently change your password combination for better protection.
- Last but not the least, some of our respondents share that they received a phone call by which a male or female gave a news that the respondents won lottery worth 25 lacs or a big amount from either their mobile company or somewhere else. But the fact is this type of caller want customer's bank details or ATM card details to send the huge money and some
-

CHAPTER- 8

BIBLIOGRAPHY

8.1 WEBSITES: -

- www.google.com
- www.wikipedia.in
- www.slideshare.net
- www.scribed.in
- www.investopedia.com
- www.yahoo.com
- www.sbionline.com
- www.sbi.co.in
- www.linkedin.com
- www.rbi.org.in
- www.rbi.in