



# BEST SECURITY PRACTICES FOR ONLINE TRANSACTIONS

<sup>1</sup>Kiran Kulshrestha, <sup>2</sup>Jyoti Nain

<sup>1</sup>Student, <sup>2</sup>Assistant Professor

<sup>1</sup>Galgotias University,

<sup>2</sup>Galgotias University

## Abstract

Due to the rapid development of Internet applications, data security is becoming increasingly important during transmission from one end to the other, i.e. between sender and receiver, particularly in web-based applications such as Online Transactions and E-commerce. Since the implementation of various techniques to provide security and authentication to online transactions. Here in this thesis various techniques that are implemented for the security and authentication of E-commerce applications are discussed and analysed their various advantages and issues in the technique. The various issues or limitations in the existing technique can be removed, so a complete survey and their advantages and issues are analysed here, so that a new and efficient technique can be implemented in the future based on their various advantages and limitations. Two-factor authentication techniques are used to improve the security of online applications, allowing them to be protected against various attacks. Smartphones are now widely used and accepted by the general public. It is utilised for e banking applications, and practically all personal data is stored on the smartphone, leading to complex attacks such as eurograbber, which is carried out through the installation of a mobile botnet.

## NEED FOR THE STUDY

Each business sector has embraced modern technology and the provision of online services to patrons in this tech-savvy and technologically driven corporate environment. The growing popularity of internet banking and online transactions necessitates providing patrons with security, consistency, robustness, and integrity when executing bank transactions.

The goal of this study is to explore and analyse the best security techniques used by banks and financial institutions to provide the best protection to both banks and customers.

Online security breaches and cyber-attacks put our e-commerce business at risk. Phishing, website hacking, and insecure web services are all examples of online security hazards. Many hackers are capable of breaching a company's network and gaining access to important information. We shall learn how to prohibit online transactions as a result of this thesis.

## Introduction

According to Airehrour et al. (2018), online banking has grown in popularity in the modern business environment as the trend of internet usage and online services has increased significantly. The growing popularity of internet banking and online transactions necessitates providing patrons with security, consistency, robustness, and integrity when executing bank transactions. Virtual banking, internet banking, e-banking, and other financial activities are all examples of online banking activities. It enables a quick and efficient means of conducting business with online banking and transactional features.

According to Alarifi et al. (2017), an online banking system is divided into two phases: registration and login. The registration process of banks follows a similar pattern. The login phase has security levels such as user provision. The login phase includes security levels such as providing a user id and password, followed by an advanced security system. Banks develop security systems as information is compromised by criminal hackers using modified and sophisticated attacks. Banks must have backup and contingency plans, and they must formulate best plans and practises for securing online banking and transactional activity.

Because of the growing popularity of internet-based banking and commerce, the online transaction system has continued to rise in recent years. Consumers and sellers conduct money transactions electronically through online transactions. Millions of people all around the world use the Internet to make various payments. These trade elements function as a type of electronic money. Because of the critical role they play in modern electronic commerce, online transactions have attracted a lot of attention during the last two decades. According to the Statista Fintech research, the total amount of digital payment transactions was assessed at 3,670,864 million euros in 2019, and it is expected to rise to 5,921,831 million euros by 2023.

## Importance of Security Systems For Online Banking and Online Transactions

Integrating security solutions for online banking and online transactions is critical for protecting both clients' and banks' data and information. According to Mujinga et al. (2018), internet banking and transactional activities have grown significantly and have become an indispensable component of people's daily life. Attacks have become increasingly sophisticated as technical advancements have developed. It results in a loss of both money and time. Along with compromising personal information, sensitive and payment systems are also accessed as legitimate users in order to steal the credentials and information of legitimate users.

According to Salem et al. (2019), banks ensure having a reliable security method for securing the transference of sensitive and significant information from a financial standpoint. Furthermore, there have been instances where hackers have established phishing sites that look identical to bank websites in order to lure customers into revealing personal and sensitive information. It assists in entailing information that will assist in growing clients for processing both transactions and data, which increases financial risks and causes security breaches in banks.

### PROBLEM STATEMENT

M-commerce covers a wide range of products and services, from basic applications like mobile marketing to high-security mobile payment apps. Mobile payments are quickly becoming a popular way to conduct financial transactions. Secure authentication and financial transactions must be possible with a mobile payment application.

When it comes to conducting mobile financial transactions remotely, authentication and safe payment are important security concerns.

"To discover the best online transaction security practises"

### RESEARCH QUESTION

The purpose of this dissertation is to provide a platform-independent secured authentication and payment mechanism for online transactions. To do the same, the following research question was investigated:

- What are the best security techniques for online transactions which we can use?
- What are the security requirements that a platform-agnostic authentication and payment system must meet?

### RESEARCH METHODOLOGY

People conduct research in order to discover information in a systematic manner. Research can be defined as the gathering and analysis of information on a group of people or an organization's traits, behaviour, attitudes, opinions, and possessions.

The quantitative method is about making meaning of numbers within a context, not just "doing sums." There is a greater emphasis on testing and verification, as well as facts and arguments. Variables, parameters, and assumptions are used to form relationships. Data can come from existing sources (secondary data) or must be obtained specifically for the research (primary data). A census or a survey can provide information.

The information for this thesis was gathered using a questionnaire (Google form), which is one of the most extensively utilised data collection strategies in survey research. It is an effective approach to collect data because each respondent is asked the same set of questions.

### RESEARCH DESIGN

The data collection method was a questionnaire. The purpose of this survey is to understand the best security practices which can we taken while doing online transactions. The questionnaire was consisted of 12 questions, which have 11 were closed questions and the 1 was an open question. At the beginning of the questionnaire there were two personal questions, which defined respondents name, gender and age.

The population of the research were students of Galgotias university of School of Business and my family and friends.

The amount of population who received the questionnaire by whatsapp was 38.

Google Form was used as a tool to build a questionnaire and to collect results.

# Best Security Practices for Online Transactions

Sign in to [Google](#) to save your progress.  
[Learn more](#)

Name

Your answer

Gender

- Male
- Female

Age

- Between 15-20
- Between 21-30
- Between 30-45
- Between 45-60
- above 60



Do you use Online Transaction?

- Yes
- No

Do you think that using Online Transaction makes your life easier?

- Yes
- No

Have you ever lost money due to digital fraud?

- Yes
- No

You do Online transaction on:-

- Daily
- Weekly
- Monthly
- Yearly



What security measures you think is best while doing online transactions?

- Use a secure connection
- Use a trusted website
- Read the privacy statement
- Opt for credit over debit
- Keep an eye on your Accounts

What security measures you take while doing online payment?

Your answer

---

What are your reasons for choosing online transactions services?

- Convenience( 24 hours service, anywhere connectivity)
- Easy to maintain my banking transaction activity
- Safe and Secure
- Better Rates
- Low service charge



What for you are the major barriers of online banking?

- No Barriers
- Don't trust the bank security
- Don't like entering data digitally
- Finding the Technology Difficult
- Incnvenient
- Doesn't provide all services

What are the security measures that could secure you against various kinds of online banking attacks?

- Self-awareness in security
- Installing anti-malicious software
- Limiting online activities
- User education
- Increasing/updating level of online transactions

Submit

Clear form



ANALYSIS AND INTERPRETATION OF THE DATA

I have collected a primary data from 38 people through a questionnaire in google form. That google form consist of 12 questions.

Out of that 12 questions:-

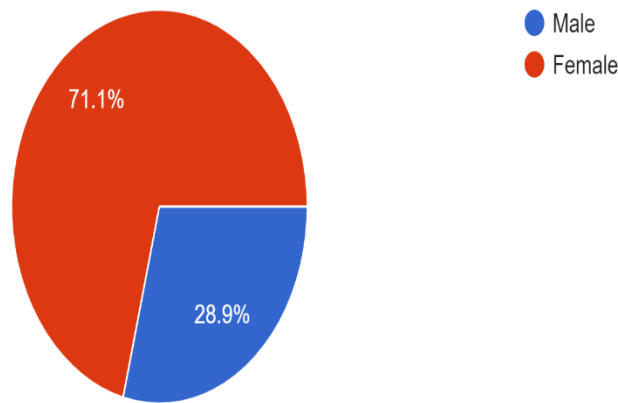
- First question was for the candidate name who is filling the form
- Second question is for there Gender
- And, third question is for there age.

So, lets analyse the data collected from 38 population:-

So, our Second question is- What is the gender of candidate who is filling the form?

Gender

38 responses



Here, We can see that this chart shows that 71.1%(27 candidates) are the female candidates who has filled the form and 28.9%(11 candidates) are the male candidates.

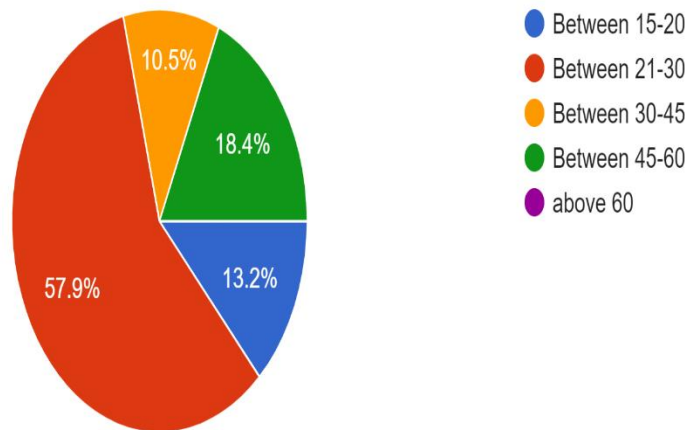
Third Question:- What is the age of candidates?

Through this question we get to know about which age of population is doing more online transactions.



### Age

38 responses



Here, we can see that the respondent who are using online transactions are 13.2%( between 15-20), 57.9%( between 21-30),

10.5%( Between 30-45), 18.4%( between 45-60) and 0% for above 60.

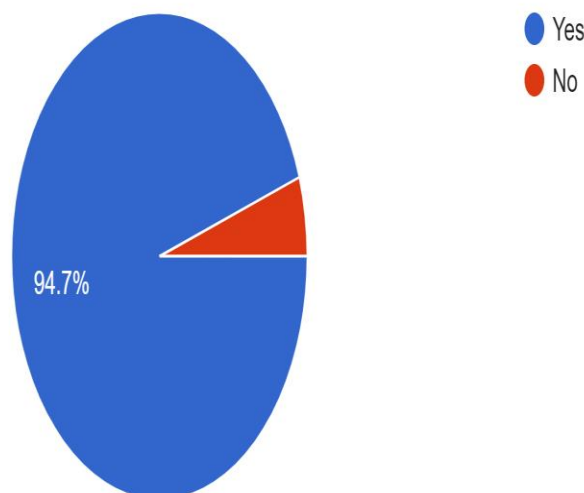
By this, we can say that the population between the age of 21-30 are doing more online transactions.

### Fourth Question:- Do you use online transactions?

Through this we get to know about how many population is using online payments and online transactions out of all the population who filled the questionnaire.

### Do you use Online Transaction?

38 responses



Here we can see that out of 38 responses, 36 people use online transaction and online payment.

Only 2 people are there who did not use online transaction.

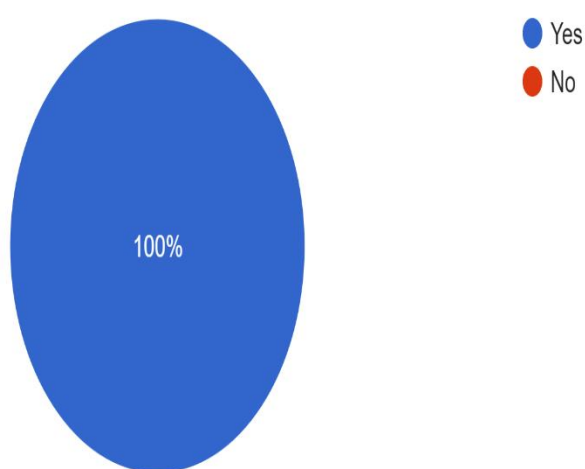
94.7% of population use online transaction.

Fifth Question:- Do you think that using online transaction make your life easier?

Through this we get to now about that people think that there life is easier with online payment and transactions or they prefer to pay by cash.

Do you think that using Online Transaction makes your life easier?

38 responses



Here we can see that 100% of population think that online transaction have make there life easier. Both consumers and business owners benefit from online transactions. This is due to the fact that online transaction payment methods like BRIVA and Direct Debit enable for immediate payment verification.

Consumers are not required to send their evidence of payment personally.

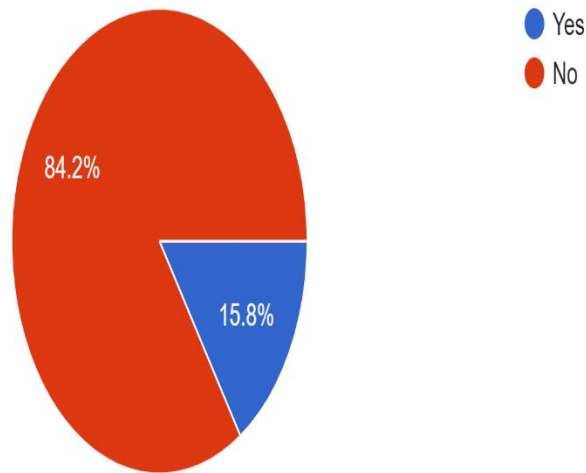
Sixth Question:- Have you ever lost money due to Digital Fraud?

Any kind of transaction on a digital platform that is illegal and unauthorized is defined as online fraud, cyber fraud, or digital fraud.

Through this question we get to know about how many respondents have experienced a Digital Fraud earlier.

### Have you ever lost money due to digital fraud?

38 responses

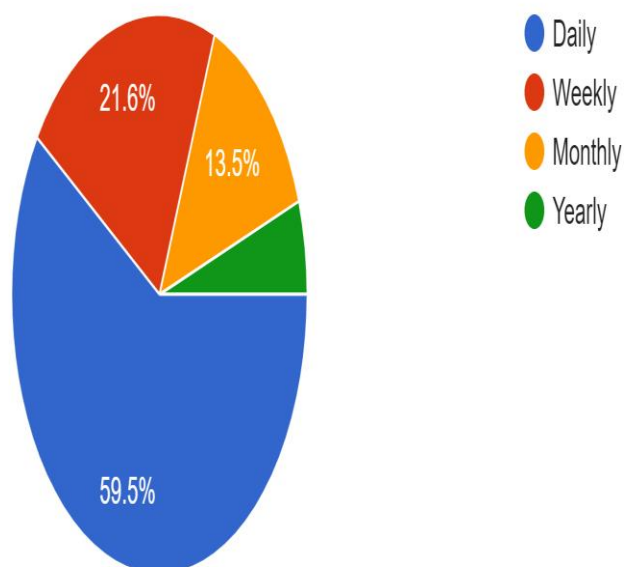


Out of total respondents, 84.2%(32 respondents) have not lost money due to digital fraud and 15.8%( 6 respondents) have lost money due to digital fraud.

### Seventh Question:- You do online transaction on daily, weekly, monthly or yearly basis?

### You do Online transaction on:-

37 responses



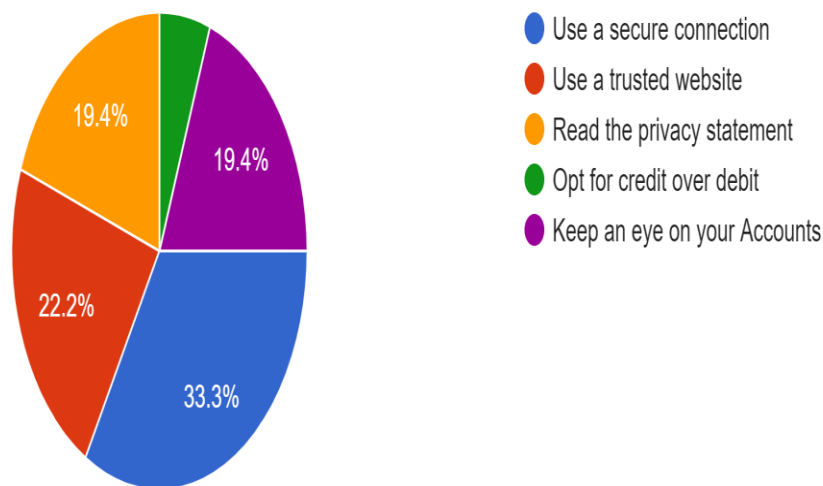
Here we can see that 37 respondents have filled this form. Out of 100%, 59.5%(22 respondents) do daily transactions, 21.6%( 8 respondents)do weekly transactions, 13.5%( 5 respondents) do monthly transaction, 5.4%(2 respondents) do yearly transactions.

#### Eighth Question:- What security measures you think is best while doing online transaction?

Through this question we get to know what are the best security measures we can take and we are taking while doing online transactions.

What security measures you think is best while doing online transactions?

36 responses



Here we can see that 33.3%(12 respondents) use a secure connection, 22.2%(8 respondents) use a trusted website, 19.4%(7 respondents) read the privacy statement, 19.4%( 7 respondents) keep an eye on your account, 5.6%( 2 respondents) opt for credit over debit.

#### Ninth Question:- What security measures you take while doing online payment?

Through this question we get to know about the security measures which all the respondents take while doing online transactions. This question is a open ended question so I have received so many answers for this question. Please find below the answers:-

- Use a trusted website and only use otp when I am doing online transaction
- Using a trusted website and this too over a secure connection. And also keep eye on my accounts.
- Taking all security measures
- Write the correct otp and write the correct amount
- There should be proper authentication from the user in order to reduce the to of frauds. Proper OTP,email OTP and two factor authentication is helpful
- Use a tursted website
- Need to ensure secure connection and trusted website
- Two step authentication or two time pin ; one for opening app and second for transaction.
- Using OTP for online transaction and use a secured website
- Don't transfer money through fraud website

- 2 security payment
- Make sure doesn't share OTP with anyone else
- Pin
- Checking my account balance now and then. Reading the privacy statement while doing any transaction
- Use trusted website and check my account on daily basis
- We should share OTP to anyone
- We should not share the OTP to any one
- The website should be genuine
- Use a trusted website
- Always wants password for security
- Use secured INTERNET
- Use secure internet
- Using secure connection and keeping eye on my account

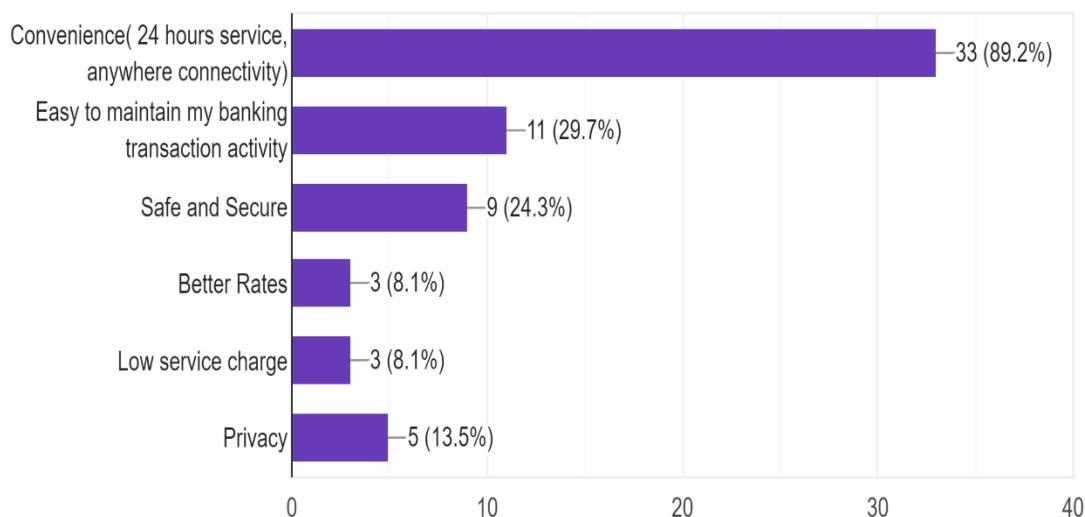
#### Tenth Question:- What are your reasons for choosing online transactions services?

Through this question we get to know about the various reasons for choosing online transactions or online payments by the people over the cash.

When you use online transactions, you can rapidly transfer money across accounts. You may quickly access monies needed to make purchases and payments to keep your business running smoothly by moving money across accounts, even while out of town.

#### What are your reasons for choosing online transactions services?

37 responses



Here, we can see that 89.2% (33 respondent) are saying that online transaction is convenience for them, 29.7%(11 respondent) are saying that it is easy to maintain my banking transaction activity, 24.3%(9 respondent) are saying that it is safe and secure, 8.1% (3 respondent) better rates, 8.1% (3 respondent) low service charge, 13.5% ( 5 respondent) privacy.

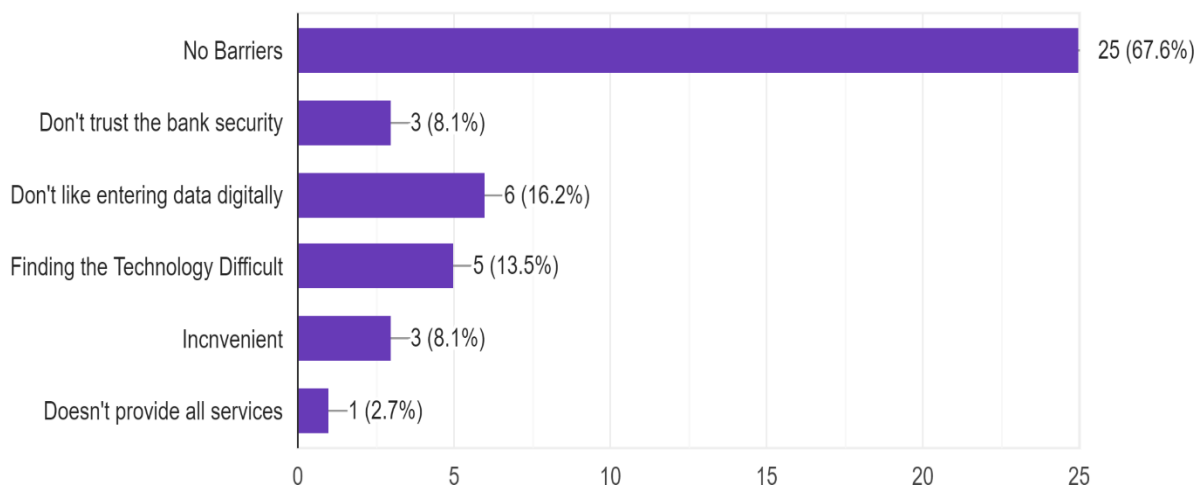
#### Eleventh Question:- What for you are the major barriers of online banking?

Through this question we want to know about the barriers which the people are facing during the online transaction.

Barriers (sometimes known as "adoption hurdles" or "conversion barriers") are obstacles that hinder a customer from progressing through the funnel. At each stage of the funnel, there may be obstacles.

What for you are the major barriers of online banking?

37 responses



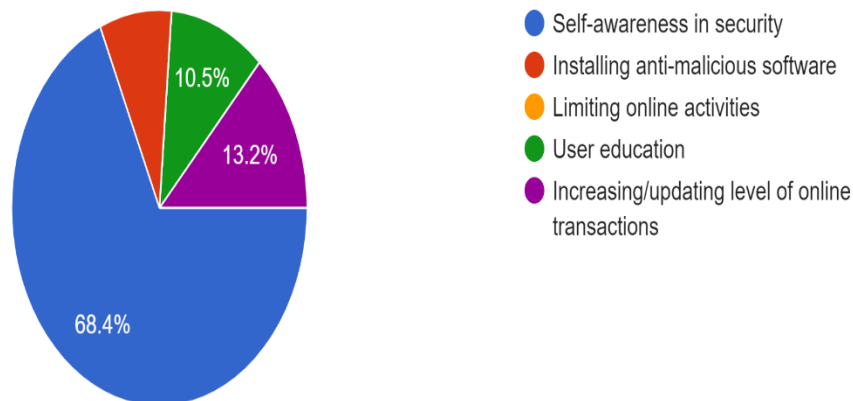
Here we can see in this chart that 67.6%(25 respondents ) are saying that there are no barriers during the online transactions, 8.1%(3 respondents) don't trust the bank security, 16.2%(6 respondents) don't like entering data digitally, 13.5% (5 respondent) finding the technology difficult, 8.1% ( 3 respondent) find it Inconvenient, 2.7% (1 respondents) Doesn't provide all services.

**Twelfth Question:-** What are the security measures that could secure you against various kinds of online banking attacks?

Through this question we will get to know about the security measures which can we take while doing online transaction.

What are the security measures that could secure you against various kinds of online banking attacks?

38 responses



Here we can see in this piechart that 68.4%(26 respondents) are saying self-awareness in security, 13.2% (5 respondent) Increasing/updating level of online transactions, 10.5% ( 4 respondent) User Education, 7.9%( 3 respondent) Installing anti-malicious software.

### RESEARCH ANALYSIS

As we can see that we have done our research by giving the questionnaire to so many people.

Through this research our aim was to find out the best security practices in online transaction which can be taken by the people while doing online transaction.

Through this study we get to know about what type of security measures people prefer while doing their online transactions so that they can protect themselves from any security issues.

We get to know about the barriers which the people are facing while doing online transaction. The security related issues to online transaction are phishing, internet scams, malware identity theft, investment fraud etc. If I analyse this question question of my research paper we can find out that mostly people are saying that they did not have any barrier while doing online transaction.

In today's world, mostly people prefer to do transactions online because it is more convenient and user friendly. We can do online transaction anywhere and anytime but the thing is that you should do that in a secured manner so that it cannot be changed into fraud like you should always prefer to choose a trusted website for online transactions and use OTP for any transactions.



## CONCLUSION

The goal of this study is to explore and analyse the best security techniques used by banks and financial institutions to provide the best protection to both banks and customers.

Phishing, internet scams, malware identity theft, investment fraud, keystroke attack, lottery frauds, Trojan horse, pharming, virus, and worm are explored in this research study as security risks associated to online transactions and banking.

As stated in this research context, the security systems that can be incorporated for online banking and transactional activities include the use of user id and transactional password, OTP, QRP, Biometric, QR Code, Grid Authority card, E-token, and security questions.

Protecting the confidentiality of a user ID with a password, logging out after completing online banking and transactional activities, using a modern browser with anti-virus software, ensuring information security, using a separate computing system for conducting high cash transactions, and using a secure website are all responsibilities of people.

According to reports, technological advancements have advanced, and attacks have become increasingly complex. As a result, security solutions for online banking and online transactions have been integrated to secure the data and information of both clients and banks.

## Reference

- Innovative Systems Design and Engineering ISSN 2222-1727/ISSN 2222-2871, Vol 3, No 6, 2012
- Wikipedia, Electronic Commerce, <http://en.wikipedia.org/wiki/Electronic-commerce>
- IBM Knowledge Center, Main frame computers
- Arora p., Singh A., Tyagi H., Evaluation and Comparison of security Issues on Cloud Computing Environment, World of Computer Science and Information technology Journal (WCSIT) ISSN: 2222-0741, Vol. 2, No.5, 179-183,2012.
- The future of identity in the information society, IFIP Advances in Information and Communication Technology, Volume 298,2009,pp 119-134.
- Trend Micro, Addressing Big Data Security Challenges: The Right tools for smart protection, [http://www.trendmicro.com/cloud-content/us/pdfs/about/wp\\_big-data-security-challenges.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/about/wp_big-data-security-challenges.pdf)
- Goode, A., 2018.Biometrics for banking: best practices and barriers to adoption. Biometric Technology Today, 2018(10), pp.5-7.
- Hossain, S.A., Bao, Y., Hasan, N. and Islam, M.F., 2020.
- Perception and prediction of intention to use online banking systems: An empirical study using extended TAM. International Journal of Research in Business and Social Science,9(1), pp.112-126.