THAKUR TRUSTS

Thakur Educational Trust's (Regd.)

THAKUR COLLEGE OF SCIENCE & COMMERCE

AUTONOMOUS COLLEGE, PERMANENTLY AFFILIATED TO UNIVERSITY OF MUMBAI

NAAC Accredited Grade 'A' (3rd Cycle) & ISO 9001: 2015 (Certified)

Azadi Ka Amrit Mahotsav Best College Award by University of Mumbai for the Year 2018-2019

tcsc CELEBRATING 25 YEARS OF GLORY

"A STUDY ON CYBER SECURITY AFFECTING ONLINE BANKING AND ONLINE TRANSACTION"

UNIVERSITY OF MUMBAI

A PROJECT SUBMITTED TO

University of Mumbai for partial completion of the degree of

Bachelor in commerce (Banking and Insurance)

Under the faculty of commerce

By

Ishika Pramod Mandliya

ROLL NO: - 7406

T.Y.B.B.I

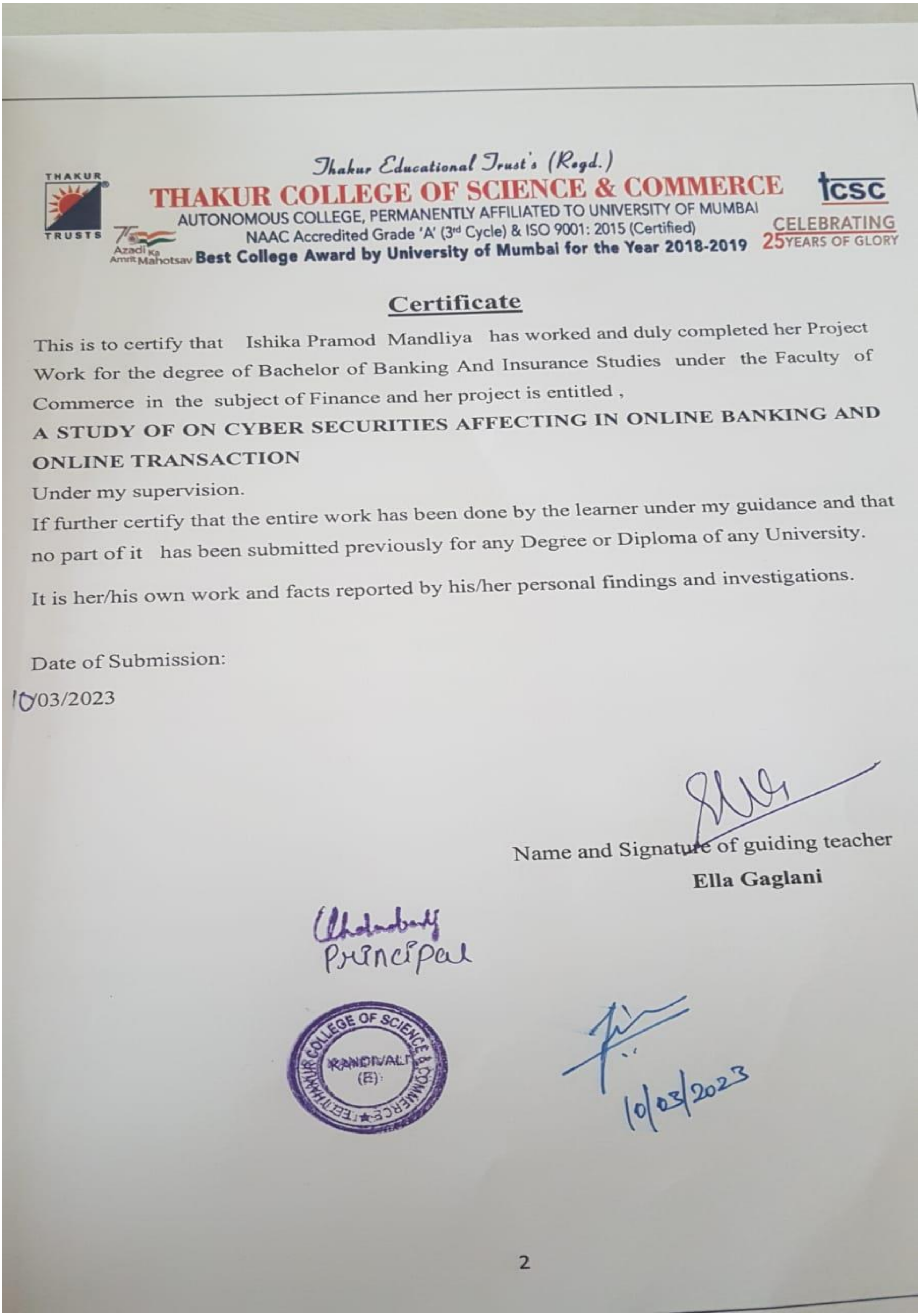
(SEMESTER VI)

Under the Guidance of

ASST. PROF. ELLA GAGLANI

THAKUR COLLEGE OF SCIENCE AND COMMERCE,

KANDIVALI (EAST)



THAKUR TRUSTS

Thakur Educational Trust's (Regd.)

THAKUR COLLEGE OF SCIENCE & COMMERCE

AUTONOMOUS COLLEGE, PERMANENTLY AFFILIATED TO UNIVERSITY OF MUMBAI

NAAC Accredited Grade 'A' (3rd Cycle) & ISO 9001: 2015 (Certified)

Azadi Ka Amrit Mahotsav Best College Award by University of Mumbai for the Year 2018-2019

tcsc CELEBRATING 25 YEARS OF GLORY

Certificate

This is to certify that Ishika Pramod Mandliya has worked and duly completed her Project Work for the degree of Bachelor of Banking And Insurance Studies under the Faculty of Commerce in the subject of Finance and her project is entitled ,

A STUDY OF ON CYBER SECURITIES AFFECTING IN ONLINE BANKING AND ONLINE TRANSACTION

Under my supervision.

If further certify that the entire work has been done by the learner under my guidance and that no part of it has been submitted previously for any Degree or Diploma of any University.

It is her/his own work and facts reported by his/her personal findings and investigations.

Date of Submission:

10/03/2023

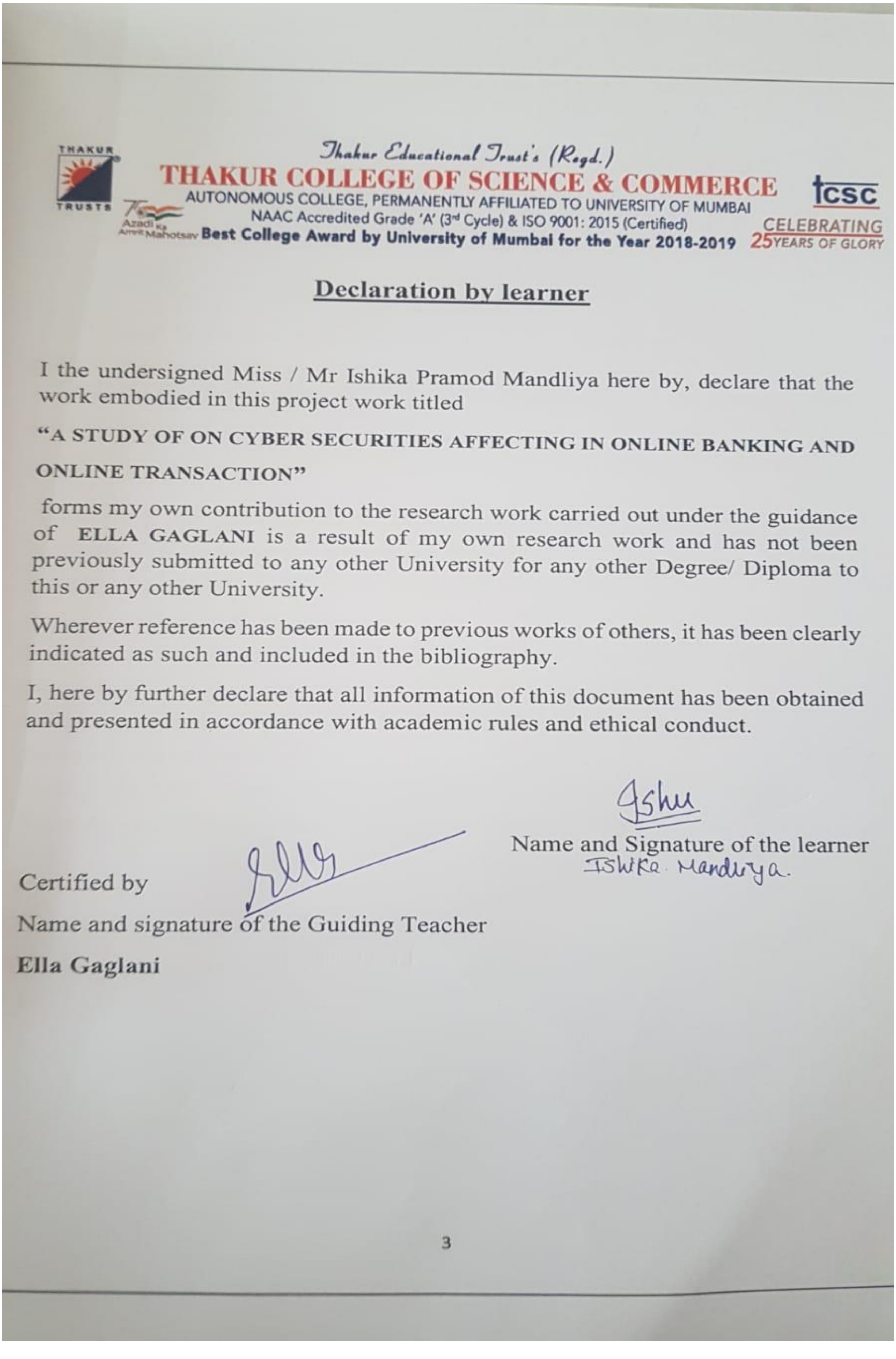
Name and Signature of guiding teacher

Ella Gaglani

Principal

THAKUR COLLEGE OF SCIENCE & COMMERCE
KANDIVALI (E)

10/03/2023



Thakur Educational Trust's (Regd.)

THAKUR COLLEGE OF SCIENCE & COMMERCE

AUTONOMOUS COLLEGE, PERMANENTLY AFFILIATED TO UNIVERSITY OF MUMBAI

NAAC Accredited Grade 'A' (3rd Cycle) & ISO 9001: 2015 (Certified)

Best College Award by University of Mumbai for the Year 2018-2019

tcsc CELEBRATING 25 YEARS OF GLORY

Declaration by learner

I the undersigned Miss / Mr Ishika Pramod Mandliya here by, declare that the work embodied in this project work titled

"A STUDY OF ON CYBER SECURITIES AFFECTING IN ONLINE BANKING AND ONLINE TRANSACTION"

forms my own contribution to the research work carried out under the guidance of **ELLA GAGLANI** is a result of my own research work and has not been previously submitted to any other University for any other Degree/ Diploma to this or any other University.

Wherever reference has been made to previous works of others, it has been clearly indicated as such and included in the bibliography.

I, here by further declare that all information of this document has been obtained and presented in accordance with academic rules and ethical conduct.

Ishu

Name and Signature of the learner

Ishika. Mandliya.

Certified by

Name and signature of the Guiding Teacher

Ella Gaglani

Acknowledgment

To list who all have helped me is difficult because they are so numerous And the depth is so enormous.

I would like to acknowledge the following as being idealistic channels and fresh dimensions in the completion of this project.

I take this opportunity to thank the **University of Mumbai** for giving me Chance to do this project.

I would like to thank my Principal, **DR. (Mrs) C.T. Chakraborty** for providing the Necessary facilities required for completion of this project. I take this opportunity to thank our Co-ordinator **MR. Nirav Goda** For her moral support and guidance.

I would also like to express my sincere gratitude towards my project guide **Prof Ella Gaglani** whose guidance and care made the project successful. I would like to thank my College Library, for having provided various reference Books and magazines related to my project.

Lastly, I would like to thank each and every person who directly or indirectly helped Me in the completion of the project especially my Parents and Peers.

PLAGIRISIM SCAN REPORT

INTRODUCTION	UNIQUE
8	100%
9	100%
10	89%
11	93%
12	100%
13	97%
14	92%
15	96%
16	100%
17	89%
AVERAGE	94%

RESEARCH METHODOLOGY		
PAGE NO	UNIQUE	PLAGARISIM
18	100%	0%
19	71%	29%
20	89%	11%
21	100%	0%
REVIEW LITERATURE	UNIQUE	PLAGARISIM
22	100%	0%
23	100%	0%
24	93%	7%
25	100%	0%
DATA INTERPRETATION	UNIQUE	PLAGARISIM
26	83%	17%
27	83%	17%
28-50	100%	0%
FINDINGS	UNIQUE	PLAGARISIM
51	100%	0%
RECOMMENDED		
52	100%	0%
FURTHER SCOPE OF RESEARCH		
53	100%	0%

LIMITATION OF YOUR RESEARCH		
54	100%	0%
CONCLUSION AND SUGGESTION		
55	100%	0%
BIBLOGRAPHY		
56,57,58	55%	45%
APPENDIX AND QUESSIONIARE		
59-63	100%	0%

Index

Summary:

In the era of globalization, internet banking or online banking has revolutionized an essential activity in the modern 21st century. As social beings, humans have developed different methods of communication in order to exchange information, ideas and knowledge that are of great importance to him. Advances in electronic banking technology have made this task very easy. Banking transactions are just one click away, super-fast. Online banking and mobile banking make everyday banking transactions fast and convenient. The increasing misuse of information technology in cyberspace is contributing to cybercrime at national and international levels. The rate of risk and related problems is increasing. However, online and mobile banking is never 100% secure. The purpose of this research paper is to review cyber-attacks. This article focused on cybercrime related to online banking and the new tricks and methods used by hackers. This study is based entirely on auxiliary data. The findings of this study reveal the increasing use of IT and cybercrime related to online banking in India. Most cybercrimes are committed by young people and men between the ages of 18 and 30. Law enforcement agencies must be properly equipped to deal with and prevent cybercrime. Finally, the researchers made some suggestions for the prevention and safe use of online banking.

Keywords - Information technology, cybercrime, cyber-attack, mobile banking, online banking, national crime record office, hacking.

CHAPTER 1:- INTRODUCTION

In 1970s were the real beginning (and necessity) of cyber security This
has been an important decade in cyber security development.
The Advanced Research Projects Agency Network (ARPANET) was the first attempt to do this.

.

In the era of globalization, internet banking or online banking has revolutionized the most important activity of the modern 21st century. We hope you remember the days when cash and valuables were safely stored. Online scams have us securing money, jewellery stores in our home lockers. Since there was no cyber security in the old days, security was also kept to avoid hacking, theft, and fraud. We also cannot give our money or jewellery to anyone. Cyber security serves as physical protection by keeping society safe. No accounts for trading or security, transfer money through people who know security.

Cyber security is a process designed to protect a networks and devices from external threats.

Companies typically hire cyber security experts to protect sensitive information, keep employees productive, and increase customer confidence in their products and services.

Since then, the banking sector has adopted a variety of ways to serve the common people when it comes to money. With the advent of Internet , the banking sector has completely changed, especially in terms of security. Because now money is in our hands with just one click. Users can manage their money through methods.

Electronic banking means the provision of banking products and services through electronic delivery channels. This is a banking method in which a customer conducts a transaction electronically over the Internet. Also known as

Electronic Funds Transfer (EFT), this is the direct transfer of funds from one account to another using electronic funds rather than checks or cash..

Banks today should be the safest place for people's money. In fact, they have a fiduciary responsibility to actively mitigate and manage the account holder's risk.
Unfortunately, bank and credit union executives often don't realize how serious the problem is. Data at risk electronically leads to identity theft and theft of funds. In the end, your reputation is ruined. We believe that financial institutions will pay more attention to implementing “password less” solutions that require multi-factor authentication (MFA). According to a 2021 Forrester survey, 67% of corporate executives were on the way to implementing password less authentication for their employees and partners. I think this trend will and should continue in banking.

Over the next few years, artificial intelligence and machine learning will remain the main drivers of cyber security in the financial services industry. We’re already starting to see this in some of the more advance security products coming to market, such a “good bots” versus “bad guys.”

Automation is another important factor in terms of risk and reward as banks and credit unions are trying to automate everything they can. We will see more low-code and no-code platforms that aim to improve the efficiency of financial institutions while reducing human error.

You all are now aware, in modern world we mostly use virtual money and also do online transaction for money management.
Online Banking makes physical and paperless banking free to everyone. Online banking also reduces the banks operating costs by reducing costs associated with 4,444 customers and reducing its branch network. Now the daily use of online banking has become a common practice of people for daily transactions.
Programme, plans and policies that bridge this skill gap in cyber security. Closing the generation gap in cyber security and enabling more diversity in the field is another critical priority of today.

Cyber security means the body of technology and practice designed to protect networks, devices etc. From attack, damage from any unauthorized access.

Cyber Security is the application of technologies, processes and controls the practice of protecting system, network, programs, devices and data form cyber-attacks. Its aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, network and technologies.

The focus of this research paper is the evaluation of the benefits and challenges of online banking, analyses the challenges faced by online banking services and offers suggestions on preventive measures and security tips to control and prevent cybercrime.

Don’t you think our online funds also deserve reliable protection? So cyber security works. Cyber security is a practice of protecting computers, services, mobile devices, electronic systems, networks and data from malicious attacks.
This is also known as information technology security or electronic information security. The term is use in a variety of contexts, form business to mobile computing and can be broken down into a few general categories. Network security is a way to protect computer networks from intruders, whether they are targeted attackers or opportunistic malware.

Application security focuses on protecting software and devices from threats. Compromised applications can provide access to data they are designed to protect. Successful security begins at the design stage, long before a program or device is deployed.
Information security protects to integrity and confidentiality of data during storage and transmission. Operational security includes processes and solutions from handling and securing data assets.
Procedures for managing the permissions users have when accessing the network and how and where data can be stored or shared fall into this category.
Disaster recovery and business continuity define how organizations respond to cyber security incidents or other events that result in loss of operations or data. A disaster recovery policy defines how an organization recovers operations and information to return to the same operational capacity as before an event. Business continuity is a plan that organizations rely on when trying to operate without certain resources
End user training focuses on the most unpredictable element of cyber security people. Anyone who does not follow security recommendations can accidentally introduce a virus into a protected system, Educating users to remove suspicious email attachments and stop connecting unrecognized USB drives is critical to the security of any organization.

Cyber Security Tips- Protect yourself from cyber-attacks.

1) Update your software and operating system. This means you can enjoy the latest security updates.

2) Use antivirus software for security solution like the Kaspersky Total Security it detect and remove threats and keep your software up to date for the best level of protection.

3) Use strong password to make sure your password is difficult to guess.

4) Do not open email attachments from unknown senders as they may be infected with malware.

5) Avoid using unsecured WI-FI networks in public places. An insecure network is vulnerable to mam-in-middle attacks.

Advantages and Disadvantages of online banking:-

1) **Convenience: -** Online banking offers exceptional convenience to its customers. Our smartphones and computers are always available and provide 24/7 access to your account. While online banking access and pay from the comfort of your home or office at the touch of a button. Non-trading funds also be used together
Online banking to finance transactions such as account renewals, new checks, and more.
2) **Security: -** Security is a top priority for financial institutions when customers use online banking. Banks take account security very seriously and invest a lot of time and money to keep your account safe. Online account security. Many mobile banking applications now accept encrypted biometric authentication for login. When a connected bank requests additional login verification, the bank can also automatically provide protection against certain risks. Used by unknown devices.

3) **Online Invoice Payment: -** With easy account login and efficient online billing. The automatic bill payment feature only requires you to enter some information at a time. The bank sends each payment statement by message or mail.

4) **Mobility: -** Online banking has taken it a step further in the last few years in the form of mobile internet banking and covers the realm of unlimited mobility.

5) **Remittance: -** Online banking speeds up the transfer of funds from one account to another, saving time and money and making it more convenient. To view transactions. Online banking allows you to access your account history and transactions from anywhere. Is because is the fastest way.

6) **Head down: -** Online banking have low online banking fees as there may be no online banking fees.

Types of cyber security:-

1) App security:-

- Most of the apps you use on your phone are safe and work according to the Google Play Store rules and regulations.
- Users can download 1.85 million different applications. Not all apps are safe just because there are other options.
- Many applications pretend to be safe, but after receiving all the information from us, the user of the application exchanges information with third parties for money and the application stops working. - Sudden cyber-attack. The app must be installed from a trusted platform other Google Chrome **Top 11 Tips for Cyber Securities:-**

Back up your data:-

Backing up your data on your devices by copying it to another, separate location is one of the most important things you can do. If you're pointed by a cyber- attack you may not be able to access or use your Pc laptops, phone, or any of your other devices. But if you backed up your data you won't lose anything no matter what happens to your device.

1) Keep your apps up-to-date:-

When you know to update your device or one of your apps, don't ignore if it install it as soon as possible. You should update your features. They're also about fixing sensitivity. In your device or an app that cyber attackers could find and use to gain access to your system. If your device can't receive any updates anymore, we should plan to upgrade a newer model. - Update your device software and applications.

- Set your system settings to update automatically, so you don't have to worry. - Remove any applications you should no longer use from your device.

2) Choose unique password:-

We all have so many online accounts now that it's become hard to keep track of all of the passwords we need for them. To fight. So many of us use the same password for all of our accounts, or stick to two or three different ones that we use over. The problem with this is that if a cyber-attacker gets access to one of your account passwords, it often gives them access to many of your other accounts as well.

- Use different passwords for every online account you create
- . Try a password manager to store and manage your passwords.
- The password manager is the only account you need to remember your login details for.
- Try short passwords or add random words to create passwords instead of passwords.

3) Turn on two-factor authentication: - Turn on two-factor authentication: - Twofactor authentication is a way that you can help to protect your online transaction s from being hacked. You can also choose to have a code sent or generated on your device, like your phone, that you can use to authenticate who you are every time you log in. That way, even if someone gets access to the account password, if they don't have your phone to receive the code So that way your account is secure. - Turn on two-factor authentication for important accounts like email and social networking accounts.

- If more than one type is available, choose the non-SMS option as SMS is less secure.
- Using SMS as a second factor is much more secure than not using two-factor authentication.
- Two-factor authentication (2FA) is another way to protect your online account from being hacked.
- You can choose to send or generate a code from a device such as a phone that can be used for authentication each time you log in.
- So even if someone gets access to your account password, they won't be able to log in to your account unless they have a mobile phone to receive the code.

4) **Mobile securities touch: -** .

1) Then you need to install all security patches on this phone.
2) You should lock all payment apps using your phone's built-in app and never share your phone password outside of your family.

- You can either
- Get an external hard drive and do an 'offline' or 'cold' backup, or - Sign up to a cloud based service like Dropbox and do a cloud backup . - Back up your data regularly (e.g. weekly).

5) **Be creative with the answers to your account recovery questions:-**

When creating a new online account, you are often prompted to set a password to secure your account in order to recover it. It is commonly used as a way to identify a user if they have forgotten their password and need a hint. It's often based on something easy to remember, like the name of your first pet or where you went to school. Unfortunately, these are easy for attackers to detect and can be used to access your account without your knowledge.

- Be creative when asked to answer account recovery questions. For example, instead of being honest about which school you went to, you could say "Hogwarts".

6) **Avoid confidential deals on free wives: -** When using hotspots or free wives (e.g. when entering a coffee shop), it is a good idea to be mindful of what you are doing online as these networks are often unsafe. If your network is not secure, anyone can access it and get your data. There is also the risk that people are looking over your shoulder to see your login details. So while it is possible to check the news or weather forecast, try to minimize the use of more sensitive transactions. - If possible, use your own device and not someone else's.

7) **Install antivirus and scan for viruses regularly**. Antivirus software can help you detect and remove malware (viruses) from your computer system. If you're running Microsoft Windows 7 or later, it comes with a free antivirus called Windows Defender. Otherwise, get a legitimate antivirus from a reputable and trustworthy company. Your local computer service company can advise which method is best for you. Do not download free antivirus software online. Because many programs that are advertised as free are fake. Instead of detecting and removing Malware or adware, it can be downloaded to your computer. Solution

- Install an antivirus program on your computer. If you're not sure if you can do it yourself, a computer service company can do it for you.
- Runs regularly (egg weekly) and removes detected viruses.
- Report any viruses you find to your IT professional the next time you find them.

8) **Note the social networks**: - Did you know that the information you post on your Facebook profile, Twitter feed or Integra account could be used to steal your identity or hack your online accounts? We are so used to sharing things online that we don't even think about it. Everyone knows your pet's name, school, job, and even when you go on vacation. Unfortunately, this window not only informs your friends and family what you are doing, but also provides information that cybercriminals can use to gain access to your data or steal your identity

- Ensure the privacy of your social media accounts. Set your full details to be visible only to your friends and family. • Do not post too much personal information on your social media accounts.
- Remember the advice about passwords. If you share a picture of your dog on Facebook, make sure you don't use your dog's name as your password.

9) **Limit the personal information you provide online. -** Scam and phishing emails often masquerade as legitimate businesses, such as banks, to trick you into providing personal or financial information. This is useful to know to understand which requests are genuine and which are not. Do not give out personal information online unless you know who is asking and why.
   - Stop and confirm before providing personal information. Find out how the companies you do business with will contact you and what information they will ask you for. For example, your bank will never email you an online banking link or ask you to log in.
   - If you are not sure why you are being asked to provide information, call the company directly to find out why the information is needed. Businesses are required to request only the information required by law.
   - If you receive an online request for personal or financial information that you are not sure about, do a background check before disclosing the information. For example, if you're insurance company is requesting information online, call or, if possible, visit your local office to request your request first

10) **Check the bank statements: -** Check your bank statements for suspicious activity such as unexpected purchases or transfers between accounts. If you notice any unusual activity, contact your bank immediately. Seeing someone transfer funds to your bank account or make unexpected payments from your credit card can be the first sign that someone has accessed your account or credit card information.
    - Track your bank accounts and credit cards and always check your statements. - Call your bank as soon as you notice a suspicious payment or withdrawal.

11) **Get a Credit Check:** - Tracking your bank account can help you see if someone else is accessing your account. A credit check can tell you if someone else is using your personal information to get a loan or loan for a large purchase like a car. Often, you first hear of this activity when credit is denied or collectors show up at the door. Tracking your credit history can give you an early warning of unauthorized activity - Get an annual credit check.
    - Take action immediately if you see anything suspicious. Call your bank or finance company on to inform them of the situation and ask how they can help.
    - Conduct an annual credit check.
    - If you notice anything suspicious, take action immediately. Call your bank or finance company to inform them of the situation.

Five Pillars:-

- ➢ Privacy
- ➢ Integrity
- ➢ Availability
- ➢ Authenticity
- ➢ Non-Repudiation

We will now help you understand all of these five pillars individually.

1) Privacy:

Privacy is one of the most important pillars of cyber security.
This ensures that your data is not disclosed to anyone (unauthorized groups, institutions or devices). Privacy is an important part when it comes to data protection. Data is encrypted as it is transmitted from one place to another. Only the recipient and sender of the can understand the information. It will be difficult for third parties to steal your data. Yes. When you chat with your sup friends, your messages are encrypted. No third party can read your messages. Only you and your friends can truly understand this message. Now imagine that other people read all these messages. Will the be a disaster? You shared your personal information and now a third party has it too. Available from third parties. You may be invited to many or different services. Confidentiality is therefore important. As long as your communications remain private, your personal information is safe. You can do whatever you want without any worries. Therefore, privacy is the use of passwords such as encryption and biometric scanning to control access to data.

2) Integrity: -

A message sent to someone by is always stored in its original form. Messages should not be altered in transit. Protect data from tampering by third parties.
An effective security system has been created to keep your data in its original form. Third parties cannot change your information without your
consent. If your data has been changed without your permission , it just means that someone has tampered with your data. Honest model. Let's say you're using an Instagram and chatting with your friends. Someone interrupted you, the person you sent a message to edited your message before received it. This can cause a lot of problems between you and the person you're talking to. Yes. I used my credit card and it suddenly stopped working. When I contacted the authorities of they told me that the information had changed.
How would you respond to that? You can respond positively to.
Therefore, data integrity is essential to prevent such incidents. The data is kept in its original format and no modification by third parties is allowed.

3) **Accessibility:-**

Accessibility means that your data can be easily accessed by anyone with permission to access it at any time. Either way, it will keep your system fully functional. Access your data at your convenience.Resource availability allows them to easily access available information. Availability requires resources to maintain stability and continued access to data through timely updates and maintenance.
Example: Many people use online banking. Assume that all transactions of are done through online banking. You want to access your transaction history and account balance. Now suppose your bank provides access to this information at certain times of the day. The feelings you are feeling are beyond words. Therefore, in order to avoid this, the company tries to provide access to information when necessary (if authorized). It is important to remember that events such as fires and power outages can occur, leaving your data vulnerable to hackers.

4) **Authenticity: -**

Authentication protects data from hackers and requires users to provide proof of access to data. Only access data if you have the right to access it. It is important to check sources of information and links. Authentication controls include passwords, biometrics, and many other methods. Let's look at an example to better understand authenticity. Yes many people use Instagram Log in to your account with your username and password. Now suppose that Instagram allows someone to access your account without asking for a password or username. And this person stole your data, including your photos and other things. How do you feel after all this? It's not good? Some of them might even contemplate suicide. But "authenticity", a pillar of cyber security, seeks everything. Prevent unauthorized people and devices from accessing your information. This is only possible if people have access to your data.

5) **Reliability: _**

Non-repudiation is another important factor in ensuring that data is only sent to the sender. This ensures that the recipient of the message can also verify the sender. You can verify the sender and receiver by opening the logs provided by the information protection system. No

third parties can control the sending and receipt of your information by only two people can modify a sent message. To each other.
This example helps us better understand the second element of network security: nonrepudiation. You text me just because you want to chat with your friends on
. And the message will be sent to someone other than your
friends. Now you can imagine the importance of this pillar. This way your message will only be sent to your friends and no one else.
Second example Imagine you and your friend are talking and sharing your personal information
. : A third party suddenly appeared in the middle of the chat,
changed the information and could not send it to be friends.
Aren’t you mad? Non-repudiation will help
. This will prevent third parties from blocking the from sending or receiving data.
Let's look at a third example to help and understand other non-repudiation operations.
Suppose something happened to and now you want to get the sender data of Non-repudiation stores all the evidence of sender and message recipient. You can check it.
Thus, the principle of non-repudiation secures data in three ways.
Retention of proof of message sender and recipient.

➢ No third party controls the sending and receiving of data.

➢ Make sure the data is sent to the right person.

CHAPTER2:-RESEARCH METHODOLOGY

INTRODUCTION

A methodology is a systematic theoretical analysis of strategies applied in a field of study. It contains the theoretical analysis of the body of ways and concepts such as paradigm, theoretical model, phases and quantitative or qualitative techniques.

A methodology doesn’t started to supply solution it’s thus, not the same as a method. Instead a methodology offers the theoretical underpinning for understanding which method, set of methods or best practices can be applied to a particular case, for example, to calculate a particular result

.TITLE OF THE STUDY:-

The title of the study is: A Study of Cyber securities issues affecting in Online Banking and Online Transaction. Using Cisco Umbrella, the industry leader in threat detection,* to capture and analyse billions of queries, we identified the biggest cyber threats to businesses now.

PROBLEMS IN ONLINE TRANSACTION:

If your cyber securities are missing from your gadget, mobile or online application, you may encounter problems during online trading.
Transaction account requires two-factor authentication via incorrect password. This is why hackers cannot use them to hack your account and this is why online trading is a problem.
Expand online banking by closing commercial bank branches or shortening business hours separately from those who cannot use internet banking due to physical or mental limitations such as old age or illness.

RESEARCH METHODOLOGY RESEARCH DESIGN:

Research has tried to collect more and more relevant information with tools like Primary and secondary data collection methods. Primary data is original, collected by researcher through structured questionnaire used for the first time for any investigation and evaluated with the help of statistical analysis techniques. The primary data collection is made by personally visiting the colleges and academic institutes in the district. The sample of 91 respondents has been selected for the study.

Collection of secondary data is a purposive assembling of information relevant to the subject matter of the study from the units under investigation. Secondary data is collected by others and used by others. It is mostly published in newspapers, periodicals Journals and authentic websites etc.

Sources of Data:-

1) PRIMARY DATA:

Primary data is a type of data that is collected by researchers directly from main sources through interviews, surveys, experiment, etc. Primary data are usually collected from the source where the data originally originates from and are regarded as the best kind of data in research.

2) SECONDARY DATA:-

Secondary data is the data that has already been collected through primary sources and made readily available for researchers to use for their own research. It is a type of data that has already been collected in past. A researcher may have collected the data for a particular project, and then made it available to be used by another researcher. The data may also have been collected for general use with no specific research purpose like in the case of the national census. A data classified as secondary for a particular research may be said to be primary for another research. This is the case when a data is being reused, making it primary data for the first research and secondary data for the second research it is being use for.

The project is made from collecting both primary and secondary data. A major part of the study was primary backed by secondary data in the form of articles and data available on the websites and reference books.

PRIMARY DATA:-

The primary data has been obtained from the selected group of population with the help of questionnaire.

SECONDARY DATA:-

The secondary data has been obtained from published literature on the topic and from Research Journal, Research Articles, Thesis, Websites, and Newspapers.

Independent and Dependent Variables

Example:-

1) Let's look at an example of test results.

2) I would like to know how studying and sleeping affect my test scores.

3) In this example, "test result" is the dependent variable. Study and sleep are independent variables. Because these factors influence a student's performance on a test.

SAMPLE SIZE

Sample Decision Sample Size:-

Appropriate number of sample size (i.e., 91) was use for the purpose of collecting primary data from the selected population.

Sampling Method:-

Non- probability sampling design based on a convenient sampling method has been used for this research study.

Research Investment:-

A structured non- disguised questionnaire has been prepared to get the relevant information from respondents. Presented to the respondents for their response.

The collected information and primary data have been subjected to data analysis and interpretation. The collected primary data has been pre-coded considering the designing of the structured and non-disguised questionnaire.

The primary data has been scrutinized, edited and validated and thereafter it has been presented in the forms of data's, charts, graphs and diagrams.

OBJECTIVES:-

1) A study analysing categories of cybercrime in the banking sector 2)
A study on Investigations to investigate cybercriminal activity.
3) A study on Research to identify current cybercrime profiles.
4) A study on Surveys to provide instructions to follow as a victim of cybercrime.
5) A study on Suggests mitigations and security tips to control and curb cybercrime.

HYPOTHIES:-

Ho - No significant association between cybercrime category and banking sector.

H1- There is an important link between the cybercrime category and the banking sector.

H2- There is no significant connection between the current depiction of cybercrime and the banking sector.

H3- There is an important link between the technologies used by cybercriminals and the banking sector.

H4- No significant association between victims of cybercrime and the banking sector.

H5:- There is a link between controlling and deterring cybercrime, blocking factors and security tips related to the banking sector.

CHAPTER 3:- LITERATURE REVIEW:-

1) Rd. S. Natarajan.

Abstract:-

On November 8, 2016, the Government of India announced that the demonetization of online banking in India and the transition to online operations had revolutionized our overall business in the modern 21st century. The public consumes a lot of online transactions, and they suffer from cybercrime.

Cyber attackers perform cyber threats such as lending, credit granting and hacker attacks. Cybercrime defendants gained unauthorized access and compromised data and personal information. Some important methods are recommended here to protect against cyber-attacks.

2) Rd. Kamal Mohan Bansal.

Abstract:-

Cyber security issues affecting online banking are the subject of this survey. Due to the rapid development of this technology and the wide application of in many industries, cybercrime is on the rise. The online banking industry, made up of 4,444 different companies, faces cyber security and data breach challenges.

The study of many techniques and methods of creating complex software is facilitated by modern computer technology. Modern computer technology can solve problems that are difficult to solve by traditional computer methods in one step. They provide a new method for performing calculations. Modern computer technology is used to create specific types of computer security technology. Modern computer systems use various encryption strategies to solve network related problems. Today, mobile banking has also produced positive social effects in management, medical care, agriculture, education and other fields.

3) Rd. Menasha Giada*1, Mgrs. Saline*2 * 1Associate Professor, Department of commerce, IPS Academy, Indore, M.P. * 2 Research scholar, Department of commerce, DAVV, Indore, M.P.

Abstract:-

Cyber security issues affecting online banking are the subject of this survey. Due to the rapid development of this technology and the wide application of in many industries, cybercrime is on the rise. The online banking industry, made up of 4,444 different companies, faces cyber security and data breach challenges. The study of many techniques and methods of creating complex software is facilitated by modern computer technology. Modern computer technology can solve problems that are difficult to solve by traditional computer methods in one step. They provide a new method for performing calculations. Modern computer technology is used to create specific types of computer security technology. Modern computer systems use various encryption strategies to solve network related problems. Today, mobile banking has also produced positive social effects in management, medical care, agriculture, education and other fields.

4) ADITI SINGH Amity Law School, Noida B.A., LL.B (H) 2 ND Year, 4th Semester

Abstract:-

In the digital age, data plays an important role in our daily lives. It exists very clearly. The digital world has transformed our lives, creating new ways to communicate, organize and access information. It has also spawned new threats, often referred to as cybercrime, which are increasing dramatically every day. In response, cyberspace is increasingly seen as inherently dangerous. Need to verify more control and so on. Apart from various measures, cyber security remains a major concern for many at. In today's society where the Internet is ubiquitous, data protection has become the biggest challenge. This article examines why this framework itself poses a threat to the human rights and security of the digital environment. Finally, it will help to understand the main ways in which threats are posed in the cyberspace. Why this framework is problematic and how to engage in these debates. This article seeks to identify ways we can work with governments and citizens to protect and enhance these rights. It also focuses on modern and ethical technologies that are changing the face of cyber security. Keywords: cyber security, cybercrime, cyber ethics, cyberspace, data, digital, social media, government.

5) Dr. Aparajita Bhatt1:-

Abstract:-

Information technology has become one of the most important growth catalysts for sustainable economic development. Specifically, cyber security is considered one of the key factors for to ensure global sustainable development. Saw how cyber security and a safe and secure cyber environment are prioritized in the United Nations Sustainable Development Goals
(UNSDGs). Trust in cyberspace or ICT is essential to achieve the goals set in the United Nations Sustainable Development Goals. The absence of a secure cyberspace will make it difficult to achieve the Sustainable Development Goals.

The document highlights the role
that states, along with industry and other non-state actors, can play in ensuring better cyber security standards
as an enabler of sustainable development. Better policymaking, better tools and technology, better network architecture design, collaborative efforts of private groups such as industry
, media, civil society, and other national and international organizations can do more than just improve online safety and protect global security.

Vulnerabilities and Threats, but will also serve as an infrastructure to achieve Global Sustainable Development Goals.

6) Mrs Kalpana Nayar* Priyanka Rathod*

Abstract:-

The issue of cyber security is as central to our way of life as technology itself. In fact, they cannot be separated: our economic health, our national security, and indeed our social fabric are now defined by the technologies we rely on every day. Cyber security concerns our national security, our national interest and our economic prosperity. Cyber is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from Cybernetic, the Greek word for “helmsman" and "governor", which was first used in cybernetics, a term coined by Norbert Wiener. The virtual world of the Internet is called cyberspace, and the law governing this area is called Cyber Law, and all Internet users (citizens of the Internet) in this space fall within the scope of the Cyber Law because it is a universal jurisdiction network. A crime is defined as a crime in which a computer is targeted (hacking, phishing, spamming) or used as a tool to commit a crime (child pornography and hate crimes). Cybercrime can also be called computer crime. Cybercriminals can use computer technology to obtain personal information, trade secrets, or use the Internet for exploitative or malicious purposes. This research paper focuses on the cyber security issues facing Indian banks. It also helped analyse cybercrime awareness among 4,444 general citizens.

7) Giulia Napolitano:-

Abstract:-

Today, the growing sophistication and volume of cyber-attacks are forcing businesses to face tremendous pressure from internal and external threats, which affects day-to-day operations and
stakeholders' perceptions of the market, highlighting the importance of putting implement a strong security framework to counter these threats and ensure that data is safe and sound.

Indeed, while governments, agencies, businesses and other stakeholders should be concerned about cyber security investment strategies and their application to accounting, senior management still fails to consider the risks of cyber security
at board level and persists
in organizations Uncertainty about who is responsible for cyber security (ideally senior management). 4244 This study therefore aims to fill a gap in the literature and contributes to previous publications 4244 which provide insight into the impact of cyber security on management accounting, management, and auditing over time.

This examines how this technology informs practice by analysing existing research, from oldest to newest, and proposes a future agenda for fostering innovation in the field. Therefore, this study, through a bibliometric review of the cyber security literature, aims to quantify

research trends in publications and reveal valuable insights to scholars and practitioners in the area of interest.

8) Kristin YiJie Chen

Abstract:-

In the last few years, the concern over cyber security has grown dramatically. With all the existing, and sometimes competing, guidelines and frameworks intended to inform cyber risk strategies, organizations face the problem of deciding which is right for them. To resolve the confusion, this research proposes a practical and effective model that can be used by organizations of any size or in any industry for cyber risk management. We propose a Cyber Risk Cube (CRC) tool designed to be practical for all parts of an organization, which examines three fundamental pairings for looking at cyber risk: Internal/External, Measurement/Management, and Qualitative/Quantitative. The CRC tool can be used as a common language for sharing ideas and solutions to cyber risk management. Ultimately, the CRC provides details for implementing solutions to managing cyber risks in a concise and standardized manner.

9) Marinela Vrîncianu1⁎ and Liana Anica Popa2

Abstract:-

A large number of security breaches in electronic banking (e-Banking) systems are reported each year, drawing attention to the need to protect and inform customers of the risk of exposure to malicious acts by cybercriminals. Financial institutions and consumers are aware that attacks and financial fraud are increasingly sophisticated and perpetrated by different categories of criminals. This class is increasingly sophisticated and uses technology as part of its strategy. Additionally, experts

predict that the current global recession could increase the frequency of insider fraud and security breaches.

This study attempts to:

(1) Analyse the potential dangers that threaten the security of electronic banking services through a comprehensive review of the relevant literature.

(2) Identify tools and methods that can provide consumer protection in electronic banking.

(3) It present information on the results of a pilot study on consumer perceptions of consumer protection and electronic banking security
Services

Keywords: electronic banking, security, consumer protection, cyber-attacks.

10) <u>Zafar Kazmi</u>

Abstract:-

Internet banking has become one of the fastest and easiest way of banking. The threat of cyber security attacks set a great challenge for the Internet banking and electronic commerce (E-commerce) industries. In this paper, we first analyses in detail the cyber security of Internet Banking in Emerging Countries and then propose a novel model to reduce the cyber security risk to bridge the gap between banks
And customers. The proposed model is based on results of surveys conducted on Internet banking in three emerging countries (Saudi Arabia, Pakistan and India). The survey focused on users practices in Internet banking. The questions were based upon user's knowledge about cyber security and user's awareness of common threats in Internet Banking. The results obtained support the argument that there is an emerging gap between banks expectation and user actions related to Internet banking. The proposed model bridges
The gap taking into account user's IT literacy and IT equipment (Hardware and Software) increasing the responsibility of banks to reduce the cyber security risks for users.

CHAPTER 4:- DATA ANALYSIS INTERPRETATION AND PRESENTATION.

Businesses are more vulnerable to cyber-attacks than ever before. However, calculating this risk is not simple. This article provides an overview of traditional computational methods and a glimpse into the future of cyber security risk measurement: statistical analysis.

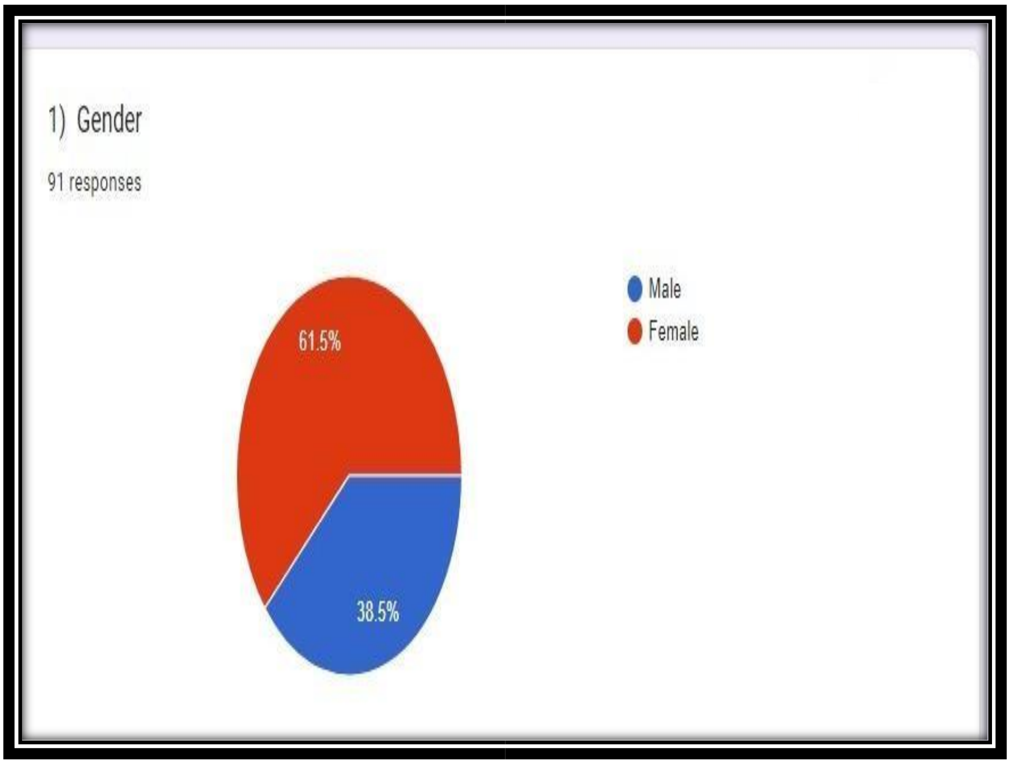
The cost of cyber-attacks is very high, and in some cases it can be so high that it completely cripples your business. A 2020 study found that cybercriminals lose $2.9 million per minute and the average cost of a data breach in 2021 is $4.24 million.

One of the largest financial services providers in the United States, Flagstar Bank, suffered a massive data breach in June 2022 that leaked the social security numbers of nearly 5 million customers. This is the second attack against the Michigan-based online banking giant in as many years.

Currently, many service providers use cyber security frameworks such as the National Institute of Standards and Technology (NIST) framework. To meet regulatory requirements such as the General Data Protection Regulation (GDPR).

A cyber security risk is the chance that an organization will experience data, financial, or operational disruption. This type of risk is often related to events that can eventually lead to a data breach. Vulnerabilities, ransom ware, phishing, distributed denial of service (Dodos) and malware are the most common cyber security threats.

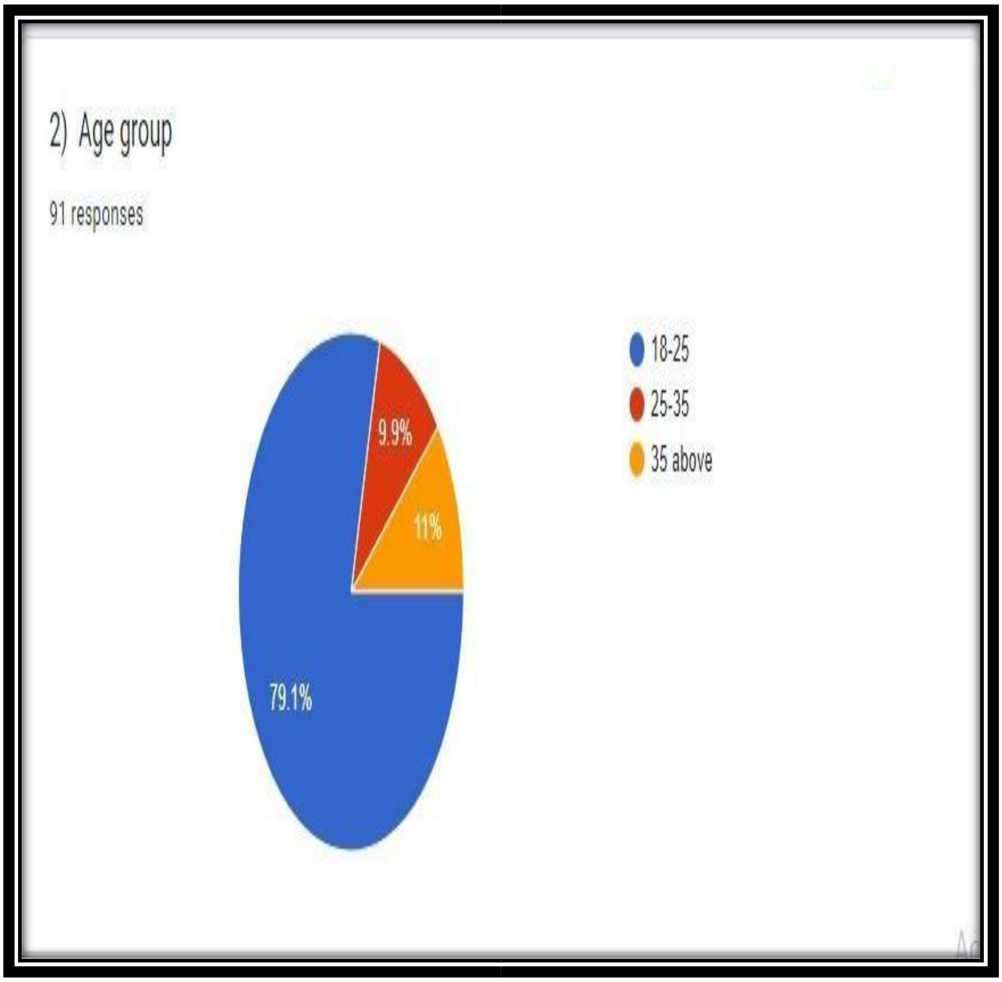
RESPONSES:-



GENDER	PERCENTAGE
FEMALE	61.5%
MALE	38.5%

1) Interpretation:-

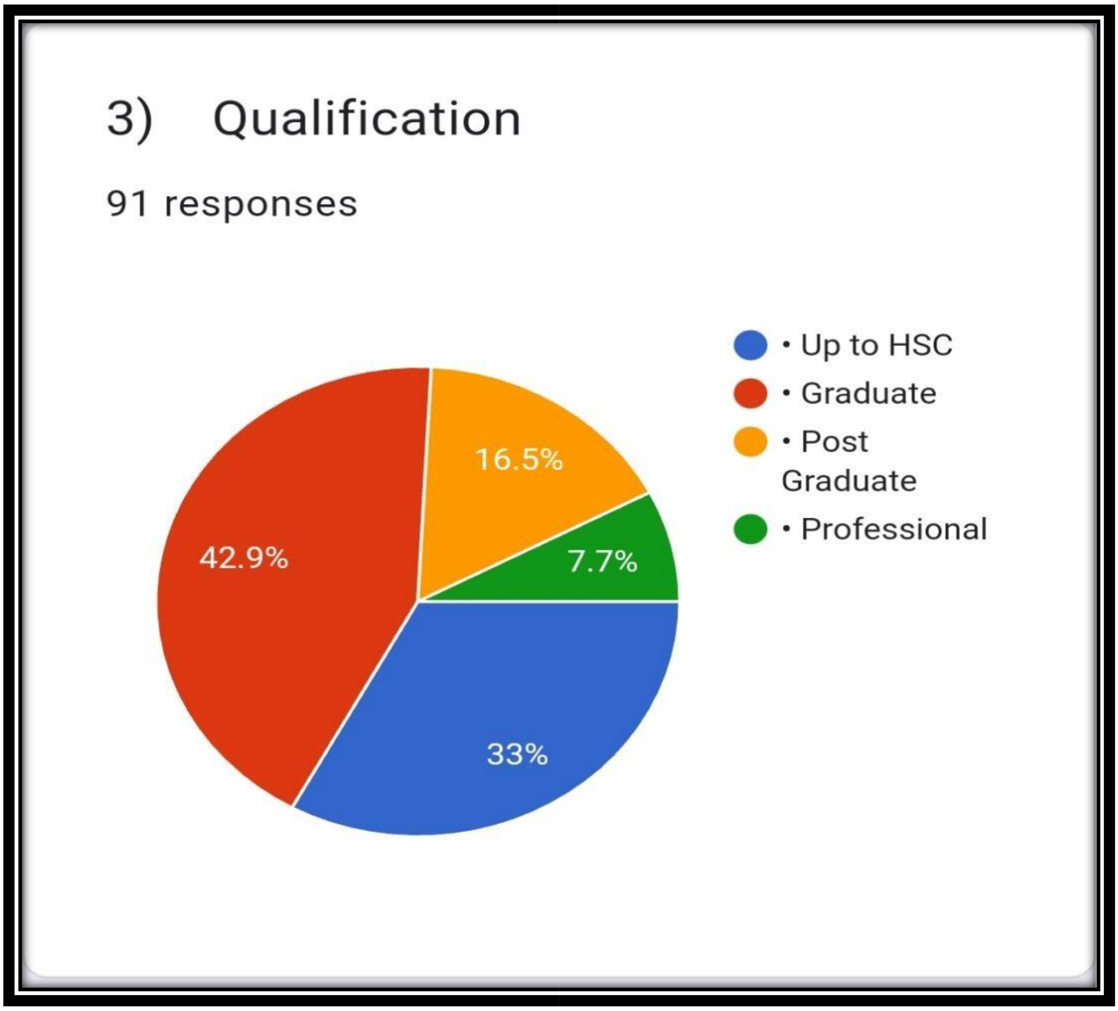
The above data show information about gender of the respondents, as we can see 38.5% of respondents are male and 61.5% respondents are female. Majority of respondents are female.



NUMBER	AGE	PERCENTAGE
1)	18-25	79.1%
2)	25-35	9.9%
3)	35 above	11%

2) <u>Interpretation:-</u>

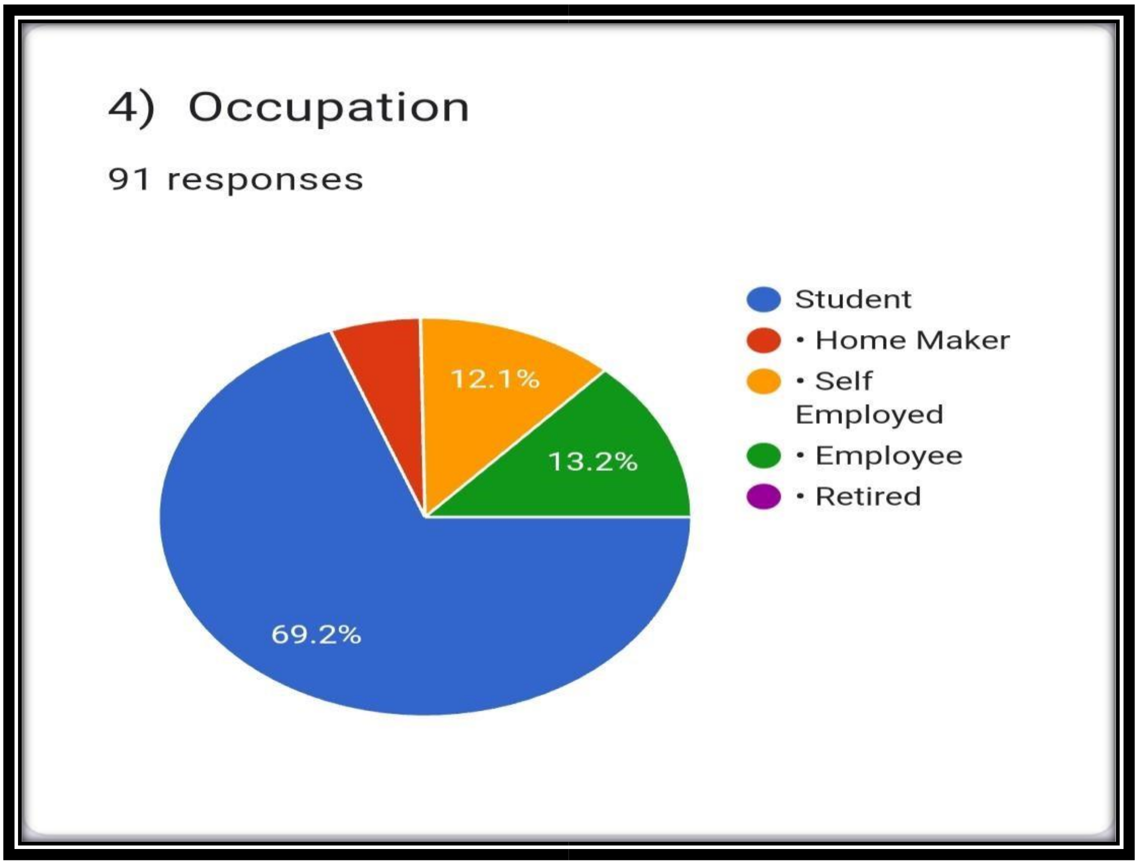
In the above data we can see that 79.1% of respondent are below the age of 18-25, 9.9% of respondents are between the ages of 25-35 years, 11% of respondents are the age of 35 above years. The majority of respondents are between the ages of 18-25 years.



NO. SR.	QUALIFICATION	RESPONSE PERCENTAGE%
1)	UPSC TO HSC	33%
2)	GRADUATE	42.9%
3)	POST GRADUATE	16.5%
4)	PROFESSIONAL	7.7%

3) Interpretation:-

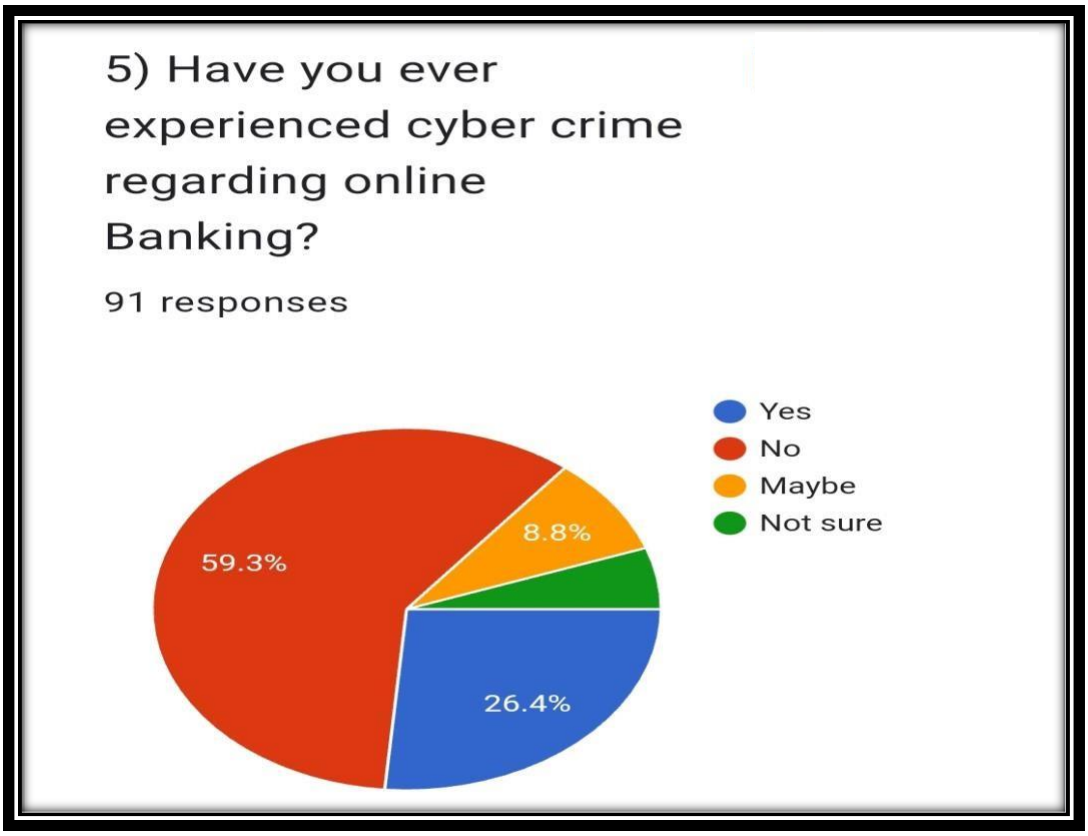
In the above data, information related to qualification of respondents is given 33% to upsc to hsc, 42.9% belongs to the graduate, 16.5% of the respondents have their post graduate and 7.7% respondents have their professionally qualified.



NO. SR.	OCCUPATION	RESPONSE PERCENTAGE%
1)	Student	69.2%
2)	Home maker	6.1%
3)	Self-Employee	12.1%
4)	Employee	13.2%
5)	Retired	Nil

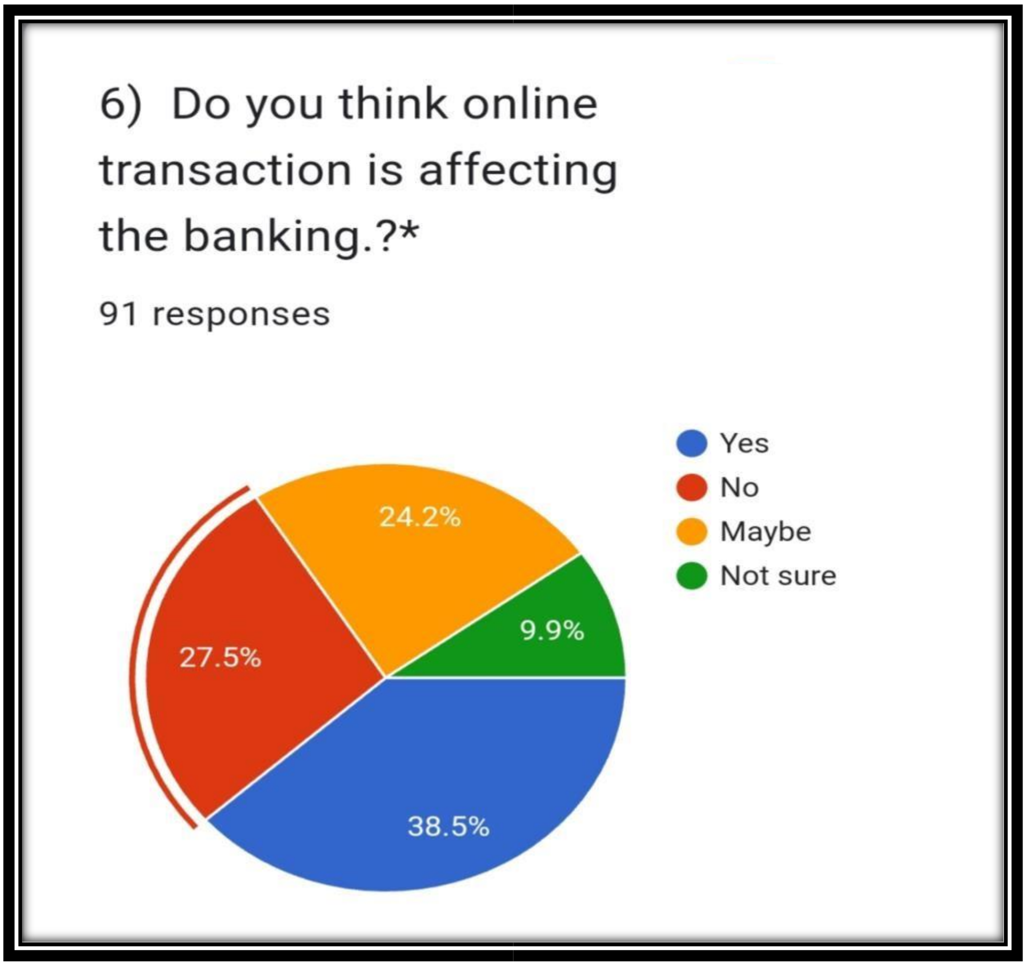
4) <u>Interpretation:-</u>

In the above data, information related to occupation of respondents is given 69.2% of respondents are student, 6.1% there are home maker, 12.1% of respondents are Self-employed ,13.2% belong to the employee category, and 0% respondents are retired.,



5) **Interpretation:-**

The response are is show that the 26.4% people have experienced in cybercrime regarding online banking, due to improper securities. 5.95 people didn’t have any experience I cybercrime, 8.8% people are maybe had experience in cybercrime 5.2% people are not sure.

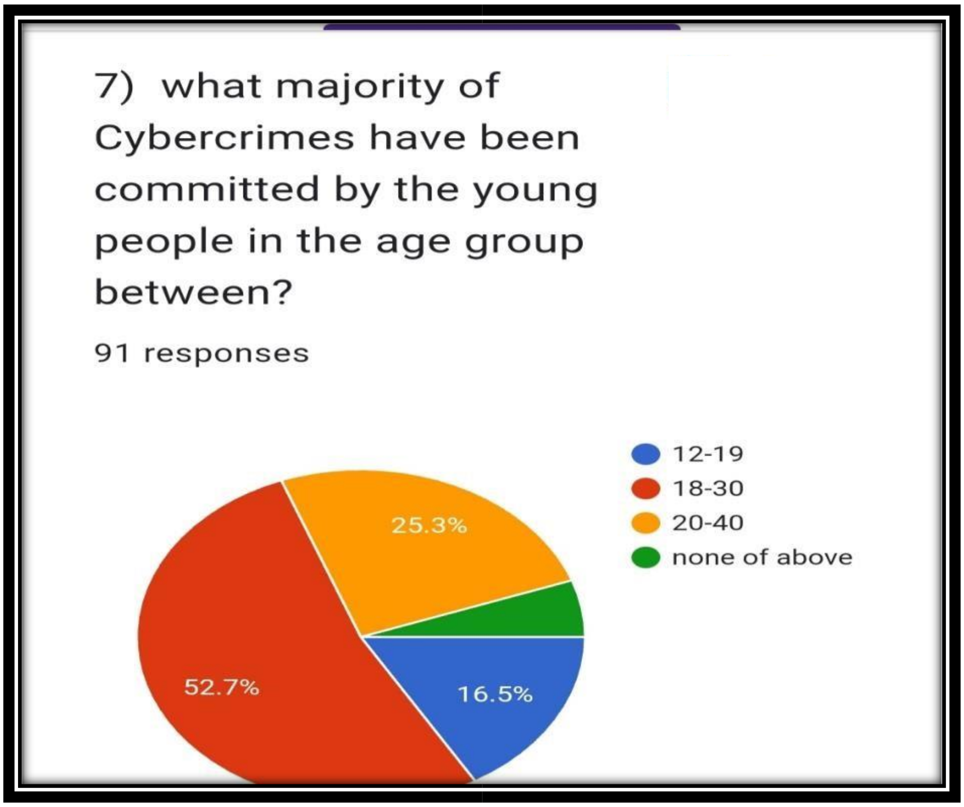


6) Do you think online transaction is affecting the banking.?*

91 responses

6) <u>Interpretation:-</u>

In this chart 38.5% people are known that in online transaction affect in online banking, 27.5% people think no they don’t affect while transact your money in particular bank. 24.2% of people think average it maybe be affect or it cant be affect, 9.9% people are not sure.

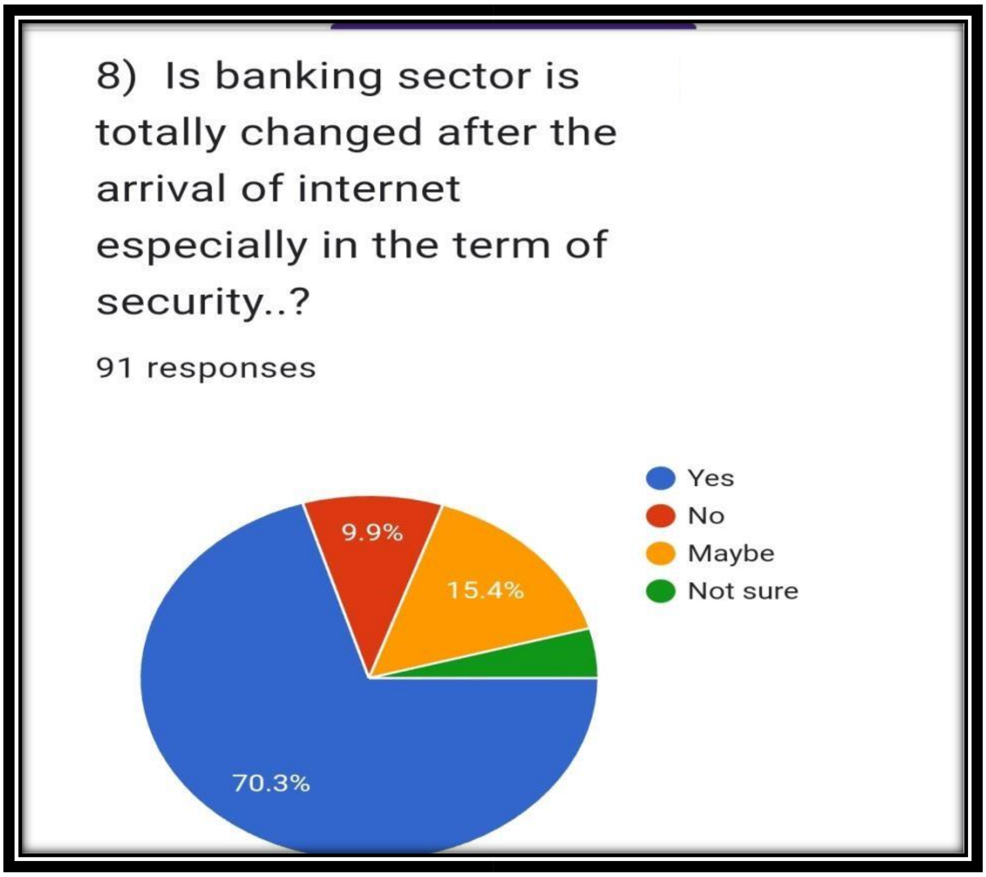


7) what majority of Cybercrimes have been committed by the young people in the age group between?

91 responses

7) Interpretation:-

The people of age group 12-19, 16.5% the cybercrimes have been committed in the age group 18-30 there were 52.7% cybercrimes have been committed due to poor securities. In the age group of 20-40 there are 25.3% committed in cybercrimes. Majority the age group of 18-30 people have committed the cybercrimes.

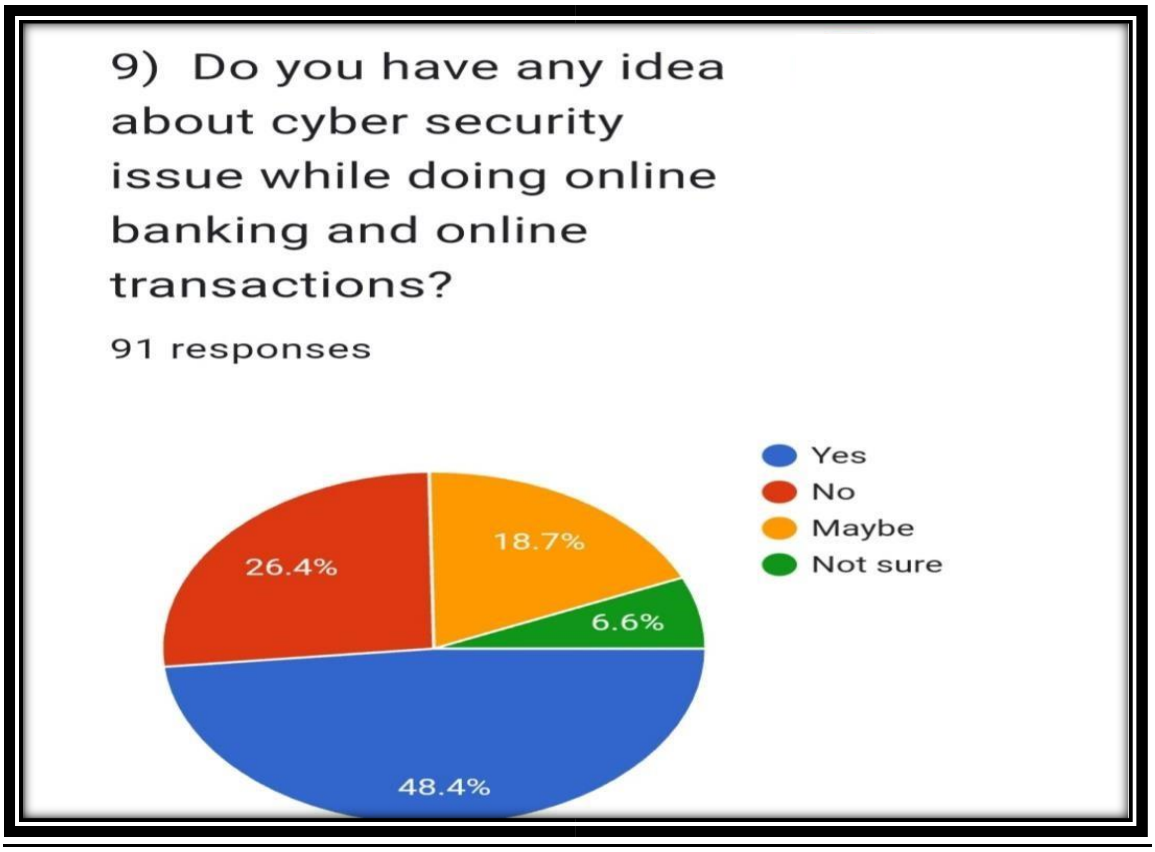


8) Is banking sector is totally changed after the arrival of internet especially in the term of security..?

91 responses

8) <u>Interpretation:-</u>

In this chart 70.3% people think that the banking sector is totally changed, after the arrival of internet 9.9% people think no. Maybe 15.4% of people think that their maybe be changes in banking sector. Majority people are saying yes because, nowadays securities are useful for us due to avoid any blockage in account.

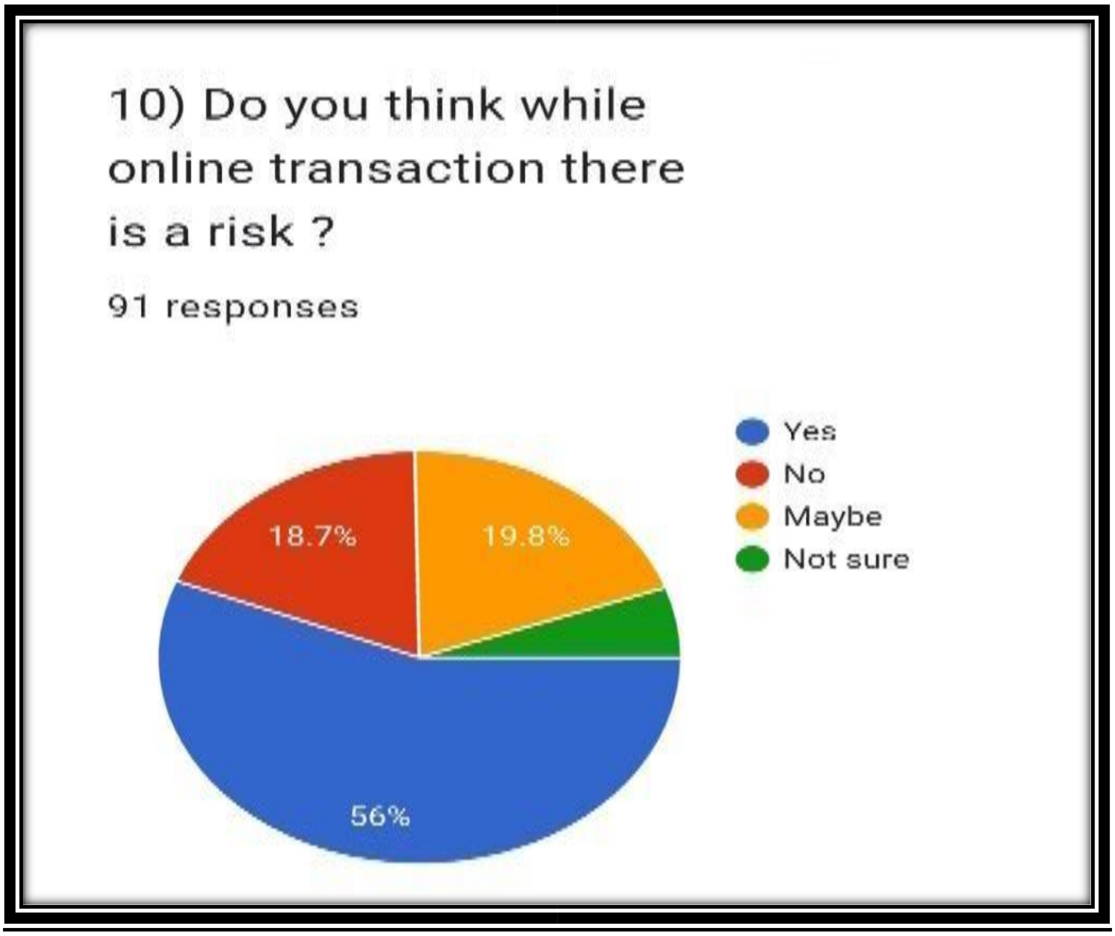


9) Do you have any idea about cyber security issue while doing online banking and online transactions?

91 responses

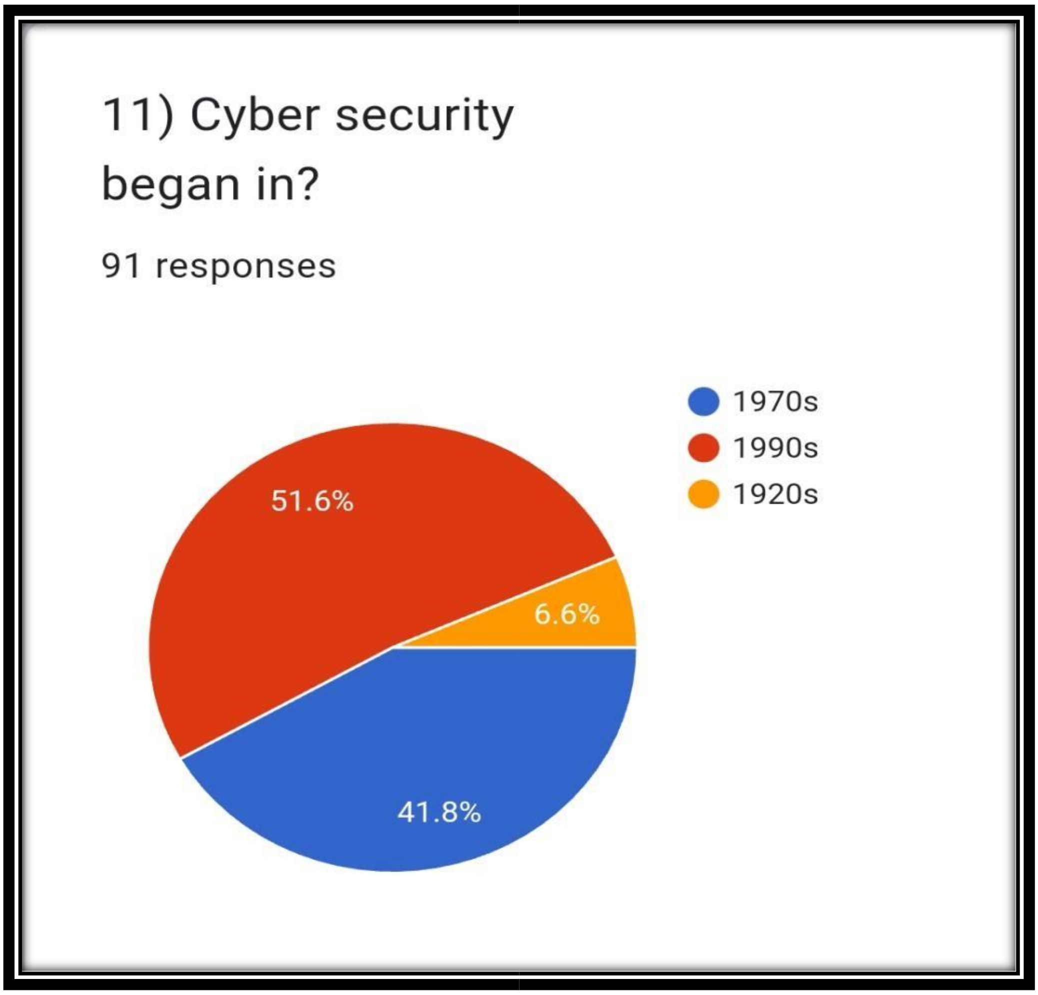
9) <u>Interpretation:-</u>

In this chart 48.4% people have idea about cyber security, the 26.45 of people don’t have any idea about cyber security, 18.7% people maybe have idea and 6.6% people are not sure. Majority people have idea about cyber security which is issue in doing online banking and online transaction.



10) Interpretation:-

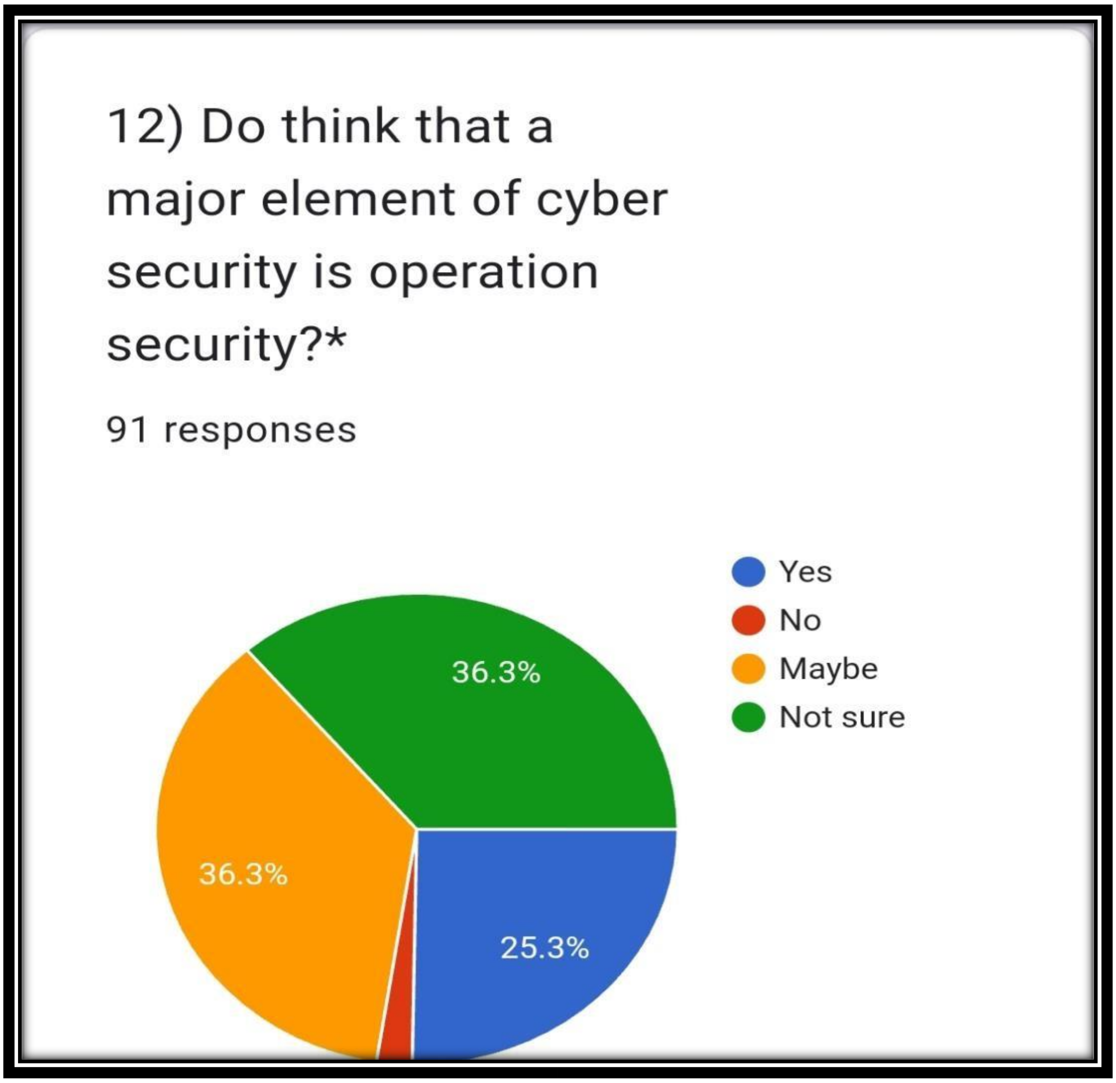
In this pie chat 56% of people think there is a risk while online transaction because, some people five there password, OTP , etc. were the hacker can hack your account to that's why the cyber securities are used to avoid risk. 18.7% people don't think there are risk, 19.8% people think there maybe the risk 5.2% people are not sure.



.

11) <u>Interpretation:-</u>

In this chart 41.8% people have respondent that in 1970s cyber security began, 51.6% people have respondent 1990s 6.6% of people have responses 1920s. Majority 51.6% people have respondent 1990s cyber security began.

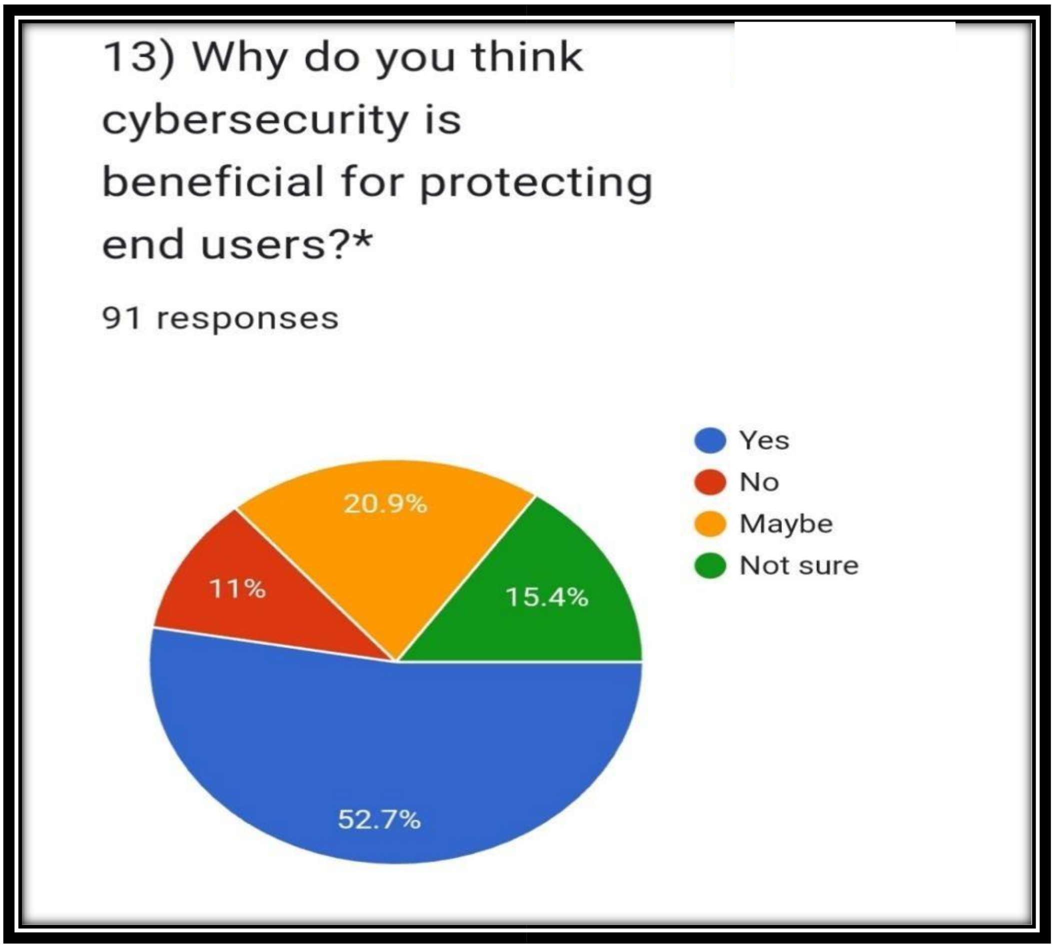


12) Do think that a major element of cyber security is operation security?*

91 responses

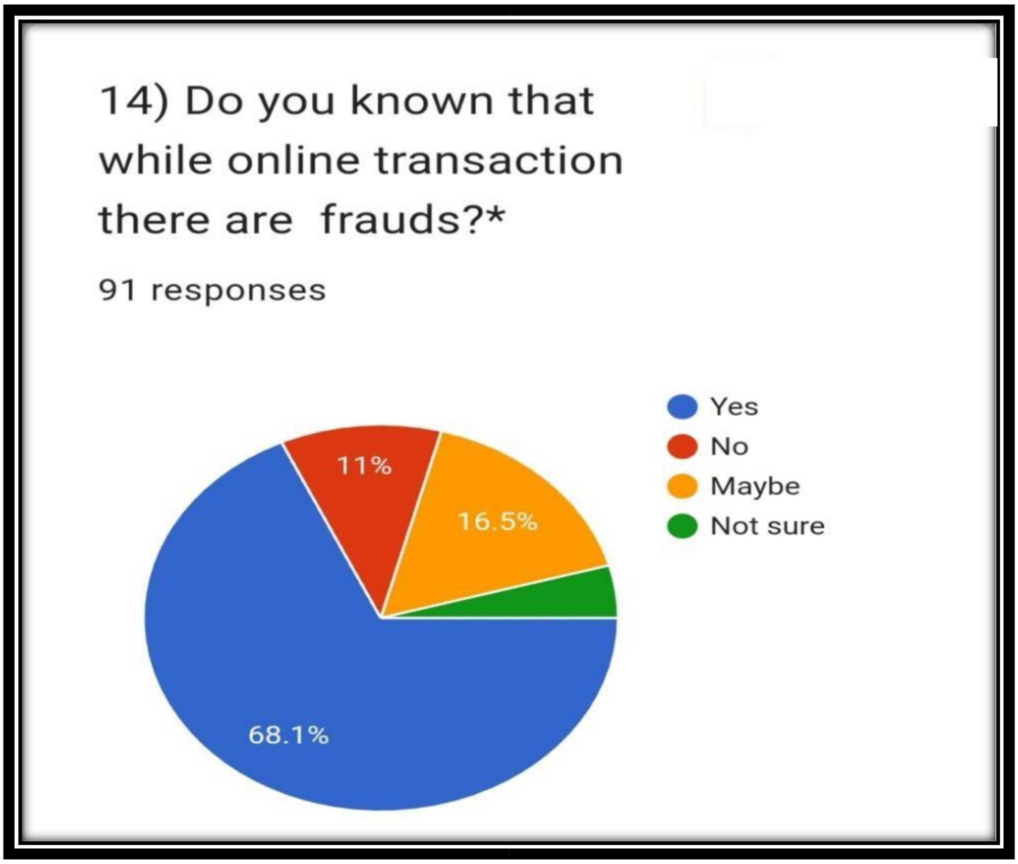
12) <u>Interpretation:-</u>

In this chart 25.3% people think that major element of cyber security is operation security Operational Security is a risk management methodology that promotes the visualization of operations from an adversary's perspective. 2% people think no 36.3% people think maybe and 36.3% people are not sure .Majority people maybe think element of cyber securities is operational security.



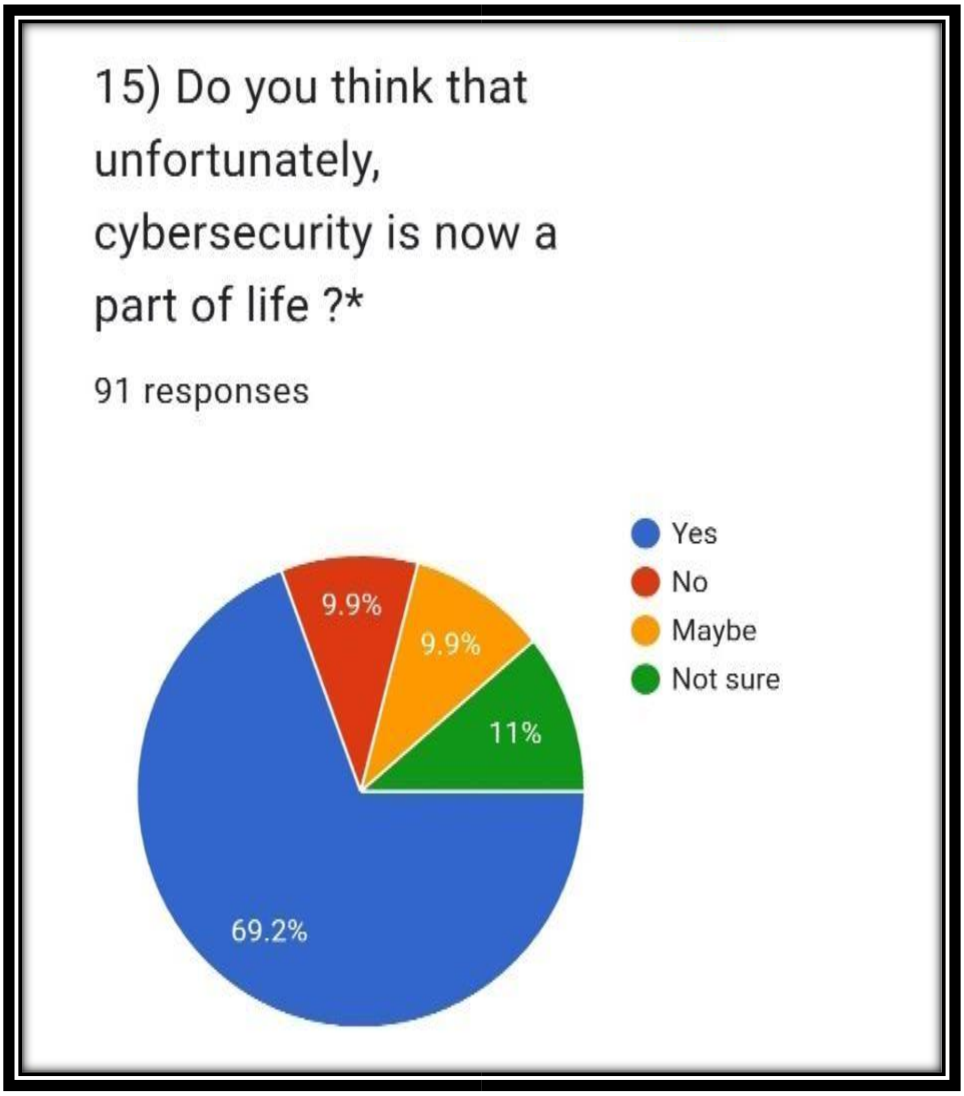
13) <u>Interpretation:-</u>

In this chart 52.7% of people think cyber securities is beneficial for protecting end users. Using password to protect your account two step verification, 11% of people think no it is not beneficial 20.9% people think maybe it is beneficial to protecting end users. 15.4% people are not sure.



14) Interpretation:-

In this chart 68.1% people know that while online transaction there are frauds, 11% people think there are not frauds, 16.5% people maybe know there are frauds If you share your password or OTP to some person so they can hack and take the money from your account that’s why while online transaction there are frauds.

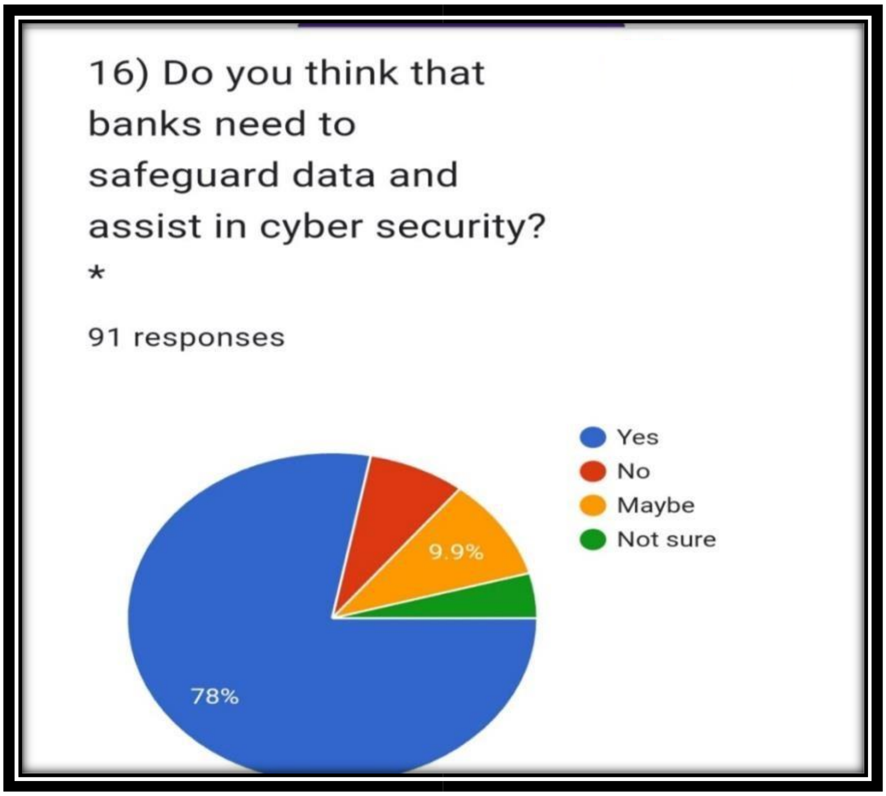


15) Do you think that unfortunately, cybersecurity is now a part of life ?*

91 responses

15) **Interpretation:-**

In this chart 69.2% people think that, unfortunate cyber security is now a part of life, 9.9% people think no, 9.9% think maybe and 11% of people are not sure. Majority people think it is very useful for us in nowadays.

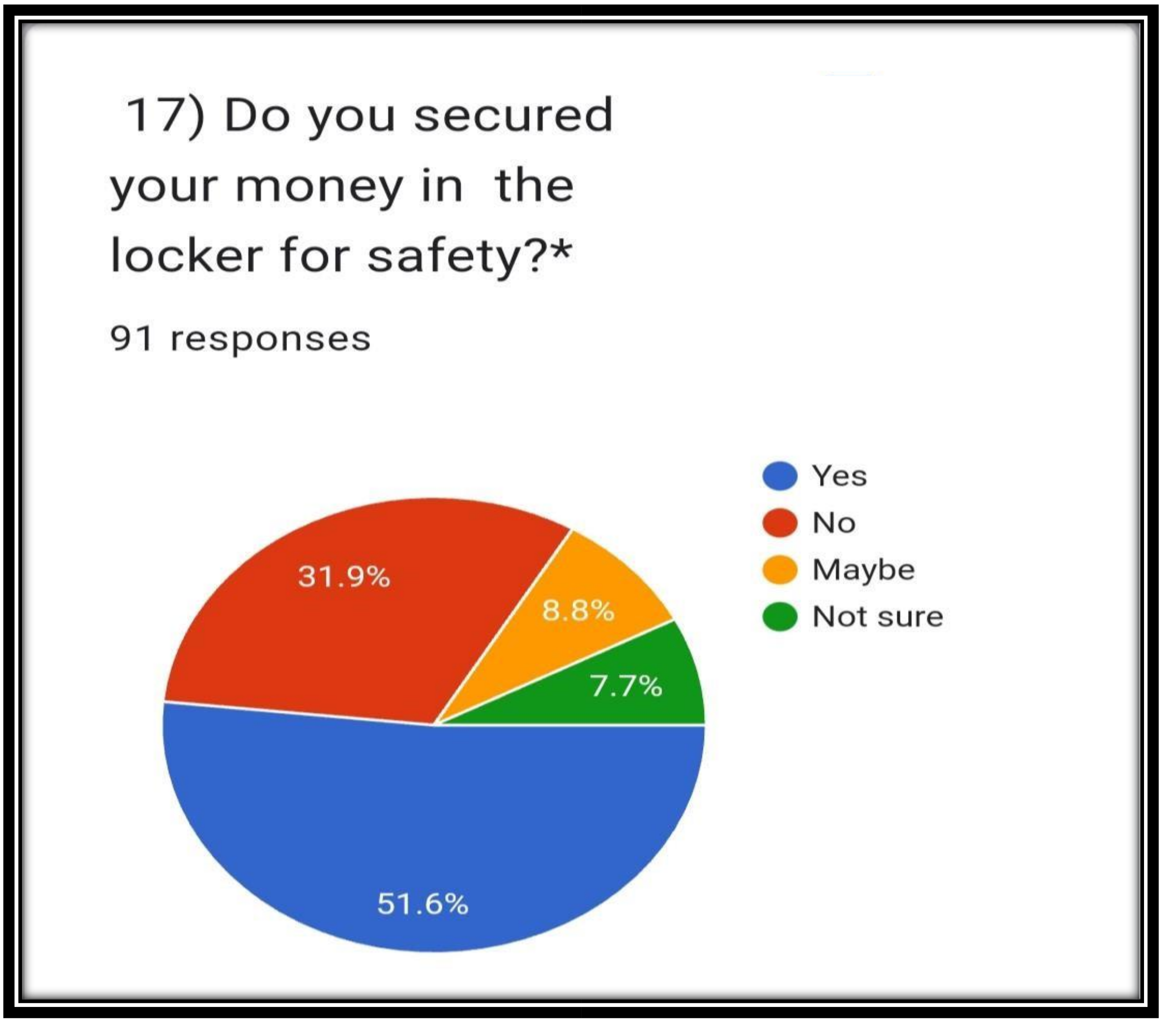


16) Do you think that banks need to safeguard data and assist in cyber security? *

91 responses

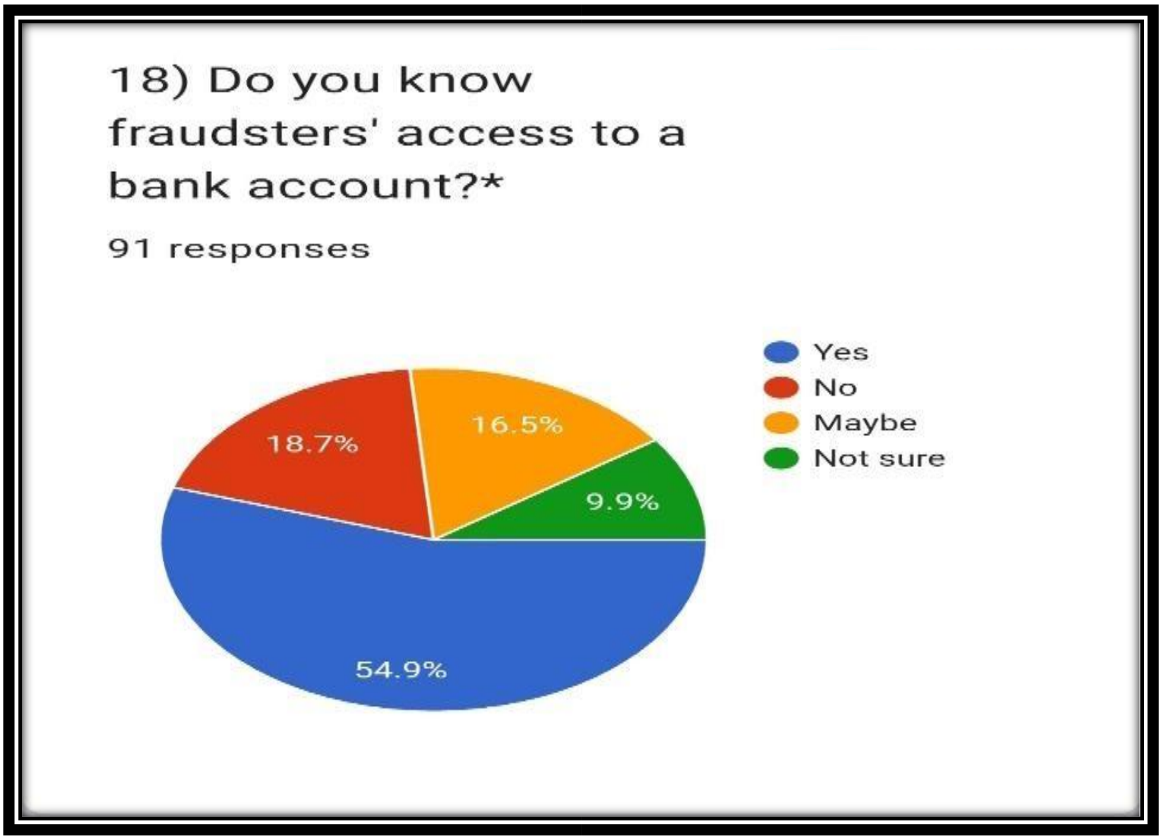
16) <u>Interpretation:-</u>

In this chart 78% people think that banks need   to safeguard data and assist in cyber security, 9.9% people think maybe assist in cyber security.



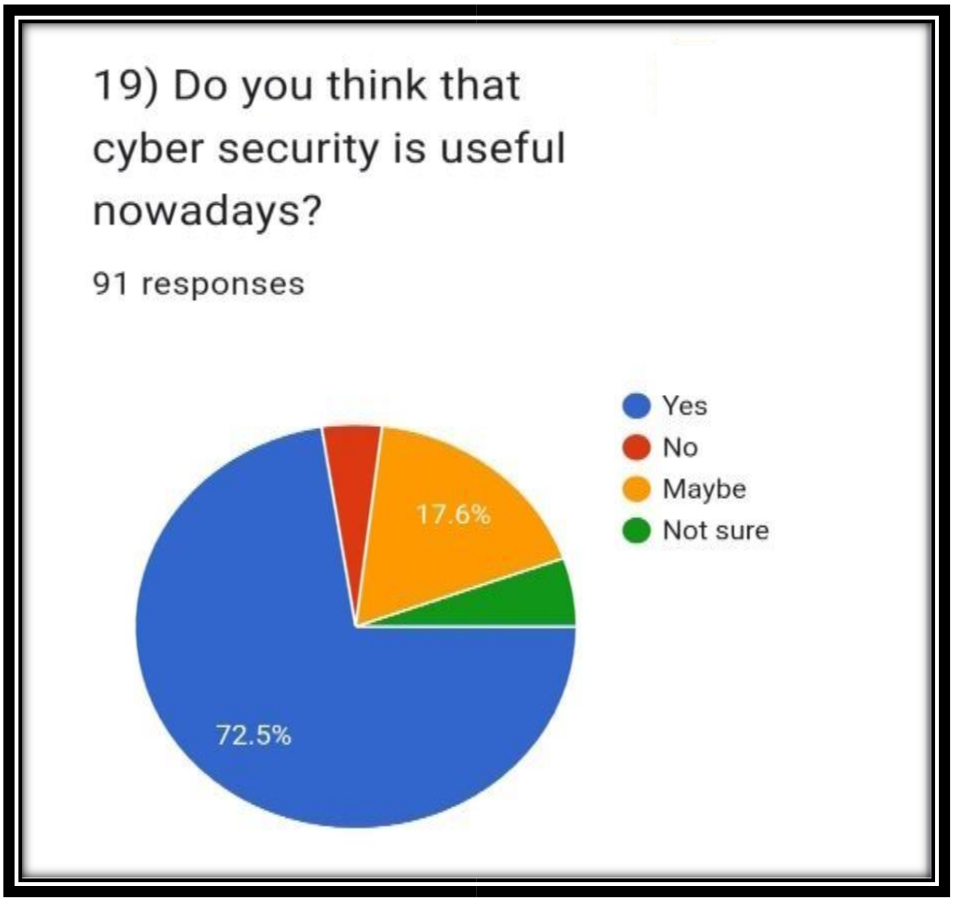
17) Interpretation:-

- More than 50% of people still fills that hard money to be secured in the locker.
- Nearly 30% of people feels that money keeping in locker is not needed.
- Nearly 20% of people are not sure.



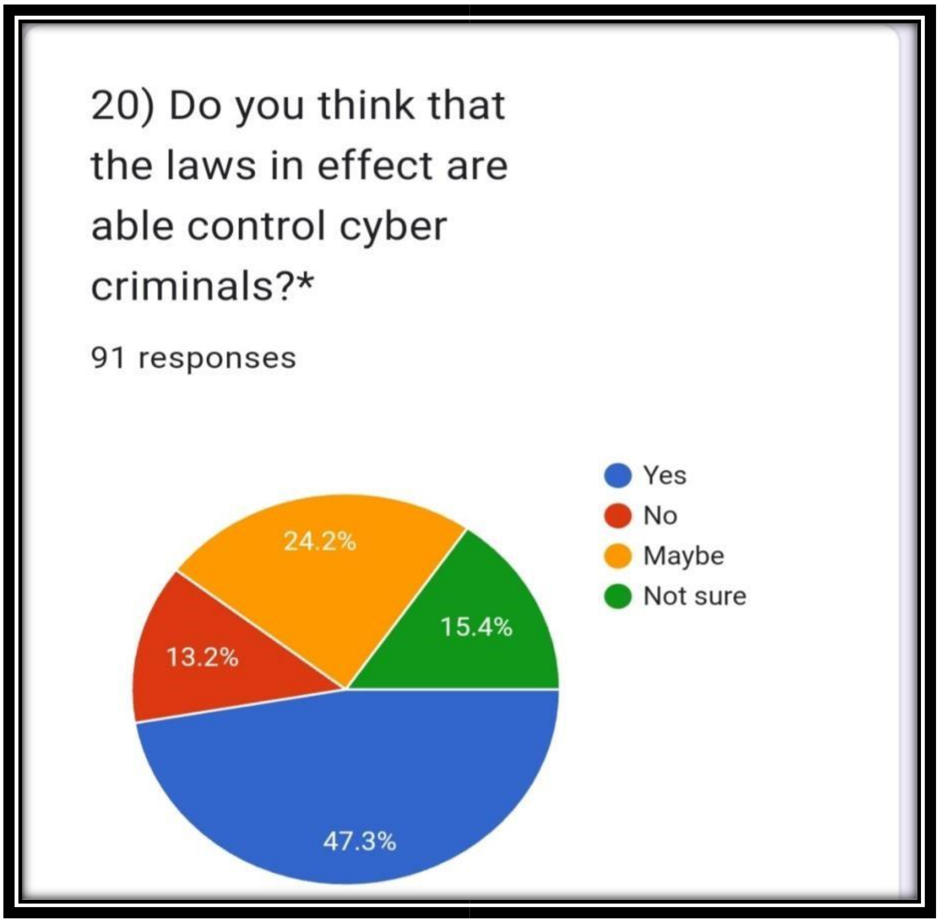
18) **Interpretation:-**

- Glad to see more than 54% people aware about fraud access of bank
- Rest 50% people has mixed reaction.



19) <u>Interpretation:</u>

- As we are the biggest country doing online transaction, it’s good to see more than 72% people know the significance of cyber security.

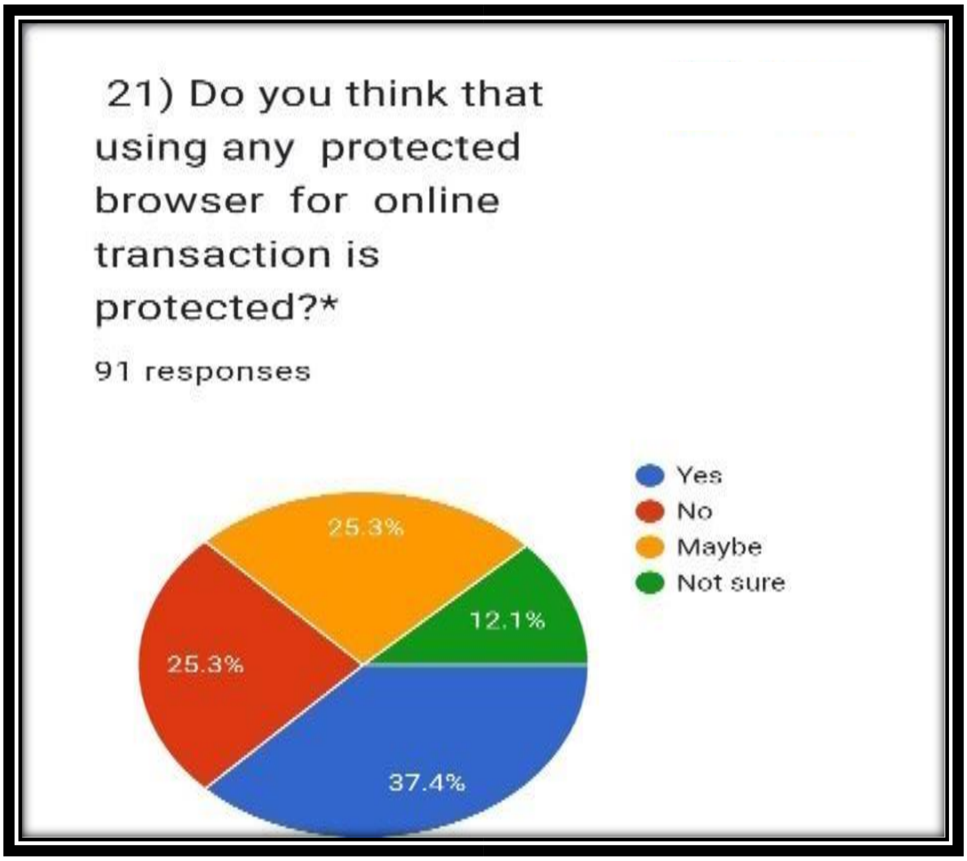


20) Do you think that the laws in effect are able control cyber criminals?*

91 responses

20) Interpretation:-

- Only 47% people are confident that law of cyber control are effective, means still we need to strengthen cyber law to gain other’s confidence as well.

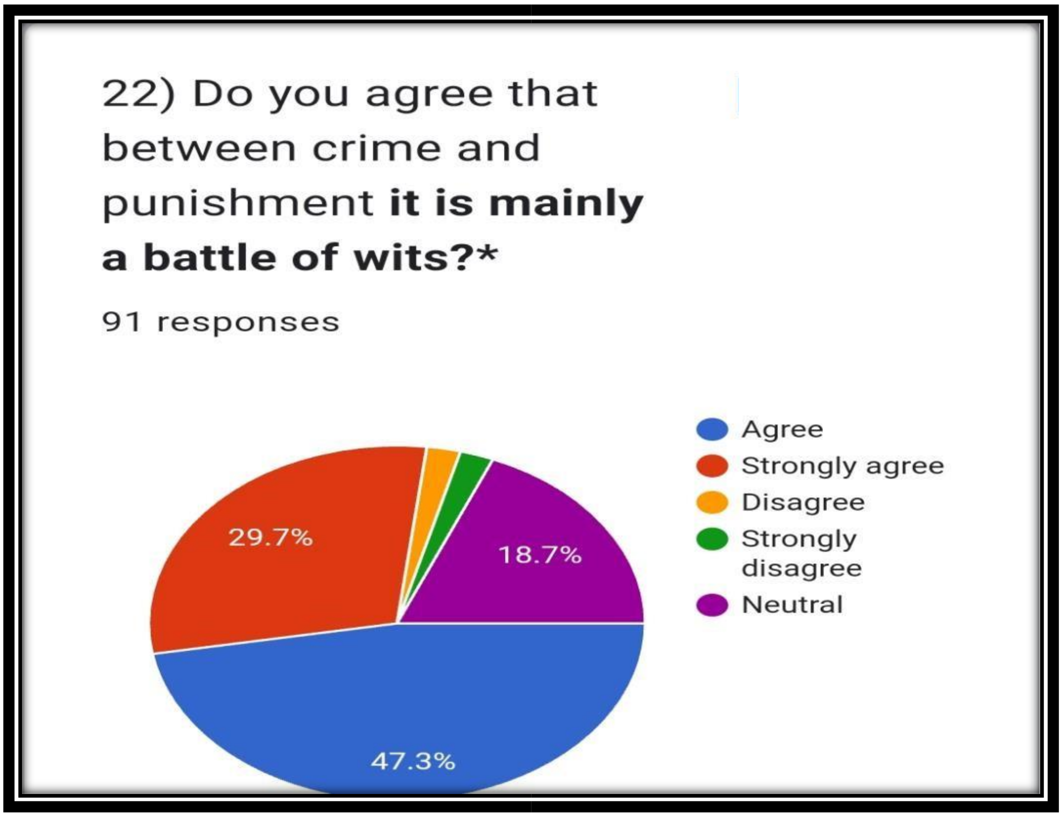


21) Do you think that using any protected browser for online transaction is protected?*

91 responses

21) <u>Interpretation:-</u>

- Mixed reaction for browser protect, means protection must be enhanced and awareness of protection to be created.

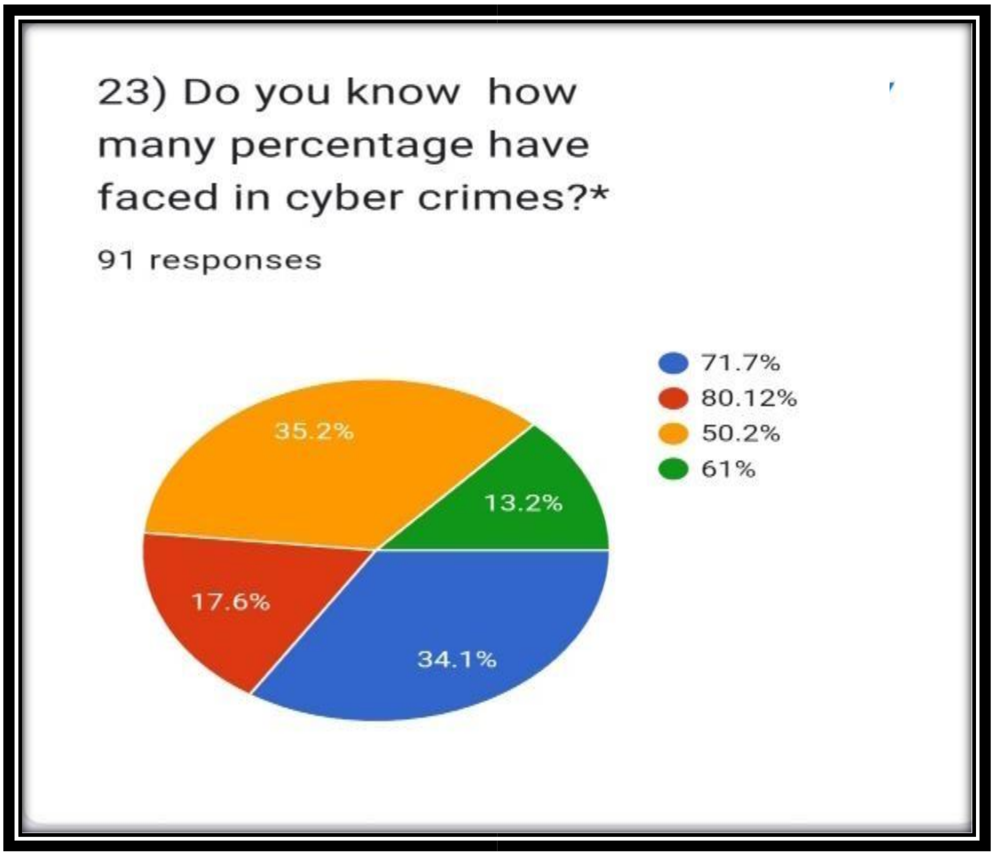


22) Do you agree that between crime and punishment **it is mainly a battle of wits?***

91 responses

22) Interpretation:-

- Nearly 50% people feels that crime and punishment is battle of dealing each other.



23) Do you know how many percentage have faced in cyber crimes?*

91 responses

23) <u>Interpretation:-</u>

- Nearly 34% of people think that 71.7% percentage have faced in cybercrimes.
- As 65% of people think that there may be 80.12%, 50.2% or 61% faced in cybercrimes.

FINDINGS

Cyber security impacts all ICT areas. Below we consider the CONCORDIA taxonomy of domains. Iota, edge computing, and smart devices are changing the environment in many ways, including smart transportation, sustainable mobility, smart cities, e-health, smart vehicles, and UAVs. The exponential growth of connected devices (from small sensors to larger machines), expected to reach 200 billion by 2020, according to Intel [2], is revolutionizing today's IT systems. The existence of billions of Internet-connected devices with limited resources poses fundamental risks that can threaten users' lives and privacy.

Network-Centric Security: Traditional network environments are characterized by welldefined boundaries and trusted domains. The network was originally designed to create internal segments separated from the outside using fixed boundaries. Internal networks were classified as trustworthy, while external networks were classified as potentially hostile. Perimeter devices such as firewalls and intrusion detection systems are traditional technologies used to protect networks.

System-Centric Security: The term "system" is synonymous with an operating system (OS) or, more generally, software that enables applications to take advantage of the computing connectivity and storage capabilities of hardware. Often used as Operating systems have historically been prime targets for many devastating attacks (e.g. IIS buffer overflow Code Red to exploit, Sesser to target the Local Security Authority Subsystem Service, Shakos Linux server rootkit). Features such as authentication. Nonetheless, operating systems will continue to play an important role as they become integrated into increasingly complex environments (e.g.

Mobile devices, virtualized systems, etc.),

Data-Centric Security: The ability to quickly and remotely share, manage, distribute and access data is the cornerstone of the digital revolution that began decades ago. The role of data in today's technology has become even more important after entering the so-called datadriven economy. Data management and conclusions based on it are fundamental to any business, from small to large enterprises. In addition, data management allows businesses to remain competitive in the evolving global marketplace. The data domain observed important changes at all layers of an IT chain: I) data layer: from data to big data, ii) database layer: from SQL to Nosily, iii) platform layer: from the data warehouse and DBMS to Big Data platforms, IV) analytics layer: from data mining to machine learning and artificial intelligence. For example, data mining focuses on discovering unknown patterns and relationships in large data sets, whereas machine learning focuses on discovering patterns in data by learning pattern parameters directly from data.

.RECOMMENDATION

Tip #1 – You Are Targeted by Hackers

Never say things like ``this is not going to happen to me" about your reputation and the reputation of the university.

Cyber security is everyone's responsibility.

By following these tips and staying vigilant, you can do your part to protect yourself and others.

Tip #2 – Keep Your Software Up to Date It is very important to install software updates for your

Operating system and programs. Always install the latest security updates on your device:

Enable automatic operating system updates.

Use a web browser that receives regular automatic security updates, such as Chrome or Firefox.

Please keep your browser plugins (Flash, Java, etc.) up to date.

Tip #3 – Avoid Phishing Scams – Beware of Suspicious Emails and Phone Calls Login IDs and passwords, bank or credit card details.

Phishing scams can be carried out via phone, SMS, or social media, but email is the most common.

Be suspicious of official-looking e-mail messages or phone calls requesting personal or financial information. For more information on how to identify and protect yourself from Phishing scams, see our Phishing Resources section.

Tip #4 – Practice Good Password Management

There are too many passwords to manage. B. Reusing the same password. A password manager helps you maintain strong, unique passwords for all your accounts.

FURTHER SCOPE OF RESEARCH

Cyber security is an integral part of any business or enterprise worldwide, so the scope of cyber security is immense.Cybersecurity protects devices, programs, and data from damage, attacks, and other unauthorized access. Technologies, processes and practices designed to protect. Cyber security, also known as information technology security, focuses on protecting computers, applications, systems, and networks from unauthorized access, tampering, or destruction. The former component is a fundamental component of any business, so you can imagine what the scope of cyber security would be.

Many licensed agencies, such as armed forces, government agencies, financial institutions, and the banking sector. Store sensitive information on your computer and send it over the network. With the increase in cyber-attacks, it becomes necessary to protect this sensitive data and personal information. To do that, we need thousands, if not millions, of cyber security experts.

Why do we need cyber security in today's world?

Cybercrime is he one of the fastest growing crimes in the world today. This is mainly due to the increase in information leaks on the Internet through cloud services. Networks and devices that manage your infrastructure can be disrupted at scale. The sole goal here is not to stop identity theft, but to protect data integrity. As cybercriminals become more sophisticated, we need to understand how their goals are changing, how they impact organizations, and what methods they use in their attacks. .

Social Engineering – Social engineering is the most common and easiest cyber-attack. Phishing and ransom ware are the simplest forms of network intrusion.

LIMITATION OF YOUR RESEARCH

1) Configuring a firewall properly can be difficult.

2) Improper firewall settings can prevent users from performing certain actions on the Internet until the firewall is properly configured.

3) The system is slower than before.

4) You need to keep updating new software to keep your security up to date.

5) Can be costly for the average user.

CHAPTER 5:- CONCLUSION AND SUGGESTION:-

Organizations must respond quickly to the dynamic growth of cyber security threats. Because attackers use the attack lifecycle, organizations must also develop a vulnerability management lifecycle. The vulnerability management lifecycle is designed to respond to attack attempts as quickly and efficiently as possible. In this chapter, we discussed the vulnerability management lifecycle in relation to vulnerability management strategies. This includes asset registry setup, information flow management, risk assessment, vulnerability assessment, and reporting and remediation procedures. Neural networks and artificial intelligence are two examples of modern computing approaches that provide many powerful tools for addressing enterprise cyber security challenges. Phishing attacks, Dodos attacks, ransom ware attacks, and many other cyber security issues have compromised networks and systems. State-of-the-art computational methods simplify and a accelerate cybercriminal detection, and 7738 Rd. Kamal Mohan Bansal Cyber security Issues Affecting Online Banking: A Case Study of Protecting Data from Cybercriminals Compared to Traditional Computational Methods. Cloud Security protects sensitive data. Currently, artificial intelligence and machine learning can help businesses protect their data from virus attacks. This study showed how artificial intelligence counters cyber threats with the help of DL and DNN. It is believed that AI will dominate all fields in the near future. Every organization is concerned about cyber security.

SUGGESTION

1) World has changed very fast and we all are doing maximum soft transaction compare to hard transaction.

2) So it is very important for us to secure our all online transaction.

3) In case we do or we have hard money, Jewellery, property paper etc., we must keep them in the bank locker rather than keeping it in our house and increase risk of life.

4) India has become world’s no’ 1 in online transaction, so possibility of cyber- crime also increase. Hence we all need to ensure safe and secure online transaction by using authorised websites, not to share log-in credentials, change password frequently, not to share any opt with any one.

5) In my opinion, In case of any cyber -crime happen with you weather if is small or big, you must report to cyber cell.

6) Do online, keep online and live safe life.

CHAPTER 6:-BIBLOGRAPHY

(1) Due, M., Hit, L.M. and Chen, P.Y., 2011. Determinants and outcomes of internet banking adoption. Management Science, 57(2), pp.291-307.

(2) Akola, M.A., 2011. Internet banking in Pakistan: finding complexities. Journal of internet banking and Commerce, 16(1), p.1.

(3) Cheung, R. and Vogel, D., 2013. Predicting user acceptance of collaborative technologies: An extension of the
Technology acceptance model for e-learning. Computers & Education, 63, pp.160-175.

(4) Martins, C., Oliveira, T. And Popover, A., 2014. Understanding the Internet banking adoption: A unified theory of
acceptance and use of technology and perceived risk application. International Journal of Information
Management, 34(1), pp.1-13.

(5) Ivan, I., Curia, C., Dionne, M. and Avramiea, A., 2012. Collaborative Management of Risks and Complexity in
Banking Systems. Informatics Economical, 16(2), pp.128-141.

(6) Gharaibeh, N., 2013. The impact of customer knowledge on the security of Ebanking. International Journal of
Computer Science and Security (IJCSS), 7(2), p.81.

(7) Council, F.F.I.E., 2005. Authentication in an internet banking environment. Financial Institution Letter, FIL-103-2005.
Washington, DC: Federal Deposit Insurance Corp. (FDIC). Retrieved March, 18, p.2005.

(8) 1 Chen, C.J., 2016, July. User Adoption Decisions in Self-Service Technologies: A Study of the Internet Banking.
In Advanced Applied Informatics (IIAI-AAI), 2016 5th IIAI International Congress on (pp. 1207-1208). IEEE.

(9) Kesharwani, A. and Singh Bight, S., 2012. The impact of trust and perceived risk on internet banking adoption in India:
An extension of technology acceptance model. International Journal of Bank Marketing, 30(4), pp.303-322.

(10) Martins, C., Oliveira, T. And Popover, A., 2014. Understanding the Internet banking adoption: A unified theory of
acceptance and use of technology and perceived risk application. International Journal of Information

Management, 34(1), pp.1-13.

(11) Al-Aja, A.S. and Mad nor, K., 2015. Challenges of adoption of internet banking service in Yemen. International
Journal of bank marketing, 33(2), pp.178-194.

(12) Yuen, Y.Y., Yew, P.H. and Lim, N., 2015. Internet banking acceptance in the United States and Malaysia: a cross-
Cultural examination. Marketing Intelligence & Planning, 33(3), pp.292-308.

(13) Alwen, H.A. and Al-Zuni, A.I., 2016. Determinants of Internet Banking Adoption among Customers of Commercial
Banks: An Empirical Study in the Jordanian Banking Sector. International Journal of Business and
Management, 11(3), p.95.

(14) Hanafizadeh, P., Keating, B.W. And Khedmatgozar, H.R., 2014. A systematic review of Internet banking
Adoption. Telematics and informatics, 31(3), pp.492-510.

(15) Al-Somali, S.A., Gholami, R. and Clegg, B., 2009. An investigation into the acceptance of online banking in Saudi Arabia. Tec novation, 29(2), pp.130-141.

(16) Internetlivestats (2017), accessed on January 8, 2017 from http://www.internetlivestats.com/

(17) Saudi Arabian Monetary Agency (SAMA) annual report (2016):
http://www.sama.gov.sa/en-US/Economic Reports/Pages/AnnualReport.aspx

(18) Baharat Poddar, Yashraj E., Neeta Chit Kara, Abhinav Bansal, 2016. Productivity in Indian Banking. Boston Consulting Group, Aug, 16.

(19) State Bank of Pakistan annual report (2015/2016):
http://www.sbp.org.pk/reports/annual/index.htm

(20) Kierkegaard, S., 2007. Swallowing the Bait, Hook, Line, and Sinker: Phishing, Pharming, and Now Rat-in!.
In Managing Information Assurance in Financial Services (pp. 241-260). IGI Global.

(21) Gann, G.G.G., 2008. Phishing: A Growing Challenge for Internet Banking Providers in Malaysia. Communications of The IBIMA, 5, pp. 133-142.

(22) Dhanalakshmi, R., Prabhu, C. And Chaliapin, C., 2011. Detection of phishing websites and secure

Transactions. IJCNS, 1(11), pp.15-21.

(23) Alphas, J.M. and Karim, Z., 2013. Social Engineering in Phishing Attacks in the Eastern Province of Saudi
Arabia. Asian Journal of Information Technology, 12(3), pp. 91-98.

(24) Ago, W. And Kim, J., 2007. Robbing the cradle is like taking candy from a baby. In Proceedings of the Annual
Conference of the Security Policy Institute (GCSPI), pp. 23-37.

(25) Dodge, R.C., Carver, C. and Ferguson, A.J., 2007. Phishing for user security awareness. Computers & Security, 26(1), Pp.73-80.

(26) Khari, M., Shrivastava, G., Gupta, S., and Gupta, R., 2017. Role of Cyber Security in Today's Scenario. In Detecting and Mitigating Robotic Cyber Security Risks (pp. 177-191). IGI Global.

(27) Khari, M., Shrivastava, G., Gupta, S. and Gupta, R., 2017. Role of Cyber Security in Today's Scenario. In Detecting and Mitigating Robotic Cyber Security Risks (pp. 177-191). IGI Global.

(28) Le, D., Kumar, R., Mishra, B.K., Khari, M. and Chatterjee, J.M., 2019. Cyber Security in Parallel and Distributed Computing. Wiley, Hoboken.

(29) Wechuli, N.A., Franklin, W. and Jotham, W., 2017. User Perceived Secure Mobile Banking Service Provision Framework. International Journal of Computer Engineering and Information Technology, 9(10), pp.225-232.

(30) Zhang, T., Lu, C. and Kizildag, M., 2018. Banking “on-the-go”: examining consumers’ adoption of mobile banking services. International Journal of Quality and Service Sciences.
https://enterslice.com/learning/cybersecurity-in-digital-banking-threats-challengesandsolution/#:~:text=Unencrypted%20data,online%20must%20be%20fully%20encrypted.

APPENDIX AND QUESTIONNAIRE

1) What is your name?
2) Age Group

- 18-25
- 25-35
- 35 above

3) Gender
   - Male
   - Female

4) Qualification
   - Up to HSC
   - Graduate
   - Post Graduate
   - Professional
   -

5) Occupation
   - Student
   - Home Maker
   - Self Employed
   - Employee
   - Retired
   -

6) Have you ever experienced cybercrime regarding online Banking?
   - Yes
   - No
   - Maybe

- Not sure

7) Do you think online transaction is affecting the banking?

- Yes
- No
- Maybe
- Not sure

8) What majority of Cybercrimes have been committed by the young people in the age group between?

- 12-19 • 18-30
- 20-40
- none of above

9) Is banking sector is totally changed after the arrival of internet especially in the term of security..?

- Yes
- No
- Maybe
- Not sure

10) Do you have any idea about cyber security issue while doing online banking and online transactions?

- Yes
- No
- Maybe
- Not sure

11) Do you think while online transaction there is a risk?

- Yes
- No
- Maybe
- Not sure

12) Cyber security began in?

- 1970s • 1990s

- 1920s

13) Do think that a major element of cyber security is operation security?*

- Yes
- No
- Maybe
- Not sure

14) Why do you think cyber security is beneficial for protecting end users?*

- Yes
- No
- Maybe
- Not sure

15) Do you known that while online transaction there are frauds?*

- Yes
- No
- Maybe
- Not sure

16) Do you think that unfortunately, cyber security is now a part of life?*

- Yes
- No
- Maybe
- Not sure

17) Do you think that banks need to safeguard data and assist in cyber security?*

  - Yes
  - No
  - Maybe
  - Not sure

18) Do you secured your money in the locker for safety?*

- Yes
- No
- Maybe
- Not sure

19) Do you know fraudsters' access to a bank account?*

- Yes
- No
- Maybe
- Not sure

20) Do you think that cyber security is useful nowadays?

- Yes
- No
- Maybe
- Not sure

21) Do you think that the laws in effect are able control cyber criminals?*

- Yes
- No
- Maybe
- Not sure

22) Do you think that using any protected browser for online transaction is protected?*

- Yes
- No
- Maybe
- Not sure

23) Do you agree that between crime and punishment it is mainly a battle of wits?*

- Agree
- Strongly agree
- Disagree
- Strongly disagree
- Neutral

Do you know how many percentage have faced in cybercrimes?*

- 71.7%
- 80.12%
- 50.2%
- 61%