Security awareness in online banking among college students

Rakesh Patil[1], Ganesh Vilas Bawaskar[2]
[1]*Assistant Professor, Department of Computer Science, Tilak Maharashtra Vidyapeeth, Pune*
[2]*Student of MCA, TMV*

***Abstract*—The fast growth of smartphones and digital technology has changed the banking sector in India, making mobile banking apps one of the most common ways to manage money, especially for young people. This case study looks at how postgraduate students use and feel about mobile banking apps, as they are usually skilled with technology and prefer quick and simple ways to handle their finances. A survey was used to find out what factors affect their use of these apps, such as ease of use, usefulness, security, and trust. The findings show that most students actively use mobile banking because it saves time and makes services like money transfers and bill payments available anytime and anywhere. However, many of them still worry about the safety of online transactions and the privacy of their personal information. The study concludes that although postgraduate students like mobile banking for its speed and convenience, banks need to keep improving security measures, protect users' data, and build trust to keep students confident and satisfied with these services**

***Index Terms*—Online Banking, Security Awareness, Phishing, Two-Factor Authentication (2FA), Mobile Banking**

I. INTRODUCTION

Today, almost everyone uses online banking to send money, pay bills, and check account balances. It's fast and easy, but it also comes with risks like hacking and fraud. College students, who are regular users of mobile apps and online services, might not always be fully aware of the dangers. This project studies how much college students know about keeping their online banking activities safe and secure

Objectives of research:

1. Find out how much students know about online banking security.
2. See which online banking services students use the most.
3. Spot common mistakes students make while using online banking.
4. Check if students know about online threats like fake emails and hacking.
5. See if students use extra security steps like two-factor authentication.
6. Find out how often students change their banking passwords.
7. Understand how students react when they notice something wrong in their accounts.

Hypothesis:

1. If mobile banking apps are easy to use, students will use them more.
2. If students find mobile banking useful, they will want to use it.
3. Worries about data safety and secure transactions make students less likely to use mobile banking.
4. When students trust banks and mobile apps, they are happier and keep using them.
5. Students with better technology skills feel more confident about using mobile banking safely.

II. LITERATURE REVIEW

The review of literature for this study identified several key findings about security awareness in online banking among college students. Research indicates that while young adults are frequent users of digital banking platforms, their awareness of essential security practices
remain inconsistent. They often recognize basic measures, such as the need for strong passwords, but tend to overlook critical aspects like identifying phishing scams or the risks associated with public Wi-

Fi usage for financial transactions.
Several studies highlight the role of banks in enhancing security awareness through in-app tips, alerts, and user-friendly interfaces. However, gaps persist in outreach efforts, with many students relying on peers or unverified online sources for information, which may lead to misinformation or incomplete understanding.
The literature also underscores the importance of incorporating cybersecurity education into academic programs. Workshops, seminars, and interactive learning tools have shown promise in improving knowledge and fostering proactive behavior. However, the availability and consistency of these educational initiatives are often limited.

Aslam Sayeed, Sharadha Singh, (2024): Describe in the study which
examines the impact of security concerns on e-banking adoption, blending qualitative and quantitative methods to explore customer perceptions.
Qualitative insights reveal diverse security apprehensions, while quantitative analysis highlights trust as a mediating factor. Addressing these concerns with robust security measures and transparent communication strategies can enhance e-banking adoption, driving the sector's digital evolution amidst technological advancements and changing consumer
preferences. Patchan Bhujanga Rao, (2024) – in their study thoroughly explores cyber security challenges in online banking**,** emphasizing the need to understand and mitigate risks posed by cyber threats. It addresses issues such as phishing, malware, identity theft, and data breaches, along with regulatory hurdles and mobile banking vulnerabilities. Through its
analysis, the research purposes to offer visions and suggestions to strengthen safety and trust in digital banking within the digital financial landscape.

Jane Smith, Chen Liu, (2024): In this study examines the intricate regulatory environment leading digital
safety, and monetary guidelines. It investigates how regulatory bodies enforce compliance to alleviate threats and safeguard customer benefits. Additionally, the study traces the impact of governing adherence on secure system strategy and execution, analyzing risk management and encryption practices to bolster digital infrastructures against cyber threats. Challenges such as inter country
dealings and efforts towards governing synchronization are discussed, alongside incipient styles in governing machinery (Retch) and the use of progressive analytics to improve amenability observing. Dipti Ben Ghelani, Surendra Kumar Redd (2022): In today's digital age, safeguarding data against cyber threats is crucial, especially in mobile environments like airplanes and ships. We aim to enhance data security measures by leveraging machine learning, biometric recognition, and hybrid approaches. One proposed solution involves integrating “http://eelet.org.uk” biometric impressions and digital signatures into banking systems, reducing intrusion risks and ensuring secure
transactions.
Suganya K, (2022): The study discusses the perpetual threat cybercrime poses to the security of financial and business sectors, particularly in online banking. It emphasizes the need to raise awareness among customers about cyber threats and suggests staying updated on security measures to mitigate risks during digital transactions. The research underscores the
importance of safeguarding sensitive financial data and advocating for proactive measures to combat cyber threats in online banking**.**

Haitham M Alzoubi, Taher M. Ghazal (2022): Digital banking encounters security risks from hackers and fraudsters, necessitating robust measures like multiple verifications and data encryption. Existing research underscores cyber security threats as a major concern in digital banking, often underestimated by users. This study supports hypotheses from
previous works through theoretical analysis, stressing the need for further research to enhance security measures.

III. RESEARCH METHODOLOGY

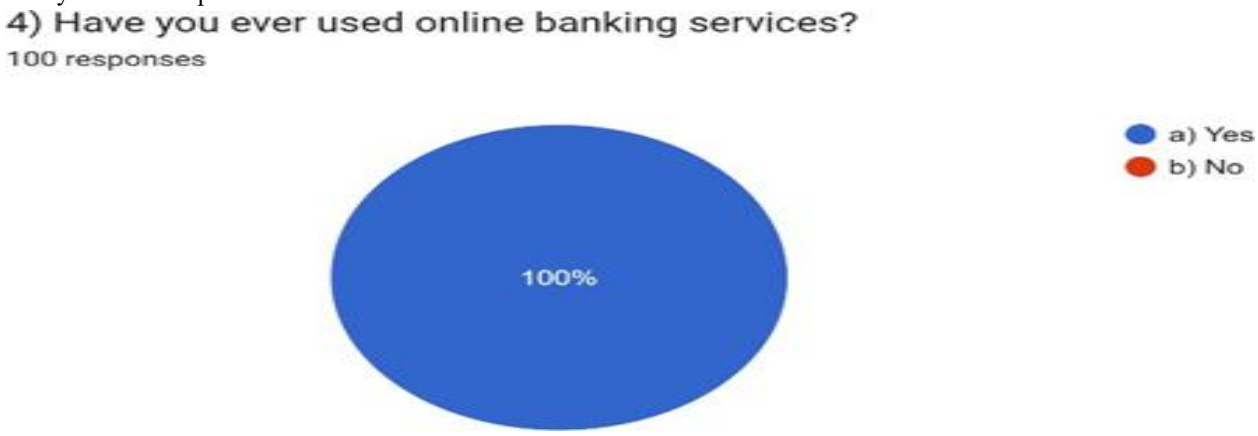
banking, spanning facts defense, virtual
Type of Research: Descriptive research.
Researches titled "Security Awareness in Online Banking Among College
Students" employs descriptive research methodology to explore and evaluate the levels of security

awareness, perceptions, and practices among college students. This type of research focuses on gathering data through surveys and questionnaires to understand the current state of knowledge and behaviour
related to online banking security. (collected directly from students).

Research Design
The study is descriptive in nature, which means it will describe how aware students are about online banking security. It will collect data directly from students using a questionnaire to understand their awareness, behaviour, and experiences

Sampling Design
Target College student: College/university students who use online banking.
Sampling Method: Convenience sampling (selecting students who are easily available).
Sample Size:
The sample size for this study will range between 100 respondents, depending on the availability of participants and the resources of the researcher
Data Collection Primary Data
Survey and questionnaires: Online (Google Forms) or Offline (Printed questionnaires) collected data directly from students.
Interviews: In-depth interviews with a selected group of students can provide additional insights into their experiences, challenges, and suggestions for improving security awareness.
Focus Groups: Small group discussions are conducted to explore collective opinions, behaviors, and attitudes towards online banking security in greater detail.
Secondary Data Collection:
Literature Review: Secondary data is sourced from academic journals, books, reports, and prior research studies related to cybersecurity and online banking.
Digital Platforms: Information from trusted banking websites, cybersecurity resources, and public awareness campaigns is used to support and validate findings.
Technology-Driven Tools:
Online Surveys: Tools like Google Forms, SurveyMonkey, or similar platforms are used to distribute questionnaires and collect responses conveniently.
Data Analytics: Analysis of anonymized online banking transaction data or behavioral patterns (if accessible and permitted) could be incorporated for enriched insights.
Data Collection Tool: A structured questionnaire will be used as the primary tool for data collection.
Multiple-choice questions: Demographics questions awareness questions, experience questions and suggestions basic questions

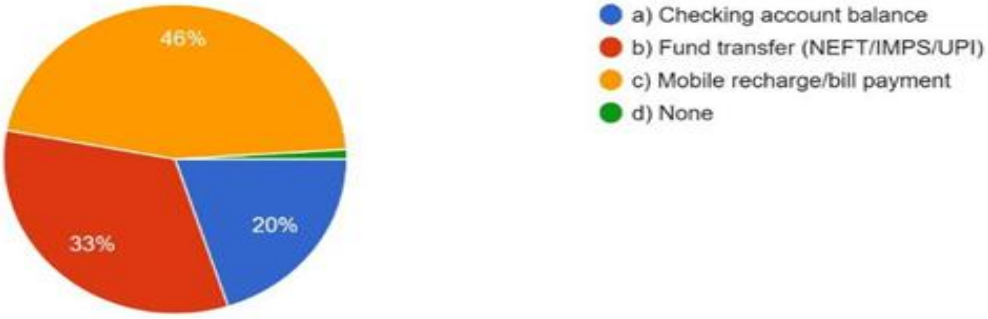
Analysis and Interpretation



Interpretation:
All 100 respondents (100%) reported that they have used online banking services. There were no participants
who answered “No.” Conclusion:
The data shows full adoption of online banking among the respondents. This suggests that the target group is highly digital

5) Which of the following online banking services do you use most often?

100 responses



Interpretation

The majority (46%) of respondents use for mobile recharge/bill payments

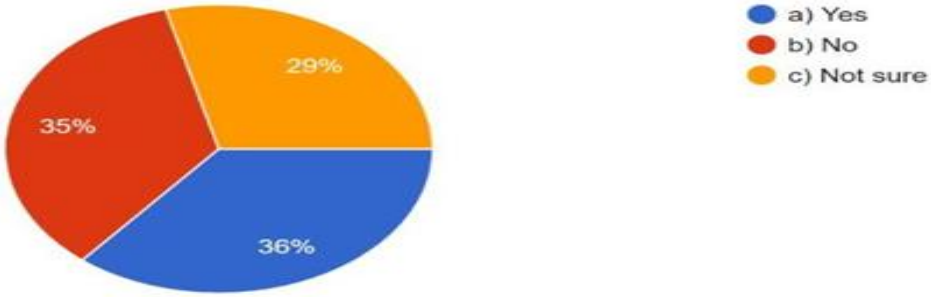
The second most common 33%, of the respondents Fund transfers (NEFT/IMPS/UPI). the least frequent at 20% of respondent checking their account balance.

1% reported not using any of the listed online banking services.

mobile recharge/bill payments is the most popular online banking service used among the surveyed participants.

7) Do you know what phishing is?

100 responses



Interpretation

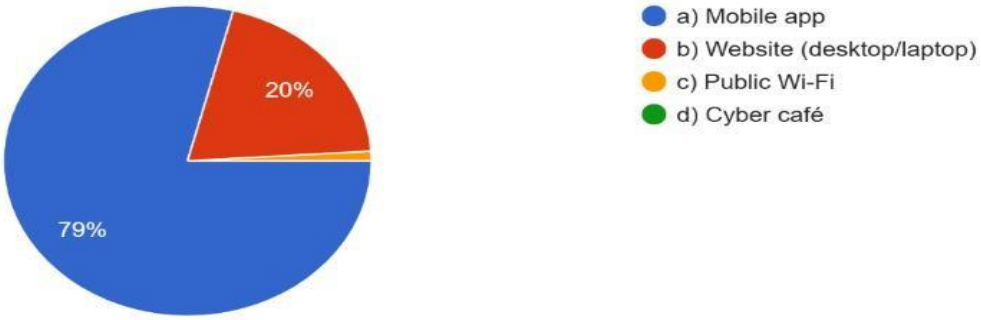
36 people said yes, they know about it.

35 people said no, they don't know what it is. 29 people said they're not sure.

Only a few people really understand phishing. Many don't know or are confused.

8) Which of these do you think is safest for online banking?

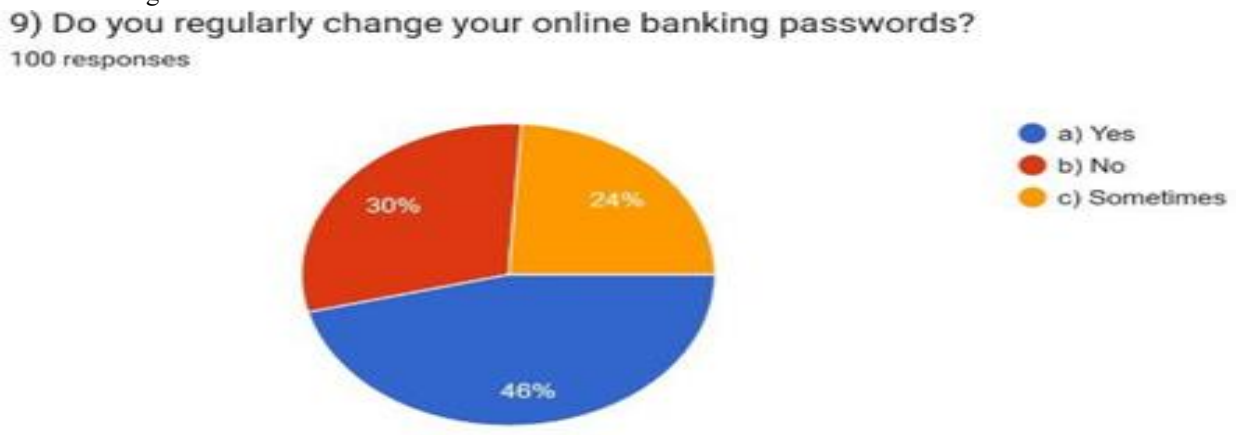
100 responses



Interpretation

A large majority (79%) believe that using a mobile banking app is the safest option. A smaller portion (20%) selected using a website on a desktop or laptop computer. Very few people (less than 1%) chose public Wi-Fi or a cybercafé as the safest option.

Based on this survey of 100 respondents, there's a strong preference for mobile banking apps as the safest method for online banking.

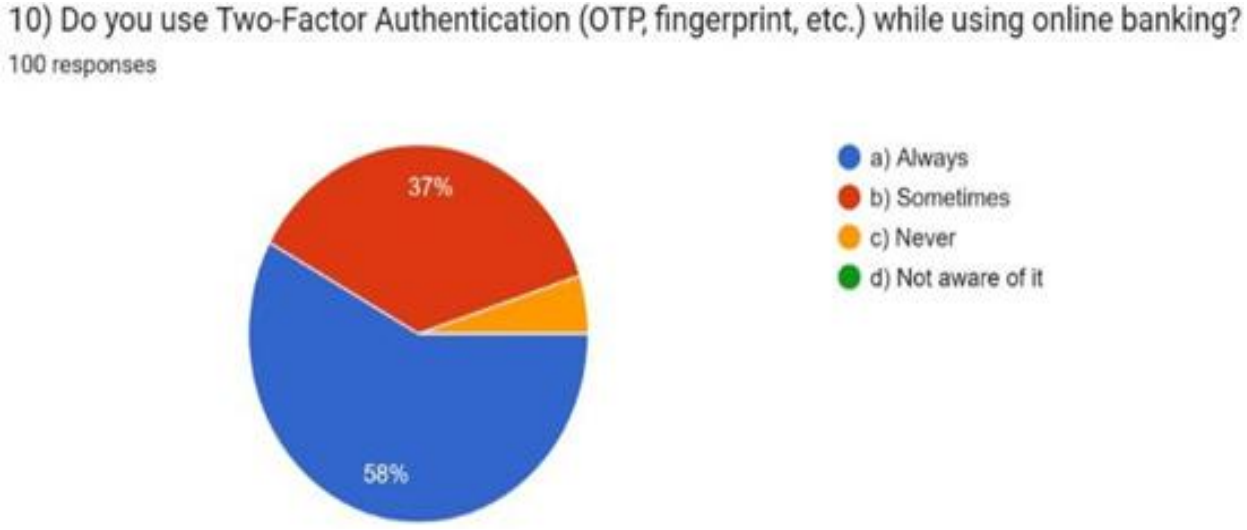


Interpretation

46% of respondents reported changing their passwords sometimes. This is the largest group. 30% said they never change their passwords (a significant security risk).

Only 24% of respondent regularly changing their passwords,.

A large proportion of users consistently update their passwords and need to be more careful with their online security.



Interpretation

58% of people always use two-factor authentication like OTP or fingerprint.

37% use it sometimes.

Only 5% never use it.

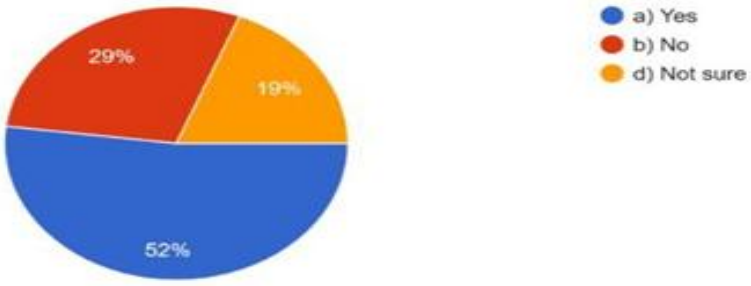
No one said they are not aware of it.

This means that most people use two-factor authentication regularly, which is good for online banking security. Very few people don't use it at all.

11) Do you check the URL before logging into your bank account?
100 responses

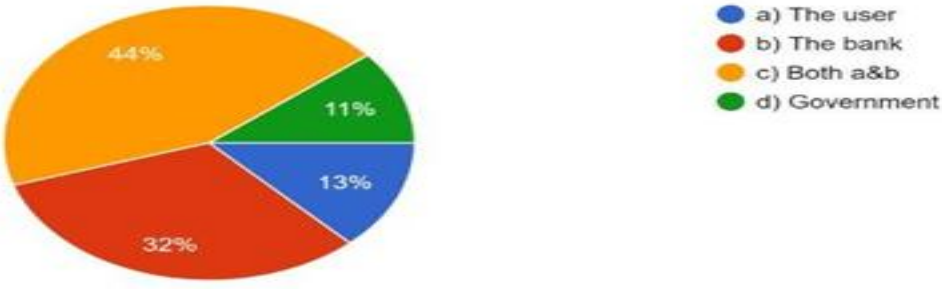
Interpretation
42% of respondents always check the URL. 31% never check it.
16% check it sometimes.
11% don't know what to check.
While many are cautious, a large number either don't check or are unaware of how to check, posing a security risk. This show that although some users are careful, there is still a large group that lacks knowledge or awareness about basic online security steps.

12) Have you ever received a suspicious message or email asking for your banking details?
100 responses



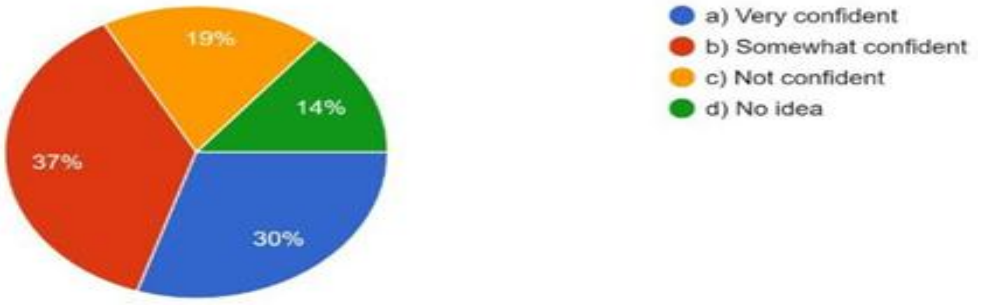
Interpretation
52% said yes.
29% said no.
19% were not sure.
More than half of the people said they have received fake or suspicious messages asking for their bank details. This shows that online scams are common, and people need to be very careful.

13) Who do you think is responsible for ensuring online banking security?
100 responses



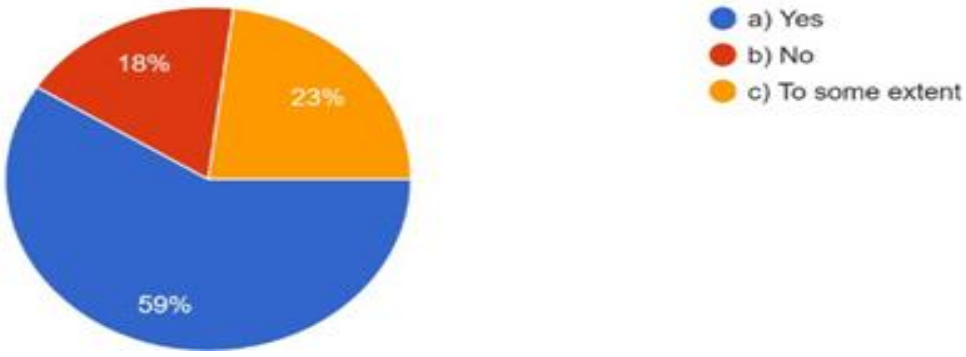
Interpretation
13% say the user is responsible. 32% think it's the bank's job.
44% believe both users and banks are responsible. 11% believe the government is responsible.
This shows that people understand that security is a joint effort and not the responsibility of one party alone.

14) How confident are you in identifying a fake banking website or app?
100 responses

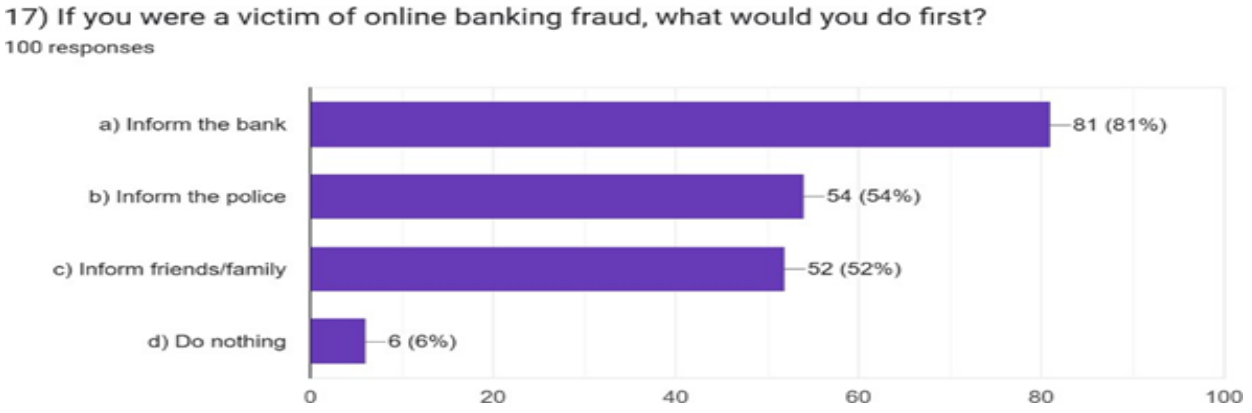


Interpretation
30% are Very confident, meaning they believe they can spot fakes. 37% are Somewhat confident, indicating some uncertainty.
19% are Not confident.
14% have No idea, showing a lack of knowledge.
Even though many feel confident, a large portion of students are unsure or not confident in identifying fake banking sites or apps.
Interpretation
Most people (59%) think students know about online banking risks.
Some (23%) believe students know a little, but not everything A smaller group (18%) feel students are not aware at all .so, while most students seem aware, there is still a need to improve their understanding.

16) Do you feel college students are well aware of online banking risks?
100 responses



Interpretation
Most people (59%) think students know about online banking risks. Some (23%) believe students know a little, but not everything
A smaller group (18%) feel students are not aware at all
.so, while most students seem aware, there is still a need to improve their understanding.

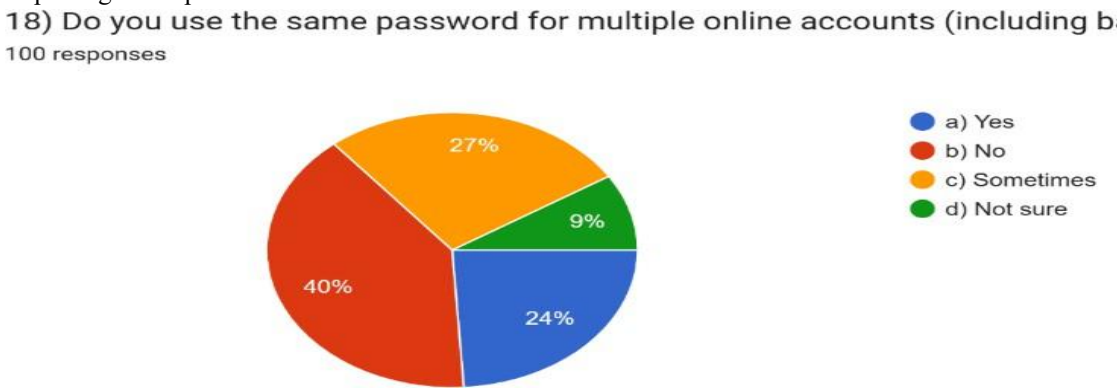


Interpretation

81% would inform the bank immediately—an ideal response. 54% would inform the police, and 52% would tell friends/family.

6% would do nothing, showing a lack of confidence.

The data clearly show that informing the bank is the most common and immediate response to online banking fraud. Reporting to the police and also inform to friends.

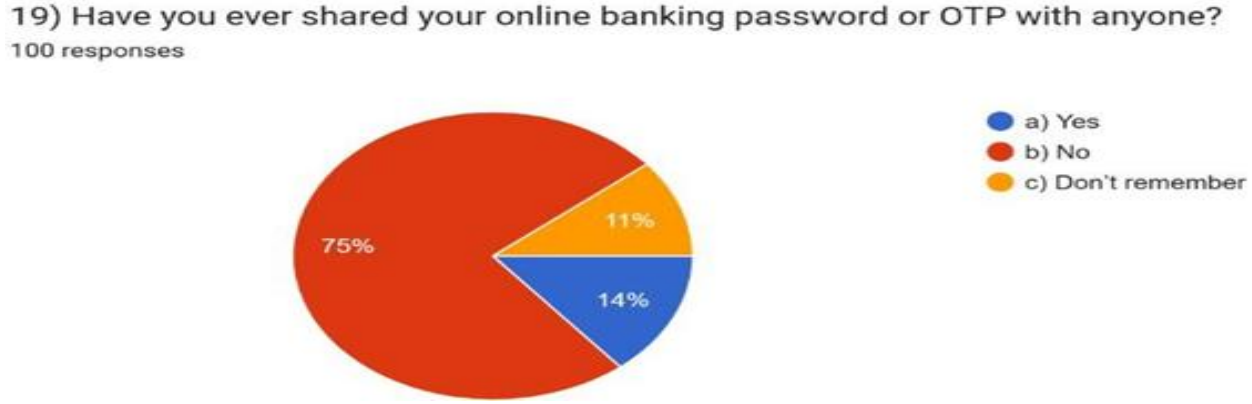


Interpretation

40% of respondents said No, indicating awareness of password security. 27% said Sometimes, which still poses a security risk.

24% admitted to Yes, suggesting a significant number use the same password. 9% were Not sure, highlighting lack of awareness.

This show that need for increased education and awareness campaigns around secure password among users.



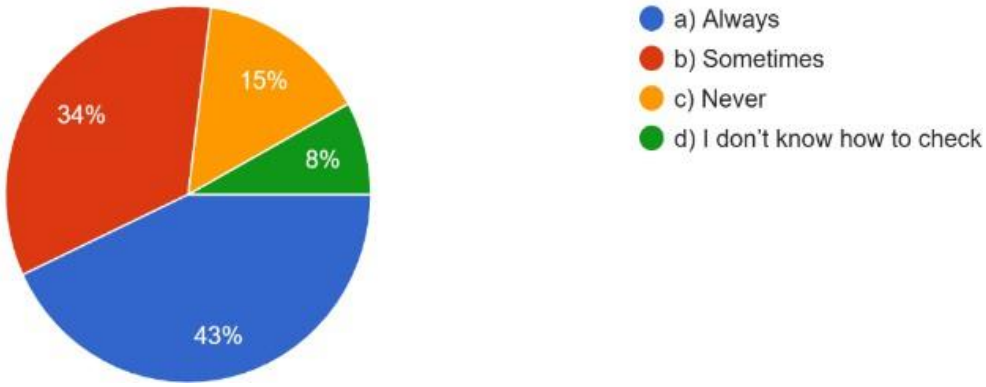
Interpretation

75% of people said “No”, never shared their online banking password. 14% said “Yes”, shared their password. 11% said they don’t remember if they have shared it.

This means that most people are careful and keep their online banking password private, but a small number have shared it, which could be a security risk.

20) Do you verify app authenticity before installing a banking app?

100 responses



Interpretation

43% of respondents always check if the banking app is genuine. 34% check sometimes.

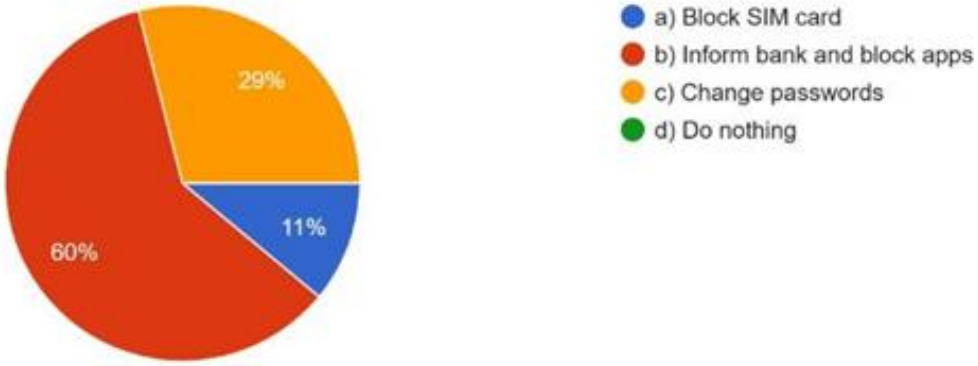
15% never check.

8% don’t know how to check app authenticity.

This show that while many users are cautious, a significant number either don’t check or don’t know how to check security.

21) If you lost your phone with banking apps installed, what would you do first?

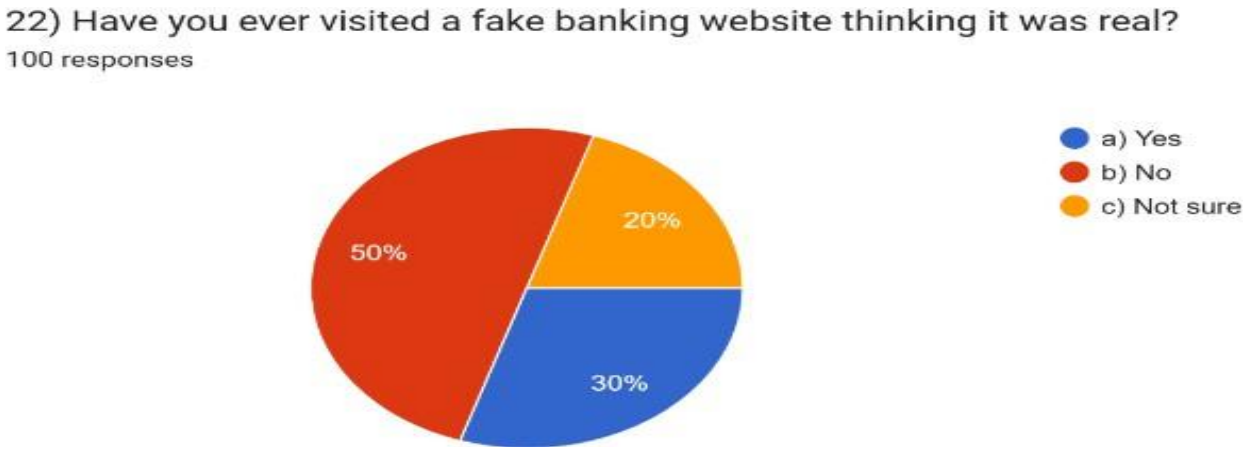
100 responses



Interpretation

The majority (60%) would immediately inform their bank and block the banking apps. (29%) would change their passwords first. A smaller percentage (11%) would blocking their SIM card, Only 0% indicated they would do nothing.

The survey highlights the public’s awareness of the importance of securing their banking information following phone loss. While blocking the SIM card is a crucial step, directly contacting the bank



Interpretation
30% said Yes, they have fallen for a fake website. 50% said No.
20% are Not sure.
This shows that half the users are confident, but a third have already been tricked, and some don't even sure.

IV. CONCLUSION

1. Young and Digital-Savvy Group: Most respondents are aged 21–23 and are students. They are digital users who frequently use online banking services.
2. Gender and Education: Majority are male and well-educated, with most having at least an undergraduate degree. This group is expected to understand technology and banking.
3. 100% Online Banking Usage: Every respondent has used online banking, showing full adoption and strong interest in digital banking.
4. Popular Uses: The most common use is for mobile recharge and bill payments (46%), followed by money transfers (33%). Checking account balance is less common (20%).
5. Low Awareness of Phishing: Only 36% know about phishing. Most people are either unaware or unsure, which is a serious security issue.
6. Strong Preference for Mobile Apps: Most (79%) believe mobile banking apps are the safest method.
7. Weak Password Practices: Only 24% regularly change their passwords. Many (30%) never change them, which is risky.
8. Good Use of Two-Factor Authentication: 58% always use it, but a small group still does not.
9. URL and App Checking: Many users don't check URLs or verify app authenticity, which puts them at risk.
10. Phishing and Fake Messages: Over half have received suspicious messages. Scams are common.
11. Security Responsibility Awareness: Most believe both banks and users share the responsibility of protecting online banking.
12. Mixed Confidence in Detecting Fraud: Some feel confident spotting fake apps or sites, but many are unsure or not confident.
13. Password Sharing: Most people don't share passwords, but a small group still does, which is dangerous.
14. Good Emergency Response: Most would report to the bank immediately after fraud or phone loss.

Challenges
1. Lack of Awareness About Phishing: Many don't know what phishing is or how it works.
2. Weak Password Habits: Many never change their passwords or reuse the same ones.
3. Overconfidence or Confusion: Some users are unsure or overconfident about identifying fake banking sites.
4. Neglecting App and URL Checking: Not everyone checks if an app or link is safe before using it.
5. Sharing Passwords: A small group still shares their banking passwords.
6. Students Still Need More Awareness: Even though most are aware of online banking risks, many still fall for scams or are not fully

informed.

7. Incomplete Security Actions: Some people would only block their SIM and not take other steps like informing the bank.

Suggestions

1. Awareness Campaigns on Phishing: Organize online or offline workshops to teach students how phishing works and how to avoid it.
2. Teach Strong Password Practices: Encourage regular password changes and teach how to create strong, unique passwords.
3. Promote Two-Factor Authentication: Educate people to always enable and use two- factor authentication.
4. Teach How to Check URLs and Apps: Show simple ways to identify fake banking apps and websites.
5. Encourage Reporting of Scams: People should be encouraged to report any suspicious activity immediately to the bank and police.
6. Use Real-Life Examples: Share stories of banking fraud and how it happened to make people more alert.
7. Involve Banks in Education: Banks can send safety tips through emails, SMS, or in- app messages.
8. Mobile Safety Training: Educate users on what to do if their phone is lost—such as blocking the SIM and bank apps.

REFERENCE

[1] Chandra Sekhar, M., & Kumar, M. (2023). An overview of cyber security in digital banking sector. East Asian Journal of Multidisciplinary Research, 2(1), 43–52.

[2] Haitham, M., & Hasan, M. K. (2022). Cyber security threats on digital banking. International Conference on AI in Cybersecurity.

[3] Alzoubi, H. M., & Ghazal, T. M. (2022). Cyber security threats on digital banking. Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE).

[4] Rao, P. B. (2024). A study on cyber security issues affecting online banking and transactions. International Journal of Advance Research and Innovative Ideas in Education, 9(6).

[5] Pavithra, C. B. (2021). Factors affecting customers' perception towards digital banking services. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 1608–1614.

[6] Borgave, S., & Kalkar, P. (2022). A review of cyber security issues in online banking and online transactions. International Conference on AI in Cybersecurity, 20(18), 405–418.

[7] Sankararaman, G., Suresh, S., & Kumar, M. N. (2021). A study on users opinion on cyber security. International Journal on Global Business Management & Research, 10(2), 61–68.