Cybersecurity Challenges in Digital Banking

Dr.C.Mallesha[1], Peddholla Sai Kiran[2]
[1]*Assistant.Professor, School of Management, Anurag University.*
[2]*Student, School of Management, Anurag University.*

Abstract: Digital banking has revolutionized finance, offering convenience but also significant cybersecurity challenges. Interconnected networks, online platforms, and mobile apps increase the attack surface for cybercriminals. Safeguarding customer information is a primary challenge, with phishing and malware threats. Financial fraud prevention is another key concern as cybercriminals exploit vulnerabilities. Ensuring service integrity and availability is also difficult. Institutions need multi-factor authentication, encryption, audits, training, and incident response plans. Collaboration with regulators and experts is crucial. The study focuses on cyber fraud types, reasons, and individual awareness through a questionnaire.

Key Words: Banking Industry, Fraud, Prevention, Security, phishing, malware attacks.

INTRODUCTION

Digital banking allows customers to conduct banking services and transactions using electronic channels like the internet and mobile devices. It offers convenience and flexibility with features such as account management, transfers, payments, and investment management. To ensure security, banks employ technologies like AI, chatbots, and blockchain. Cybersecurity protects computer systems, networks, and data from digital attacks like viruses, malware, and hacking. In the banking sector, measures like firewalls, encryption, multi-factor authentication, and employee training are employed to prevent cyber-attacks and maintain public trust. As the banking sector relies more on digital technology, investing in cybersecurity remains crucial to mitigate cyber risks.

NEED OF THE STUDY

Digital banking in India started with internet services, but real growth came with mobile apps and the push for a cashless economy. UPI's introduction in 2016 revolutionized payments. Cyber frauds have increased, with 2,059 cases in FY 2020-21. Despite risks, digital banking grows rapidly, facing evolving cybersecurity challenges. Studies are needed to identify threats and best practices.

OBJECTIVES OF THE STUDY

To examine the cyber security awareness among the online banking user

RESEARCH METHODOLOGY

Sources of research data:
Primary Data-Collected from the individuals about awareness of the cyber frauds through questionnaire.
Secondary Data- Collected from published sources like research articles, books, RBI reports, new papers, websites, annual reports of banks etc.

LIMITATIONS OF THE STUDY

Study based on small participant size limits generalizability. Challenges:

- Rapidly evolving threats.
- Human error & insider threats.
- Risks from third-party vendors.
- Compliance complexities.
- Resource allocation.
- User awareness.
- Balancing security & user experience.

REVIEW OF LITERATURE

1. Dr. Meenakshi Gaikwad and Mrs. Shalini (2022) discuss cyber security threats in online banking, preventive measures, and the role of the government and banks in their research paper "Cybersecurity Affair in Online Banking."
2. In their 2020 research paper, Mohammad Salman Husain and Dr. Mohammad Haroon highlighted major concerns about attacks on E-transactions in the digital

space, impacting both consumers and financial security systems. They emphasized the need for more validated services despite significant security mechanisms in place for online transactions.

3. Al-alawi's 2020 study investigates the importance of cyber security systems in the banking and financial sector for risk management. The research highlights the significant impact and benefits of implementing cyber security to keep information secure. However, it notes that some institutions are hesitant due to higher implementation costs.

4.Ponemon's 2020 research on "TAILORING CYBER SECURITY" reveals the rapid escalation of cyber threats in the banking sector. Despite digital advancements for consumer convenience and cost-cutting, modern technologies generate valuable data vulnerable to misappropriation. The study highlights an increase in cyber incidents/attacks, presenting significant challenges.

5. Ms. Neeta and Dr. V.K. Baksh (2019) collaborated on a research article on Cybercrimes in the Banking Sector, recommending that cyber-attacks be avoided by adhering to strict legal compliance.

6. In a 2019 study, A. Lakshmanan conducted research solely focused on cybercrime and discovered that cybercrime activities will increase in the coming days with no end in sight.

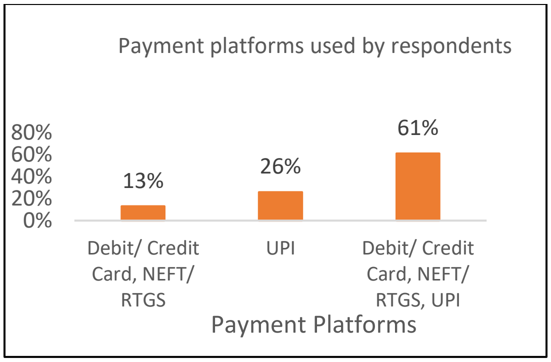
Objective 1: To examine the cyber security awareness among the online banking users Primary data regarding the awareness of the cyber security is collected through a questionnaire

Table: 1Various Payment platforms used by respondents.

Payment Platforms	No. of Respondents	Percentage
Debit/ Credit Card, NEFT/ RTGS	13	13%
UPI	26	26%
Debit/ Credit Card, NEFT/ RTGS, UPI	61	61%
Total	100	100%

Source: Calculated from primary data

Figure: 1Various Payment platforms used by respondents.



Source: Computed from primary data

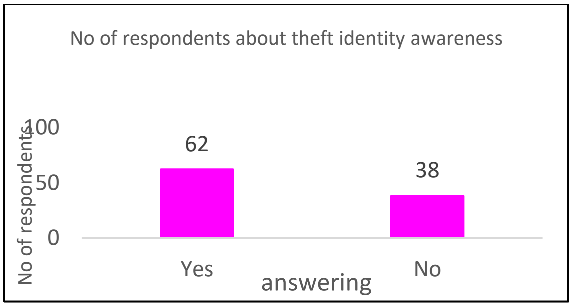
Interpretation: Majority of the respondents uses all the payment platforms altogether with an highest of 61% followed by only UPI users with 26%.

Table: 2 Awareness about identity thefts from respondents.

Awareness on theft identity	No. of Respondents	Percentage
Yes	62	62%
No	38	38%
Total	100	100%

Source: Calculated from primary data

Figure: 2 Awareness about identity thefts from respondents



Source: Computed from primary data

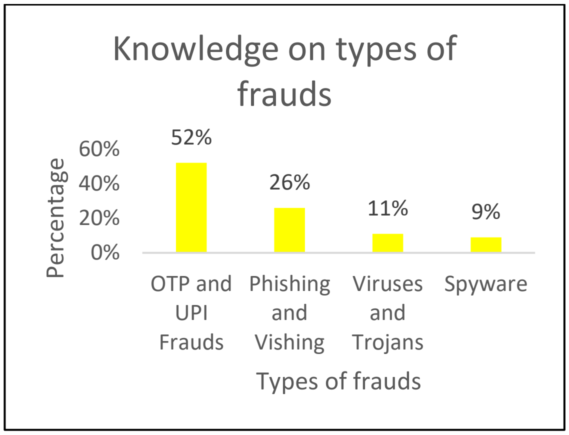
Interpretation: 62 respondents aware of identity theft, 38 respondents not aware of identity theft.

Table: 3 Knowledge about types of frauds by the respondents.

Types of frauds	No. of Respondents	Percentage
OTP and UPI Frauds	52	52%
Phishing and Vishing	26	26%
Viruses and Trojans	11	11%
Spyware	9	9%
Total	100	100%

Source: Calculated from primary data

Figure: 3 Knowledge about types of frauds by the respondents.



Source: Computed from primary data

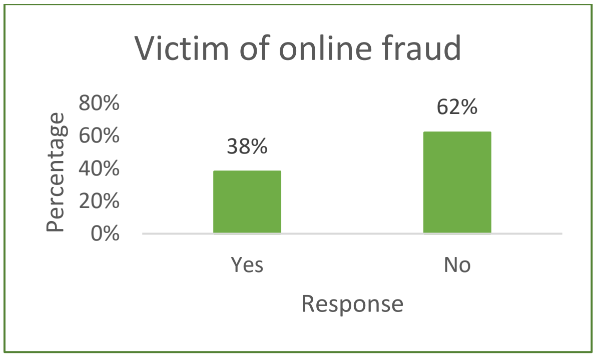
Interpretation: 52% aware of OTP and UPI frauds, 26% aware of phishing and vishing,
11% aware of viruses, 9% aware of Trojans and spyware.

Table: 4 Victim of online banking fraud.

Response	No. of Respondents	Percentage
Yes	38	38%
No	62	62%
Total	100	100%

Source: Calculated from primary data

Figure: 4Victim of online banking fraud.



Source: Computed from primary data

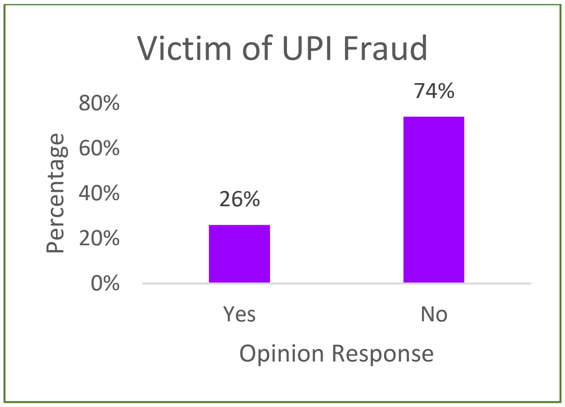
Interpretation: 62% of the respondents are not the victim of the online fraud whereas 38% of the respondents are victim of the online frauds.

Table: 5 Victim of UPI fraud.

Response	No. of Respondents	Percentage
Yes	26	26%
No	74	74%
Total	100	100%

Source: Calculated from primary data

Figure: 5 Victim of UPI fraud



Source: Computed from primary data

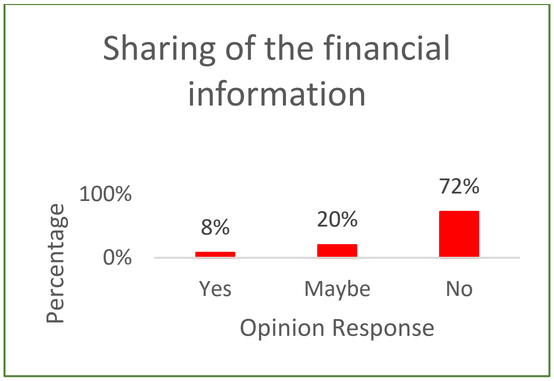
Interpretation: 74% of the respondents are not the victim of the UPI fraud whereas 26% of the respondents are victim of the UPI frauds.

Table: 6 Respondent's opinion related to sharing of financial information with anyone including bank officials.

Response	No. of Respondents	Percentage
Yes	8	8%
Maybe	20	20%
No	72	72%
Total	100	100%

Source: Calculated from primary data

Figure:6 Respondent's opinion related to sharing of financial information with anyone including bank officials



Source: Computed from primary data

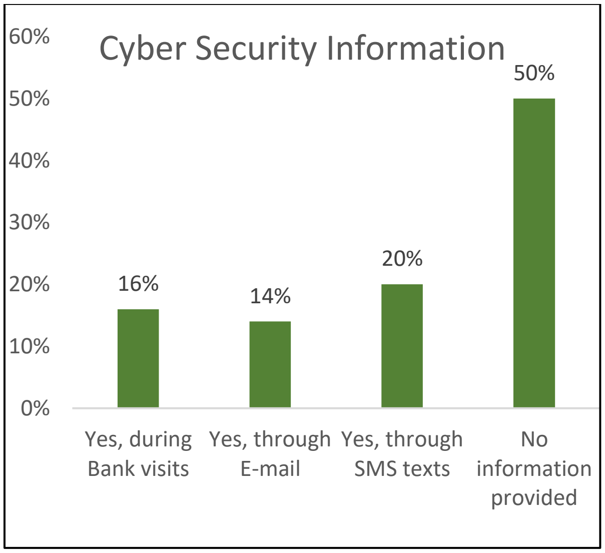
Interpretation: 72% of respondents don't share financial information,28% of respondents may share financial information.

Table: 7 Opinion about cyber security education by banks according to respondents.

Response	No. of Respondents	Percentage
Yes, during Bank visits	16	16%
Yes, through E-mail	14	14%
Yes, through SMS texts	20	20%
No information provided	50	50%
Total	100	100%

Source: Calculated from primary data

Figure: 7 Opinion about cyber security education by banks according to respondents



Source: Computed from primary data

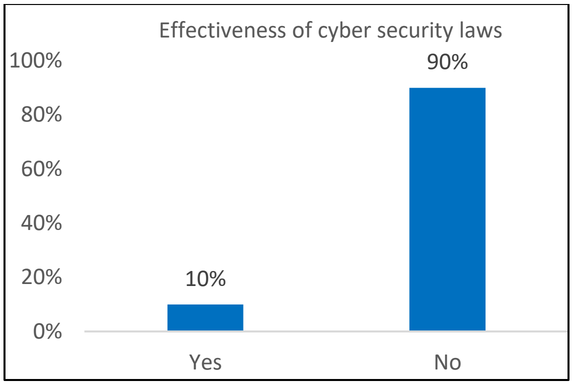
Interpretation: 50% say no information from bank personnel,16% say information provided during bank visits,14% say information provided through emails,20% say information provided through SMS.

Table: 8 Respondent's opinion regarding the effectiveness of cyber security laws.

Response	No. of Respondents	Percentage
Yes	10	10%
No	90	90%
Total	100	100%

Source: Calculated from primary data

Figure: 8 Respondent's opinion regarding the effectiveness of cyber security laws



Source: Computed from primary data

Interpretation:90% of the respondents say that cyber security laws are not so effective where as 10% of the respondents say that the laws are effective.

CONCLUSION

Digital banking has revolutionized financial management, but it comes with cybersecurity challenges. Phishing, ransomware, and data breaches require a proactive approach with strong authentication and encryption. Educating employees and customers is crucial to prevent social engineering attacks. Continuous monitoring, incident response, and updates improve security. The survey reveals low cyber fraud awareness, emphasizing the need to educate users in the digital world. Cybersecurity in digital banking is an ongoing process requiring constant vigilance, adaptation, and investment. Staying ahead of threats fosters customer trust and a strong security culture.

REFERENCE

[1] Dr. Meenakshi Gaikwad and Mrs. Shalini (2022) "Cybersecurity Affair in Online Banking."

[2] Mohammad Salman Husain and Dr. Mohammad Haroon(2020) An Enriched Information Security Framework From Various Attacks In The IOT

[3] Al-alawi (2020) "cyber security systems in the banking and financial sector for risk management".

[4] Ponemon's (2020) "Tailoring Cyber Security".

[5] Ms. Neeta and Dr. V.K. Baksh (2019) "Cybercrimes in the Banking Sector"

[6] A. Lakshmanan (2019) Cybercrime and cybercrime.

Websites:
1. https://rbi.org.in/home.aspx
2. https://cybercrime.gov.in/
3. https://www.wikipedia.org/