Research Paper

E-ISSN NO : 2455-295X | IMPACT FACTOR VALUE : 5.983
VOLUME : 11 | ISSUE : 3 | SPECIAL ISSUE MARCH-2025

A STUDY ON CYBER SECURITY AFFECTING ONLINE BANKING AND ONLINE TRANSACTION

M.GURU NARAYANAN	II M.COM (C.A), PG DEPARTMENT OF COMMERCE WITH COMPUTER APPLICATIONS, MANNARTHIRUMALAINAICKER COLLEGE (AUTONOMOUS), MADURAI-625004, TAMILNADU, INDIA.
M.SHANMUGAPRIYA	ASSITANT PROFESSOR, PG DEPARTMENT OF COMMERCE WITH COMPUTER APPLICATIONS, MANNARTHIRUMALAINAICKER COLLEGE (AUTONOMOUS), MADURAI-625004, TAMILNADU, INDIA.

ABSTRACT:

Online banking has revolutionized financial transactions by providing convenience, accessibility, and efficiency. However, the increasing reliance on digital banking services has also introduced significant cybersecurity risks. Cybercriminals exploit vulnerabilities in banking systems through phishing attacks, malware, ransomware, and identity theft, jeopardizing the security of sensitive financial data. One of the major threats is phishing, where attackers deceive users into revealing login credentials. Additionally, banking trojans and keyloggers compromise personal and financial information, leading to unauthorized transactions. Weak authentication mechanisms further expose banking systems to brute-force attacks and credential stuffing, emphasizing the need for robust security protocols. Despite advancements in encryption and multi-factor authentication (MFA), cybercriminals continuously develop sophisticated methods to bypass security controls. The adoption of artificial intelligence (AI) and machine learning (ML) in fraud detection has strengthened cybersecurity measures, but the evolving nature of cyber threats remains a persistent challenge.

KEYWORDS:

CYBER SECURITY, ONLINE BANKING.

1.1 INTRODUCTION

The rapid growth of online banking has transformed the financial sector by providing customers with seamless access to banking services from anywhere in the world. While this technological advancement offers convenience and efficiency, it also exposes users and financial institutions to increasing cybersecurity threats. Cybercriminals continuously exploit vulnerabilities in online banking systems to gain unauthorized access to sensitive financial data, leading to identity theft, fraud, and financial losses.

One of the most common cybersecurity threats affecting online banking is phishing, where attackers deceive users into revealing their login credentials through fraudulent emails or websites. Additionally, malware, such as banking trojans and keyloggers, can infiltrate devices to steal sensitive information, compromising account security. Ransomware attacks have also become prevalent, where hackers encrypt banking systems and demand payment for data recovery. Weak authentication mechanisms further expose online banking platforms to brute-force attacks and credential stuffing, making security measures like multi-factor authentication (MFA) and biometric verification essential.

1.2 STATEMENT OF PROBLEM

The growing dependence on online banking and financial transactions has significantly increased the risk of cyber threats, posing a major concern for financial institutions and customers alike. Despite the implementation of security measures, cybercriminals continue to exploit vulnerabilities in digital banking systems, leading to unauthorized access, financial fraud, and data breaches. Phishing attacks, malware infections, and ransomware incidents have become more frequent, highlighting the limitations of existing cybersecurity protocols. As these threats become more sophisticated, financial institutions face the challenge of continuously adapting their security frameworks to safeguard customer data and maintain trust in digital banking services.

1.3OBJECTIVE OF THE STUDY

- A study analyzing categories of cybercrime in the banking sector
- A study on Investigations to investigate cybercriminal activity.
- A study on Research to identify current cybercrime profiles.
- A study on Surveys to provide instructions to follow as a victim of cybercrime.
- A study on Suggests mitigations and security tips to control and curb cybercrime.

1.4 METHODOLOGY

1.4.1 RESEARCH DESIGN

This study will follow a descriptive research design to analyze cybersecurity issues affecting online banking and transactions. The research will focus on identifying common cyber threats, assessing their impact, and evaluating the effectiveness of existing security measures. A combination of qualitative and quantitative methods will be used to ensure a comprehensive understanding of the topic. Surveys and structured interviews will be conducted to gather firsthand data from banking customers, cybersecurity experts, and financial institution representatives. Additionally, secondary data from industry reports, case studies, and academic literature will be analyzed. The study will use a comparative approach to examine cybersecurity policies across different banks and regions, providing a well-rounded perspective on current challenges and potential solutions.

1.4.2 DATA SOURCES

Primary Data: This study collects firsthand data through surveys, interviews, and questionnaires with banking professionals, cybersecurity experts, and online banking users to assess cybersecurity challenges and mitigation strategies.

Secondary Data: The study relies on existing literature, reports, research papers, cybersecurity frameworks, case studies, and regulatory guidelines (e.g., GDPR, PCI-DSS) to analyze cybersecurity threats and solutions in online banking.

1.5 DATA ANALYSIS

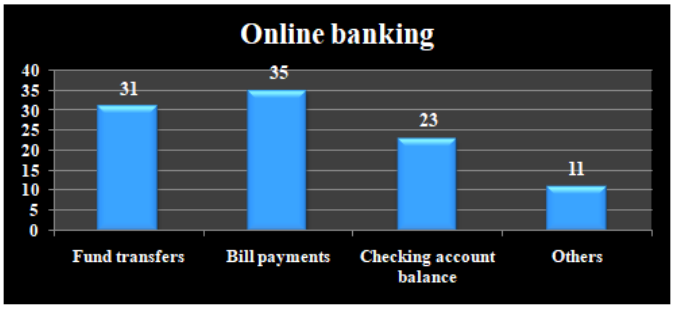
ONLINE BANKING SERVICES DO YOU USE MOST FREQUENTLY

TABLE 1.5.1

Particulars	No. of. Respondents	Percentage of respondents
Fund transfers	31	31
Bill payments	35	35
Checking account balance	23	23
Others	11	11
Total	**100**	**100**

Sources: Primary sources

CHART 1.5.1



INTERPRETATION:

The mostly frequently used online banking service is bill payments, with 35% of users opting for this feature. Fund transfers follow closely at 31%, while checking bank balance is the third most popular service at 23%. Other service makes up a smaller portion of the usage, with 11%.

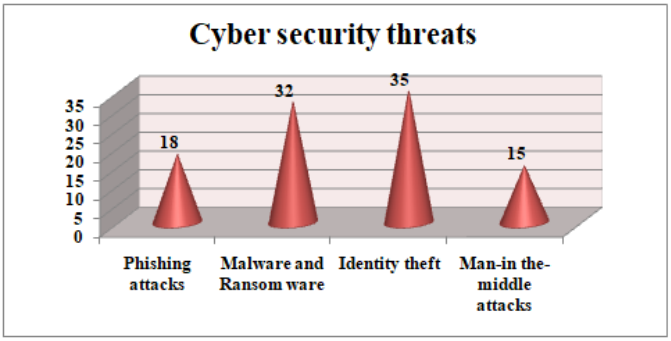
CYBER SECURITY THREATS HAVE YOU HEARD

TABLE 1.5.2

Particular	Number of Respondents	Percentage of respondents
Phishing attacks	18%	18
Malware and Ransom ware	32%	32
Identity theft	35%	35
Man-in the-middle attacks	15%	15
Total	**100**	**100**

Sources: Primary sources

CHART 1.5.2



INTERPRETATION:

Identity theft (35%) and malware/ransomware (32%) are the most common cyber threats, indicating a high risk to personal and organizational data. Phishing attacks (18%) and man-in-the-middle attacks (15%) also pose significant security concerns, though less frequently.

1.6 FINDING

- Bill payments (35%) are the most commonly used online banking feature, followed by fund transfers (31%) and checking bank balances (23%). Other services account for a smaller portion of usage (11%).
- Identity theft (35%) and malware/ransomware attacks (32%) are the most common cyber threats, indicating a high risk of data breaches and malicious software. Phishing attacks (18%) remain a gateway for fraud, while man-in-the-middle attacks (15%) are less frequent but still dangerous.

1.7 SUGGESTION

- Banks should prioritize enhancing the ease and security of bill payment and fund transfer features to cater to the largest user base. Additionally, they

could explore strategies to promote and improve the lesser-used services to increase engagement.

- Organizations should prioritize stronger defenses against identity theft and malware through advanced security protocols. Additionally, user education and awareness programs about phishing and secure communication practices should be enhanced.

1.8 CONCLUSION

This study highlights the critical cybersecurity threats affecting online banking and the impact they have on both financial institutions and users. The findings indicate that many banking customers remain unaware of proper cybersecurity practices, increasing their susceptibility to fraud. Additionally, weak authentication mechanisms and inadequate security measures further expose online banking systems to breaches. Despite the adoption of encryption, multi-factor authentication (MFA), and AI-driven fraud detection, cybercriminals continue to evolve their attack strategies.To address these challenges, financial institutions must strengthen cybersecurity frameworks by implementing advanced encryption, biometric authentication, and blockchain technology. Regular security audits, strict regulatory compliance, and enhanced incident response mechanisms are also crucial in mitigating cyber risks. Moreover, user education and awareness campaigns should be prioritized to promote safe online banking habits.

REFERENCES

1. **European Union Agency for Cybersecurity (ENISA) (2023).** Cybersecurity Threats in the Financial Sector. *ENISA Reports.* Retrieved from www.enisa.europa.eu

2. **Federal Financial Institutions Examination Council (FFIEC) (2023).** Cybersecurity Best Practices for Online Banking. *FFIEC Guidelines.* Retrieved from www.ffiec.gov

3. **Kaspersky Lab (2023).** The Evolution of Banking Malware: Emerging Cyber Threats. *Kaspersky Security Bulletin.* Retrieved from www.kaspersky.com