## **CYBERSECURITY IN E-BANKING: THREATS AND IMPLICATIONS EXPLORED**

## **Abstract**

E-banking denotes electronic banking. E-banking refers to the provision of banking services and products via electronic means. Internet banking enables customers to conduct banking transactions without the necessity of physically visiting the bank. The E-banking system is currently prevalent due to its substantially lower transaction and delivery costs compared to traditional banking systems. E-banking simultaneously enhances a banker's efficiency, while reducing operational costs. In India, the transaction volume constituted 15.6 percent in 2020, while online payments and other electronic activities accounted for 22.9 percent in the same year. It is anticipated to attain 71% by 2025. Digitization is proliferating and progressing in the financial sector. Challenges are increasing in the protection of online banking transactions and financial data. E-banking facilitates the completion of tasks more efficiently and swiftly. However, concurrently, cybercrime has established its own prevalence and emerged as a significant security issue. The study primarily focuses on cyber fraud in banking, online transactions, obstacles in e-banking, and the consequences of cybercrime. It also provides numerous valuable recommendations on cybersecurity to prevent e-banking fraud.

**Keywords:** E-Banking, cybercrimes, customers, cyber-security, digitization,

## **Backdrop**

The banking industry has been providing services since the 18th century. The revolution in Information Technology (IT) has influenced the banking sector. Contemporary banks conduct their everyday operations reliant on information and data processing, underscoring the influence of information technology on the banking sector. The E-banking system is currently extensively embraced due to its substantially lower transaction and delivery costs compared to traditional banking systems. E-banking simultaneously enhances a banker's efficiency, while reducing operational costs. The corporate sector and average consumers have significantly benefited from the proliferation of E-banking. This has necessitated the protection of customers' personal information. Consequently, client satisfaction with E-banking services is of paramount importance.

## **Research Problem**

There is a significant transformation in the activities of the banking sector. To enhance the banking sector, information technology is utilized more efficiently for customer-oriented activities. This is one facet of the issue, whereas the opposing facet has its own challenges, such as cybercrime, internet fraud, and technological misuse. In this environment, there is a significant necessity to examine cyber dangers and preventive measures in E-banking to foster awareness and ensure the seamless operation of online banking.

**Objectives**

1. To examine E-banking and its advancements;

2. To identify the issues associated with E-banking and its effects on the banking sector; and 3. To comprehend the implications of cybercrime.  
3. To propose safety measures that facilitate a crime-free e-banking environment.

**Methodology**

The current data is derived from secondary sources. Data has been gathered from books, journals, cybercrime portal websites, and other pertinent online sources.

**Need For E-Banking**

The heightened volume of business transactions, intense rivalry, and cost management compelled all banks to implement information technology to enhance service delivery while minimizing transaction costs. Consequently, internet banking has become the foundation for over 80 percent of users globally, as it provides banking services in a cost-effective manner.

## **E-Banking Services**

Internet banking enables expedited access to banking transactions and is available 24/7. Conversely, it enhances the efficiency of the banker and reduces transaction costs for the banker. Debit card, credit card, automated teller machine (ATM), national electronic fund transfer (NEFT), point of sale (POS), mobile banking, internet banking, and account statements are among the prevalent services provided by e-banking.

**Cybercrime in Banking Industry**

The banking sector offers a range of services and products to consumers, including internet banking, online payments, mutual funds, and loans. Customers from any location can effortlessly access their accounts and conduct transactions via the internet on computer systems and mobile devices. Nonetheless, these services likewise possess a detrimental aspect, encompassing hackers and thefts. Cybercrime denotes digital misconduct in which the perpetrator engages in various offenses, such as the illicit transfer and extraction of funds, utilizing the internet, computers, mobile devices, or other electronic apparatuses. Criminals infiltrate consumer accounts via online banking platforms, perpetrating theft of funds and sensitive information.

The Table clearly indicates that cybercrimes have significantly escalated during the past five years. Cybercrime has increased from 21,746 incidents in 2017 to 52,974 cases in 2021, more than doubling in number. This suggests that the efforts implemented by the Government and banking sector to prevent E-banking crimes have been ineffective in curbing such offenses.

**E-Banking Challenges**

E-banking fraud is perpetrated via internet technology. Presently, internet banking is extensively utilized for many functions such as financial transfers, account management, online shopping, and bill payments. With the advent of internet banking and remote work, the menace of cybercrime has escalated. Customers have fallen victim to cybercriminals due to ignorance and negligence. Securing the data of a single computer is insufficient; it is important to protect many accounts using cloud services from various locations. Significant and prevalent forms of cyber fraud include:

1. Hacking: It constitutes unauthorized access to a system through infiltration of client accounts or online banking platforms. The objective might be accomplished via malicious links or other viruses disseminated by fraudsters employing various means to access internet-enabled devices.  
  
2. Keyboard Capturing: In keylogging, keystrokes are covertly recorded during financial transactions, allowing for the monitoring of an individual's activities without their awareness. These pose significant risks as sensitive information, such as banking and financial details, can be readily compromised.  
  
3. Spyware: It functions by collecting or relaying data between systems and websites. Spyware is employed for deceptive objectives. It installs autonomously or through pop-up adverts prompting the download of software designed to capture and expropriate web banking credentials, including login IDs, passwords, and credit or debit card information.

4. Phishing: This crime involves sending emails to online banking users that appear to originate from a legitimate source, so creating the illusion that the entity providing electronic services is authentic. Confidential data, including customer identification, debit and credit card numbers, card expiration dates, and CVV numbers, is taken. Phishers occasionally mimic bank officials, sending links to specific consumers that lead to a counterfeit website resembling the legitimate bank page, in order to obtain personal information for fraudulent transactions. Currently, phishing crimes are being perpetrated by SMS (smishing) and cellphone calls (voice phishing).

5. ATM scanning and POS crimes: This cybercrime predominantly occurs at ATM machines and point-of-sale systems. Scanners are positioned above the machine keypad to simulate a genuine keypad or a device attached to the card reader, creating the illusion of integration with the machines to capture PIN and card numbers, which are subsequently replicated to execute fraudulent transactions. It is a scheme for compromising ATM machines and point-of-sale systems.

6. Social Networks: Fraudsters utilize WhatsApp, Facebook, Twitter, and other social media platforms to fool people by disseminating links. Users accessing the link supplied by the fraudsters may be led to an alternate website, enabling the fraudsters to obtain information shared by account holders for illicit reasons.

7. Domain Name System (DNS) Cache Poisoning: DNS servers are compromised by poisoning due to a flaw in DNS software. Consequently, the server erroneously authenticates DNS answers to verify their origin from an authoritative source. Erroneous entries will be stored locally by the server and provided to all users that submit identical requests. An attacker can ultimately capture clients by faking an IP address and altering DNS entries for a bank website on a specific DNS server, substituting them with the IP address of a server they control, so facilitating the hijacking of consumers. DNS servers are employed within a corporate network to enhance resolution response times by storing previously obtained query results in cache.

8. Identity Theft: This is a prevalent tactic employed by cyber attackers, particularly targeting e-businesses such as online banking services. It is the practice of utilizing another individual's identity, including their name, date of birth, and address, for fraudulent purposes. Data acquired via identity theft can subsequently be employed for many illicit purposes.

9. Malware: The financial sector is now experiencing a significant increase in malware attacks. It constitutes a significant threat from cybercriminals and computer fraudsters. Attackers construct malicious code using various banking malware to steal users' financial information and other sensitive data, which can subsequently be utilized for illicit purposes. The swift proliferation of mobile devices, including smartphones and tablet PCs, is facilitating the advancement of harmful software, or malware.

10. Denial of Service (DoS): This refers to an attack executed by cybercriminals that obstructs network service for users. A Denial of Service (DoS) attack is perilous as it enables a fraudster to disrupt any service offered to the target client, rendering it unreachable by inundating it with traffic or transmitting data that induces a crash.

## **Impact Of Cybercrime**

The mean incidence of cybercrimes was recorded at 3.9 per hundred thousand individuals. According to the National Technical Research Organization (NTRO), 3,855 cybercrimes were perpetrated for financial gain, while the Indian Computer Emergency Response Team (CERT-In) documented 534 phishing attacks in 2020. Motives for cybercrimes include revenge, extortion, and political agendas. The progression of information technology and mobile networks has significantly contributed to the proliferation of financial services among the general populace. Currently, mobile phones are utilized for various activities, including online shopping, internet banking, and bill payments, rendering them increasingly susceptible to illegal surveillance aimed at extracting personal consumer information. Despite the banking business offering viable and cost-effective services through advancements in information technology, the likelihood of falling victim to cyber-attacks has significantly escalated. Banks must evaluate, redesign, and recalibrate their existing banking operations to assess and mitigate risks. Risk management has emerged as the central driving force.

## **Suggestions**

A highly regarded business research company has conducted a study indicating that nearly all cybercrimes are attributable to human negligence. Consequently, awareness of cybersecurity has become essential for all bank consumers. To mitigate cyber fraud, one must remain vigilant while utilizing technology.

**Safeguarding The Identity**

Users must protect their confidential information, such as personal details, family information, address, mobile number, and identity documents, from unknown individuals or organizations. If such information is necessary, it is prudent to thoroughly contemplate and comprehend the procedures employed by fraudsters and their social engineering tactics to obtain the information. It is additionally recommended that usernames and passwords should not be stored in web browsers on public platforms such as cyber cafes. Always remember to log out of your account after use.

## **Safe Banking Activities**

Associate the mobile phone and personal email with the corresponding bank accounts. Utilize message alert services for bank transactions and online banking accounts. Remain vigilant and frequently update the passwords for online financial accounts. If fraudsters have compromised an online account, promptly log in and alter the password to prevent future fraudulent activity.

## **Social Media And Mobile Security**

Fraudsters often build counterfeit profiles on social media to disseminate harmful content and exploit them for illicit objectives. It is recommended to use caution and refrain from accepting friend requests from unknown individuals on social media platforms. Do not install or download malicious software or updates; instead, utilize reputable and certified sources for these purposes. To maintain robust security, consistently update and upgrade mobile applications and software. Consistently disregard and limit pop-up adverts that purport to offer rapid financial gains or lottery winnings. It may constitute a hoax, potentially jeopardizing security. It is advisable not to disclose any financial information regarding bank accounts to unfamiliar individuals encountered on social media; instead, protect it using encryption.

## **Protection From Skimming**

To prevent cloning or unauthorized duplication of card information, it is essential to ensure that the payment receiver swipes credit and debit cards in the presence of the cardholder. It is recommended to refrain from revealing sensitive information, including personal identification number (PIN), one-time password (OTP), card number, and card verification value (CVV), to any individual, as cybercriminals may impersonate bank officials to illicitly acquire debit, credit, PIN, CVV, and expiration date details. Consistently establish a robust PIN and frequently modify it for enhanced safety and security.

**Securing The Device**

Cybercrimes can be initiated using harmful links or software. Cybercriminals utilize this device to extract data for illicit transactions. It is strongly recommended to install the most effective antivirus software and to maintain a firewall that blocks and eliminates harmful software from further activity. Consistently update software and programs to safeguard data against emerging cyber dangers.

**Vigilance To Doubtful Message And Calls**

It is advisable to exercise caution and refrain from responding to dubious emails, texts, or fraudulent calls soliciting debit card, credit card, account information, or any other financial data, even if they promise monetary credit or debit. Additionally, obstruct and notify the relevant authorities for prompt intervention.

## **Conclusion**

E-banking has gained prominence due to its convenience and flexibility. Customers could effortlessly and conveniently access their bank accounts. Although access to banks is increasing, it is also exerting a negative impact on the banking sector. Cybercrimes such as hacking, malware, phishing, spyware, and identity theft are executed using the internet to achieve malevolent financial objectives. For a bank to launch any financial goods or services, it need information technology, as the delivery of these offerings to customers is facilitated solely through technology. The banking business has embraced numerous technological advancements to expand its services, which have subsequently introduced risks and led to an increase in cybercrimes. Fraudsters are exploiting clients through this vulnerability in the financial system.

The imperative to avoid cybercrime has led to the development of numerous techniques that require individuals to provide identification and verification during E-banking transactions. Failure to comply will result in the user being barred from further online transactions. This study has established a conceptual framework for E-banking and cybercrimes inside the banking sector. The study has emphasized the security measures that might mitigate and avoid cyberthreats.  
Moreover, to address cybercrimes, the banking sector consistently employs diverse technologies and strategies to augment safety and security within the financial system. It is collaborating with national authorities to raise awareness among the public as part of a risk management strategy to eradicate cybercrime from cyberspace and to ensure a safe environment for online banking customers.

## **References**

1. Jansson, K. & Von Solms, R. (2013). Phishing for phishing awareness. Behavior & Information Technology, 32(6), 584–593.

2. Raghavan. R and Latha Parthiban (2014). The effect of cybercrime on a Bank's finances, International Journal of Current Research and Academic Review, 2 (2), 173-178.

3. Ajeet Singh Poonia (2014). Cybercrime, challenges and its classification, International Journal of Emerging Trends and Technology in Computer Science, 3(6).120-127.

4. Manjula, R.P & Dr. Shunmughan. R (2016). A study on customer preference towards cybercrime with banking industry, International Journal of Multidisciplinary Research and Modern Education, 2 (1), 597-603.

5. Seema Goel (2016). Cybercrime: A growing threats to Indian banking sector, International Journal of Science and Technology 5(12), 552- 558.

6. Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah (2017). A brief study on cybercrime and cyber laws of India, 4(6), 1633-1641.

7. Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas (2017). The effects of cyber threats on consumer behavior and e-banking services, International Journal of e-Education, e-Business, e- Management and e-Learning,7(5), 70-76.

8. Mayur Abhyankar, Ketan Patil (2019). A study of Frauds in Banking Industry, Indian Journal of Applied Research, Vol- 9(5), 16-17.

9. Harshita Singh Rao (2019). Cyber Crime in Banking Sector, International Journal of Research Granthaalayah, 7(1), 148-161

10. Dr. Vijayalakshmi P, Dr. V. Priyadarshini, Dr. Umamaheswari K (2021). Impacts of Cyber Crime on Internet Banking, International Journal of Engineering Technology and Management Sciences, 2(5), 30-34.

11. Vihang Dilip Gaokar, Karan Harish Tundejwala (2021). Cybercrime in online banking, International Journal of Advanced Research in Science, Communication and Technology 7(1), 377-379.

12. Dr. Ramachandra Reddy. B (2013). Emerging Challenges in E-Banking, Discovery Publishing House Pvt. Ltd., New Delhi.

## 