VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CYBER SECURITY THREAT IN THE DIGITAL BANKING SECTOR

- Satwik Jain* & Shivangi Sinha**

Abstract

With the rapid digitization of banking services, the digital banking sector faces multiple challenges in safeguarding its customers' sensitive information. This Research Paper conducts a detailed analysis of cybersecurity threats in the digital banking sector. It focuses on numerous sources of threats and will make the readers aware of various types of cyber threats they could suffer. This paper also discusses implementingmultiplecyber security methodsto prevent cyber fraud. The study revolved around recent Cyber threats in Digital Banking cases and even discussed in detail how fraudsters manage to commit such Cyber threats. The paper even made its readers aware of the RBI's guidelines for Cyber Fraud. There is no separate legislation for the protection of cyber fraud in the banking sector, so all such crimes are legislated by the Information Technology Actof 2000. In the Submissions, the paper suggested that there should be a separate investigation agency to investigate any cybercrime in the banking sector. The paper also focuses on making the bank's customers aware of the complaint redressal portal of RBI, which was created under the Integrated Ombudsman scheme in 2021.[1]

Keywords

Cyber Security, Banking frauds,online transactions, cyber attack

Introduction

Cyber threats are attempts to corrupt or steal data in a computer system. These cyber-threatsoriginate from various sources like websites or computer systems. The main task of

*Mr. Satwik Jain, Student,BB.A LL.B- 3rd Year,Bharati Vidyapeeth(Deemed to be University),New Law College,Pune

**Ms. Shivangi Sinha, Assistant Professor, Bharati Vidyapeeth(Deemed to be University),New Law College,Pune

Cyber threats is to obtain crucial information through online channels from many sectors through illicit means. Of these many sectors, the digital banking sector is affected by cyber threats in the highest number. A cyber threat is any illegal act that attempts to gain access to Digital Banking without authorization or permission from the Account holder and the Bank, and where, due to a security breach, the customers of a significant bank suffer heavy losses. In the year 2021, banks from all over the world have been attacked by hackers. Cybersecurity in digital banking aims to provide safeguard measures to the users' digital transactions through debit cards, credit cards, Unified Payment Interface(UPI), wallets, and many more.

Objectives of Research

1. To study the categories of Cyber threats in Digital banking.

2. To analyze the Current security systems for Digital banking.

3. To analyze solutions for the eradication of Cyber Attacks in the Digital Banking sector.

Concept of Cyber Space and Cyber Security Threat

Cyberspace is the virtual world created by machines. With the help of Cyberspace, people within the world can communicate with each other online. Hence, it facilitates easy and fast communication. In Cyberspace, users share essential information, interact with each other, and are involved in many other activities. We would say that cyberspace is related to usingthe Internet for different reasons, whether for e-commerce, digital banking, watching online movies, playing online games, etc.

Cybersecurity threats are certain activities done by individuals in cyberspace where the main goal is to steal data in cyberspace and cause financial losses to the other party by corrupting the data in cyberspace.

Some Sources from where such Cybersecurity Threats originate:

1. **Hostile Countries:** Some enemy countries or aggressive countries might threaten Cybersecurity in cyberspace by performing cyber attacks on local companies and institutions to cause them damage by stealing data or disturbing communication.
2. **Terror Groups:** Many times, terror groups threaten cybersecurity by launching cyber attacks that harm national security, disrupt economies, and might cause bodily harm to citizens.

3. **Criminal Groups:** These criminal organizations commit cyber attacks and use sensitive data for extortion, theft,and online scams.
4. **Hackers:** These individuals do cyber attacks for personal gain, revenge, financial gain, or political activity. These hackers often develop new threats to improve their standing in the hacker community.

Types of Cyber Security threats in the Digital banking sector:

Different types of Cyber Security threats faced in the banking sector are as follows:[2]

1. **Phishing:** In this type of Cyberattack, the attacker sends Electronic mail disguising himself as the trusted source (*Bank in the case of the Banking Sector*). These fraudulent e-mails often pretend to be from a reliable source and hence ask the targeted person to input his sensitive information, which then causes financial losses to customers in the banking sector.
2. **Malware Attacks:** Malware is the abbreviated form of 'malicious software,' which includes viruses, worms, trojans, spyware, and ransomware. For Instance, Malware attacks through viruses where malicious software enters the application, and when the application runs, this malicious code executes and corrupts the data within the application.

   This malware software affects digital banking by corrupting or stealing customers' sensitive data within a particular financial institution.
3. **Spoofing:** Spoofing is a form of cyber security threat where attackers create a fraudulent website's URL which looks similar to the Original Bank's website, and the majority of banking customers get confused with the fraudulent website and input their sensitive account information there, and hence they open the way for cybercriminals to use their sensitive information for illegal means.
4. **ATM Skimming:** ATM skimming is a type of payment through card fraud. Here, a recording machine is installed over the original ATM, which records the details of the Debit card and Credit card and helps the cybercriminals steal PINs and other information of credit cards and debit cards.

[2]Dr. S. Nagaraju, *A research study on cyber Security Issues Affecting online banking and online transactions in india*, Volume 9 Issue 2 , International Journal of Innovative research in technology, July 2022.

5. **Ransomware:** In such a type of cyber attack, the organization loses access to its own data and sensitive information, and attackers usually ask for a ransom to be paid to restore their access to their sensitive information.
6. **SIM Swap, i.e., Mobile Number Scam:** Under SIM swap, a fraudster gets a new SIM card from your mobile service provider using your registered mobile number. The scammer conducts financial transactions from your bank account by receiving the OTP and alerts needed. You must immediately report to your mobile service provider if your phone or SIM card is lost or has stopped working.

Cyber security in Digital Banking can be achieved through:

a. **Encryption:** There shall be the implementation of robust encryption protocols for data that is either in transit or static. Secure Sockets Layer(SSL) and Transport Layer Security(TLS) are commonly used to encrypt data between clients and servers.

b. **Multi-Factor Authentication(MFA):** One should pass through multiple steps to access their data and sensitive information, including a combination of passwords, biometrics, and one-time passwords abbreviated as OTP. It would be easier for cyber attackers to access the data if such data is protected at multiple levels.[3]

c. **Firewalland Intrusion Prevention Systems:** Use of firewalls to monitor and controlincoming and outgoing network traffic. Intrusion Prevention Systems(IPS) can recognize and stop the cyber threat.

d.**Regular Software Updates:** Keeping the software of the system up-to-date helps prevent cyber threats, as these updates usually change the encryption code from time to time, and hence, it makes it difficult for cyber attackers to steal sensitive information.

e. **Employee Training:** Give training to the employees about cybersecurity and teach them about the importance of maintaining a secure digital environment because most cyber attacks have taken place due to human error. Hence, ongoing training of these employees is crucial for protecting data through these cyber threats.

[3] Dr. Neelam Sethi, *Cyber Security Analysis in Banking Sector*, Volume 04, No. 03(I), International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS), , pg. no. 59-64, [2021]

f. **Customer Education:**The Banking institution must educate their customers about cybersecurity and make them create Strong passwords for their Net Banking and set strong PINs for their UPI, debit cards, and credit cards to avoid any such financial loss through cyberspace. The Banks must also educate their customers about various types of cyber fraud and methods to prevent such frauds or scams.

Various Cyber Attacks in Digital Banking Sectors:

1. **Cyber Attack on Axis Bank's Account Holder in Mumbai**

The cyber fraudsters somehow managed to change the registered mobile number and e-mail ID of the Axis Bank Customer account, which led to the loss of 41 lakh rupees as the fraudsters managed to break the fixed deposit with the Bank. The fraudster managed to bypass the two-way OTP authentication to break the FD.

- ***How the fraudster managedto change the Registered Mobile No. & E-mail:***

The Account holder received an anonymous SMS stating that the reward points had been credited to his account. Believing the message to be genuine, the account holder clicked on the provided link, got access to the account holder's device, and changed the registered mobile number and e-mail ID in the bank account.

- ***Unreliable sources should not be trusted:***

As in the present instance, the account holder got attracted to the reward points link and clicked on the link, which unfortunately incurred a heavy loss due to this cyber attack. So, being a Bank customer, you should be aware of the authorized and unauthorized websites and links and never put your account details or card details in any such link or website.

- ***RBI's guidelines relating to Cyber Fraud:[4]***

The RBI, in its guidelines, has divided the liability of cyber fraud into two parts:

i.) Zero Liability of a Customer

ii.) Limited Liability of a Customer

Zero Liability of a Customer:

Under this, if any unauthorized transactionhappens due to a deficiency of the bank, then the customer is entitled to the loss that is incurred.

[4]Economic Times , https://bfsi.economictimes.indiatimes.com/news/banking/cyber-fraudsters-break-axis-bank-customers-fixed-deposit-siphon-off-rs-41-lakh/105614828 (last visited January 26,2024)

Limited Liability of a Customer:

Under this, if any unauthorized transaction happened due to negligence by a customer, such as voluntarily, without due care, sharing his payment credentials, then the customer will bear the entire loss for such transaction.

2. **RBI Phishing Scam**

The Reserve Bank of India is also kept from the cyber fraudsters. These cyber fraudsters send a phishing e-mail pretending to be sent from the RBI. Inthis E-mail, the recipient is promised prize money of 10 Lakhs within 48 hours if they click on any such given link, which exactly looks like the RBI's official website, where the recipient is asked for his personal account details and gathers the data of the recipient and eventually causes the financial loss to such recipient by using there personal information.

3. **ATM system Hacked**

The ATM servers of Canara Bank were targeted in 2018 for cyber-attacks. 20 Lakhsrupees were cleared from numerous bank accounts. According to sources, cybercriminals had access to ATM information for more than 300 users, resulting in 50 victims. Hackers used skimming machines to capture information from debit cardholders. Transactions involving stolen information varied from Rs. 10,000 to Rs. 40,000. It can be avoided if the protection mechanisms in ATMs can be improved to avoid data misuse.

Legislation for prevention of Cyber fraud:

There is no separate legislation for preventing Cyber Attacks in the banking sector, but the Information Technology Actof 2000 governs it.[5]

We have mainly been accepting technology in our day-to-day lives, and the area of concern is regarding the safety measures of technology. The usage of digital banking has been increasing every day. Nevertheless, cyber fraudhas also been competitively growing. There has been an increase in cyber fraud in the banking sector. Digital banking fraud is a mala fide illegal act by any individual or configuration to obtain, illegally possess, or receive money/data from a bank or financial institution via the Internet. The Information Technology Act of 2000 is the primary Act that governs the

[5]Ahmed, M. Shuaib and M R, Akshayaa and Gopinathan, Dr. N., Cyber Law Vis-À-Vis Net Banking in Indian Sector [3849586] SSRN: (May19,2021)

banking process via the Internet. Cyber fraud includes malware attacks, phishing, vishing, etc. The substantive and procedural laws governing the areas of Information Technology, monetary and fiscal laws, and the relevant penal provisions are effective mechanisms to prevent Cyber Crimes.

The Information Technology Act of 2000 has incorporated specific legal provisions creating legal rights and corresponding duties to the bankers and the customer to counter such crimes. Failure to adhere to such law and penal provision has also been incorporated under the act. Apart from the relevant provisions of the Indian Penal Code, the IT Act also provides punitive provisions for identity theft and cheating through technology under Sections 66C and 66D of the Information Technology Act, along with a remedial right by way of compensation and penalty for breach of data under Section 43A and 72 of the Information Technology Act 2000.The IT Act of 2000 imposes a legal duty on bankers to protect the sensitive personal data or information in the system that it owns, holds, or operates. Any negligence on the part of the bankers in safeguarding the data would result in payment of damages in the way of compensation to the victims. There's also a punitive measure against the banker in the event of failure to maintain the confidentiality and privacy of its customers.

Cyber Law Jurisdiction

The Internet knows no boundaries; banking fraud and other crimes are committed both within and outside India, explicitly targeting banking operations in India through the computer system. Therefore, it becomes difficult for the prosecuting agencies to initiate actions against fraudsters and criminals outside India to address this issue. The Information Technology Act of 2000, by Section 75, grants universal jurisdiction for offenses committed by a criminal who attacks the computer system under operations in banks in India by hacking either by operating within India or outside India. Even the prosecuting agencies have now formed a dedicated cybercrime cell across all Indian districts to effectively redress the victim's grievance.

Conclusion

Due to too much convenience, cost-effectiveness, and rapid online transactions on the tips of our hands, Indian customers are attracted more and more towards these Digital transactions. On the other hand, it has become too cost-effective for Banks to maketheir customers use Digital Services; for instance, these days, the account

statement is sent through e-mails. Still, the earlier banks had to incur heavy investments in passbook printing of the customer's account, so generally, banks promote their online digital services and give certain online offers to attract customers to use their Digital services. However, due to the increase in online transactions, the cybersecurity of such financial institutionsis struggling and hence increasing the cyberattacks.

The increasing number of cyberattacks in the banking industry hasproven insufficient skills, and there is no legislation to tackle cyber fraud. Neither is there any investigating agency that could properly investigate cyber fraud. So engaging trained cybersecurity experts becomes fruitful for achieving faster and more precise results in cybercrime investigations.

Information Technology has evolved into the primary support structure for the digital banking system, offering essential assistance to its operations. The digital banking sector is vulnerable to cybercrimes such as phishing, hacking, forgery, and cheating. Preventive measures against these cybercrimes involve ensuring robust authentication, identification, and verification techniques. Cybersecurity is a paramount tool in the digital banking sector, which is crucial against cyber threats.

The rapid growth of digitalization in banking, marked by technologies like IMPS, RTGS, NEFT, Google Pay, Phone-Pe, and others, has increased cyber threats. Despite the widespread use of online banking, instances of cybercrime in the banking sector have surged. Reports indicate that 50% of cybercrimes are related to ATM, debit card, and net banking frauds. The banking sector faces a higher frequency of cyber attacksthan other industries.[6]

This paper examines cyber attacks in the banking sector and explores strategies for enhancing cybersecurity against such threats. Cyber threats, originating from various sources such as websites and computer systems, aim to compromise the data within a computer network or system. Digital banking is particularly susceptible to cyber threats, with attempts to obtain sensitive information through online channels being common. Cyber threats manifest as malicious acts that seek unauthorized access to digital banking platforms, aiming to compromise the security of account holders.

[6] Mrs Kalpana Nayar* Priyanka Rathod**,*CYBER SECURITY CHALLENGES IN INDIAN BANKS,* Volume 8, Issue 29, International Bilingual Peer Reviewed Referred Research Journal, Page Nos. 167-172, January-March(2021)

In 2021, banks worldwide experienced cyber-attacks, highlighting the urgency for robust cybersecurity measures. The primary goal of cybersecurity in digital banking is to implement safety measures to safeguard users' digital assets, including debit and credit cards, during transactions.

In case of any Cyber Fraud that happens to a person in the Banking sector due to negligence in the bank services and security, the Bank is entitled to compensate the customer and adequately investigate the Cyber Fraud by appointing an expert agency to investigate the matter. Suppose the bank does not follow up on the customer's complaints about the cyber fraud due to the bank's negligence. In that case, the customer who has suffered financial losses through cyber fraud can register their complaint to RBI directly under the Integrated Ombudsman Scheme,2021,[7] after 30 days of complaining to the unresolved financial institution.

Integrated Ombudsman Scheme 2021 will provide cost-free redress of customer complaints involving deficiency in services rendered by entities regulated by RBI if not resolved to the customers' satisfaction or not replied to within 30 days by the regulated entity.

[7]Reserve Bank of India-Complaint Portal ,https://cms.rbi.org.in/cms/indexpage.html#eng (last visited on January 26,2024)