Cyber Crime in Banking Sector a Study Related To Indian Perspective

Hardev Kaur
Assistant Prof. PG Dept. of Commerce and Business Management Trai Shatabdi Guru Gobind Singh Khalsa College, Amritsar.

Abstract: Growth of Information technology has completely changed the every sphere of people life, work, communicate, shop, and entertain. With the emergence of advanced technologies, everything is just a click away. The banking industry is not a exception in digital age. Long queues, endless paperwork, and time consuming banking tasks have now become a thing of the past. Now banks have been able to offer personalized services to their customers, automate tasks that were once manual and time consuming, and even reach new customers in remote areas. Modern Banks now becomes tech savvy. Foundation for induction of computer technology in Indian Banking sector was laid by Dr. Rangarajan Committee's two reports in the years 1984 and 1989. Both the reports had strongly recommended computerization of banking operations at various levels and suggested appropriate Infrastructure . The number of customer base has also increased because of the convenience in 'Anywhere Banking. As the old saying goes, "there are two sides to every coin." in same way it also gives rise to some serious growing issue in the form of cyber crime that can have significant financial and reputational consequences. Higher digitization and remote operations lead to increased vulnerabilities and open up opportunities for cyber criminals, exposing banks to breaches or hacking. Around 3 Lakh cyber crime incidents were reported in the year 2020. This paper mainly focuses on banking frauds in India, types of cyber fraud in banking transaction, hardship faced by cyber victims and techniques to avoid most of the banking fraud.

Keywords: Automate, Personalized, Infrastructure, Digitization, Exposing

INTRODUCTION

A prosperous banking system is pre requirement of any economy. In this technological era, the objectives cannot be achieved using traditional banking methods. But in today's world privacy is a myth. Protecting customer privacy is critically important for every bank. With the Internet we can do almost all banking transaction with just one click, quickly and efficiently. But graph of cyber crime is also rising at fast speed. Cyber crime is illegal activity involving computers, and network resources. Cyber criminals in banking commit activities like stealing data, hacking a computer system, identity theft, initiate phishing scams, spread malware, and begin other digital attacks. cyber criminal or hackers takes advantage of online transaction for their personal gain and commit fraud with their victims and take their money. Cyber criminal targets victims from private individuals to large corporate, through various forms of phishing and illegitimate installations of malicious software, which results in financial loss and sensitive data of customers and banks. Cyber crime can be carried out by individuals or organizations. Some cyber criminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers. Technically, the first cyber attack happened in France well before the internet was even invented, in 1834. Attackers stole financial market information by accessing the French telegraph system. Around 1 lakh cyber complaints have been registered with the National Cybercrime Reporting Portal since January 2023, and around Rs 17,000 crore in cash has been defrauded in the last one year," said a source. As per the data, around 40,000 mule bank accounts were detected in branches of SBI,10,000 in Punjab National Bank (including Oriental Bank of Commerce and United Bank of India), 7,000 in Canara Bank (including Syndicate Bank); 6,000 in Kotak Mahindra Bank, and 5,000 in Airtel Payments Bank. So protection from it become the hot cake in present. Numerous measures like cyber security can stop or minimize this, and if someone suffers from Cybercrime, the person can get legal help too.

LITERATURE REVIEW

Goel, 2016 explained that Indian customers are increasingly preferring online services due to convenience, cost-saving, and swift transactions. Financial institutions are offering attractive offers to

boost cashless transactions. However, cyber security measures are being outpaced by the dynamic technological landscape and improved intruder expertise. Cybercrime has unique features, such as anonymity, global victim reach, and swift results. Insufficient awareness campaigns and traditional law enforcement policies are insufficient to address evolving cybercrimes.

Kumar. D, 2019 discussed the prevalent occurrence of elderly individuals falling prey to cyber theft. Elderly individuals were being targeted through phone calls when they were asked for their One-Time Password (OTP).

Shah, 2020 study reveals a higher share of private and foreign bank crime related to online banking, ATM cards, and other digital transactions. Cybercrime is a global concern, with most crimes resulting from hacking and identity theft. Banks can only partially prevent these crimes, as they cannot stop users from using online banking and check their computers for malware. The study also shows that customers are not alert and have limited knowledge of cybercrimes. In India, cybercrimes are increasing, with most focusing on nationalized banks. Banks must educate users about cybercrimes and take precautions to safeguard their computers and personal data.

OBJECTIVE OF STUDY

- To describe the categories of cyber crimes.
- To highlight the notable cases of cyber crimes in Indian Bank history.
- To highlights Consequences on the Banking sector
- To analyze the legal framework related to cyber crime in India.
- To describe the strategies to protect from cyber crime.

Data sources

Basically this paper is descriptive in nature, so in order to learn as much as possible about the cyber crime review of historical studies is taken. We used mostly the secondary data sources like books, magazines, case studies, published research papers, bank's publications, websites of Indian Cybercrime Coordination Centre (I4C), and other government portals etc.

Different Categories of Cyber Crimes

Hacking Hacking refers to the unauthorized access and manipulation of mobile devices, computer systems, networks, or websites. The goal of hacking is often to steal sensitive data and documents , cause damage to or corrupt systems, gather information of users.

Phishing : Phishing, act of sending e-mail that appears to be from a reputable source, such as the recipient's bank or credit card provider, Attackers commonly use phishing emails to distribute malicious links or attachments that can extract login credentials, account numbers and other personal financial information from victims. The person is then asked to "update" or "confirm" their accounts, thereby unwittingly disclosing confidential information such as their Social Security number or a credit card number. Phishers can use public sources of information, such as LinkedIn, Face book and Twitter. These resources are often used to uncover information such as names, job titles and email addresses of potential victims to craft a believable phishing email.

Ransomware : Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. Cybercriminals demand ransom money from their victims in exchange for releasing the data. The computer itself may become locked, or the data on it might be encrypted, stolen or deleted. The attackers may also threaten to leak the data they steal.

Data Breaches : A data breach or data leak is the release of sensitive, confidential or protected data to an untrusted environment. Data breaches can occur as a result of a hacker attack, an inside job by individuals currently or previously employed by an organization. Its leads to loss of financial data such as credit card numbers, bank details, tax forms, invoices, financial statements, patents, trade secrets, blueprints, customer lists, contracts.

ATM Skimming : ATM skimming is a method used by fraudsters to steal card information from unsuspecting individuals when they use an ATM. The process involves installing a small, inconspicuous device—known as a skimmer—over the card slot of the ATM. This device is designed to capture the data stored on the magnetic stripe of your debit or credit card when you insert it to make a transaction. Criminals may install a pinhole camera or overlay a fake keypad on the ATM to

capture your PIN as you enter it. With both your card information and PIN in hand, fraudsters can create duplicate cards or make unauthorized transactions, leading to financial losses.

Insider Threats : An insider threat is a threat to an organization that occurs when a person with authorized access—such as an employee, contractor, or business partner—compromises an organization's data security, whether intentionally or accidentally. Insiders are individuals with legitimate access to the organization's buildings or computer networks. In addition to having authorized access to private resources, they often have knowledge of the organization's finances, pricing and business strategies, IT infrastructure, or business goals. An insider threat survey report issued in 2022 revealed that insider attacks have become more frequent and the number of incidents has risen 44% since 2020.

Distributed Denial of Service (DDoS) Attacks: A DDoS attack is a type of hacking attack that aims to disrupt the normal operations of a targeted server, service, or network by flooding it with internet traffic. Overwhelmed with traffic, the server or network can no longer handle normal requests, which causes it to significantly slow down or crash altogether .It's made possible with the use of a considerable number of compromised computer systems. In Simple words it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

Key Logging : It is referred to as "keystroke logging or keyboard capturing". It is the process of secretly recording (logging) the keys pressed on a keyboard so that the person using it is oblivious that their activities are being tracked and these are incredibly harmful for stealing confidential information such as banking details etc. It can record instant messages, email, passwords and any other information you type at any time using your keyboard. One common example of key logging hardware is a small, battery-sized device that connects between the keyboard and the computer. Since the device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user's behavior to physically hide such a device in plain sight.

Spyware : It is a type of malicious software – commonly known as malware – that gets installed on a digital device without the owner knowing it. Its main goal is collecting your sensitive information. This can be your location, camera, and microphone data, all messages you send/receive or the words you type, websites you visit, banking information, and passwords. . It is mostly installed by bogus 'pop up' advertisements to have software downloaded

Pharming : Pharming is a type of cyber attack involving the redirection of web traffic from a legitimate site to a fake site for the purpose of stealing usernames, passwords, financial data, and other personal information. Pharming operates by exploiting the Domain Name System (DNS). When you type a website address into your browser, the DNS translates it into an IP address, directing your browser to the correct website. In a pharming attack, the hacker manipulates the DNS entries, causing the browser to redirect to a fraudulent site.

Notable cases of cyber attack in Indian banking system

1. Cyber Attack on Cosmos Bank in Pune

Cosmos Cooperative Bank Ltd situated in Pune, which has 140 branches across India and over 2 million customers, said in its annual report for 2018-19 that it had suffered two separate cyber attacks in 2018 , which shaked the whole banking system in India. As per the case details, hackers stole information of the Cosmos Bank's VISA and RuPay card customers through a malware, attacked the SWIFT system (a vast messaging network banks used by financial institutions) and syphoned off more than ₹ 94 crore on August 11 and 13, 2018.The hackers had attacked the banks' ATM switch server and withdrawn ₹ 78 crore from various ATMs in 28 countries and another ₹ 2.5 crore was taken out within India. In another attack on August 13, the hackers again fraudulently transferred ₹ 13.92 crore to a Hong Kong-based bank using the proxy SWIFT system. Out of ₹ 13.92 crore, the police managed to recover ₹ 5.72 crore.. A court in Maharashtra's Pune district has convicted 11 people in the Cosmos Bank cyber fraud case.

2. ATM System Hacked

Canara Bank's ATM servers were targeted in mid-2018. According to sources, more than 300 users' ATM details were compromised by attackers and Rs 20 crore was wiped from various bank accounts.

Hackers used skimming machines to capture information from debit cardholders. Transactions made from stolen details

3. RBI Phishing Scam

The Reserve Bank of India was not spared by the cyber criminals. Fraudsters use enticing tactics like fake letterheads and email addresses of RBI, impersonating as employees of RBI or intimidating tactics via calls, SMS or emails impersonating as RBI officials threatening to freeze/block/deactivate bank accounts of recipients and convince them to install some unauthorized/ unverified application using a link provided in the website that looked exactly like the RBI's official website, complete with the same logo and web address. After that, the user is asked to disclose personal details such as his password, pin, and savings account number. The Reserve Bank of India (RBI) has cautioned the public against unscrupulous elements that use various methods to defraud people by using the name of the central bank in some capacity.

4. Cyber Attack on Union Bank of India

The cyber attack made on one of India's biggest banks; the Union Bank of India in 2017 was another shocking event. It was a classic case of phishing which triggered from an e-mail that was circulated in disguise from the most trustworthy organization RBI. The e-mail carrying malicious codes was circulated to few email ids of customer cares, individuals, and e-banking persons. Out of all, few people reported the email to security team of the bank. But unfortunately, there were few not-so-tech-savvy people who opened the e-mail and soon after the malicious code entered inside banks network and servers which made way for hackers to cause a theft attempt of $ 170 m. But the attackers made a small mistake of deleting the transactions from SWIFT files which were caught by treasury department in the backend while doing reconciliation of their Nostro account.

5. The Bank NSP Case

In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

Legal framework related to cyber crime in India

Cyber laws are becoming more important in India due to increase cases of cyber attacks. These are the strict rules that govern the use of information, software, financial transaction performed via digital means. These laws ensure safety and security clients personal data, funds, Identity and even to extend protection to banks from the threats arise from cyber attack. Indian Government enacted different laws and set up authority from time to time, which are mentioned below.

1. Indian Cybercrime Coordination Centre (I4C)

It is an initiative of the Ministry of Home Affairs, Government of India to deal with cyber crime in the country in a coordinated and comprehensive manner. I4C focuses on tackling all the issues related to Cybercrime for the citizens, which includes improving coordination between various Law Enforcement Agencies and the stakeholders, driving change in India's overall capability to tackle Cybercrime and to improve citizen satisfaction levels. Indian Cybercrime Coordination Centre scheme was approved on 05th October 2018. Since its roll out, it has worked towards enhancing the nation's collective capability to tackle cybercrimes and develop effective coordination among the Law Enforcement Agencies. The I4C was dedicated to the Nation on 10th January 2020 by Hon'ble Home Minister. I4C has a National Cyber Crime Reporting Portal (NCRP) i.e. www.cybercrime.gov.in wherein all the complaints pertaining to cybercrime are reported by the citizens and a helpline number 1930, wherein the financial cyber fraud complaints are reported by the citizens.

Objectives of I4C

- To act as a nodal point to curb Cybercrime in the country.
- To strengthen the fight against Cybercrime committed against women and children.
- Facilitate easy filing Cybercrime related complaints and identifying Cybercrime trends and patterns.

- To act as an early warning system for Law Enforcement Agencies for proactive Cybercrime prevention and detection.
- Awareness creation among public about preventing Cybercrime.
- Assist States/UTs in capacity building of Police Officers, Public Prosecutors and Judicial Officers in the area of cyber forensic, investigation, cyber hygiene, cyber-criminology, etc.

2 . Information Technology (IT) Act, 2000

The Information Technology Act, 2000 also Known as an IT Act is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of the United Nations by a resolution dated 30th January 1997. It is the most important law in India dealing with Cybercrime acts like hacking, data theft, spreading of computer viruses, identity theft, defamation (sending offensive messages), The main objective of this act is to carry out lawful and trustworthy electronic, digital, and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 94 sections. The important sections related to cyber offences as mentioned under the Information Technology Act, 2000 are :

Section 65: Tampering with computer source documents Any person who knowingly or intentionally conceals, destroys or alters, or causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable.

Section 66A: Punishment for sending offensive messages through communication service, etc.

Section 66C: Punishment for identity theft Any person who, fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person, shall be punished

Section 66E: Punishment for violation of privacy Any person who, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished; 'Publishes' means reproduction in the printed or electronic form and making it available for public.

Section 72: Penalty for breach of confidentiality and privacy If any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

3. Indian Penal Codes (IPC) Act, 1860

In order to control the rise in cybercrime cases, specific punishments are imposed under various sections of the India Penal Code, 1860.

Section 379: If a person commits theft either electronically or physically, he or she will be punished under the provisions of this Section. It states that "whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years or with fine, or with both.

Section 419: This Section deals with fraud such as email phishing or committing the crime of password theft for impersonating and collecting data for personal benefit. According to this Section, "Whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both

Section 465: The punishment for forgery, email spoofing, preparation of false documents, etc., are dealt with in Section 465 of the IPC. It states that anyone who commits forgery should be punished with imprisonment extending to two years, a fine, or both.

Section 468: This Section deals with the forgery of documents or electronic records for committing

other serious crimes such as cheating. As per the provisions of this Section, whoever commits such a crime shall be punished with imprisonment which may extend to seven years with a fine. It is a non-bail able offence.

Section 469: According to this Section, forgery for the purpose of harming reputation is a punishable offence. Section 469 states that "Whoever commits forgery, shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine."

Strategies to Protection from cyber attack

- Keep Software Up to Date

One of the easiest and most productive ways of protecting against cyber attacks is to update your software on a regular basis. Software patches that fix security flaws are commonly included within updates. You can remove potential points of entry for cybercriminals and protect your systems from attacks by immediately installing updates for your operating system, programs, and security tools.

- Encrypt Data When Sharing or Uploading Online

Best method of preventing cyber criminals from intercepting the data during transfers is by encrypting it or using a cloud storage service that provides end-to-end encryption. Also, if you are using the software to encrypt the data before storing it online, keep the decryption key safe. otherwise you will lose the data.

- Create Complex Passwords

Employees often have trouble remembering the user credentials and this is the reason they use simple credentials. But bad and insecure passwords may expose them to huge risks, making it possible for hackers to steal credentials. Use a combination of upper- and lowercase letters, numbers, and special characters to create strong passwords for your accounts.

Easy information like your full name or birth date should be prevented. Whenever possible, enable multifactor authentication (MFA). By anything above verification from users, such as a fingerprint scan or a one-time password, MFA adds an extra layer of security.

- Avoid using public computers

If you're about to do some personal transactions like banking or online shopping, do not do it using public computers. Other people who have used the computers before you may have put programs that can record the passwords you type in.

- Avoid downloading unknown applications

The Internet is full of free software from unknown sources. These kinds of programs normally carry malicious applications with it and installing it may infect and cause serious damage to your computer

- Educate and Train Employees

Prioritizing employee training and education is an essential approach for avoiding cyber attacks. Employees can learn about the most recent threats and best practices for preventing cyber attacks by taking part in complete cyber security awareness programs.

Topics like identifying phishing emails, creating secure passwords, and comprehending the significance of routine software updates can be covered in training sessions.

Giving employees knowledge allows them to serve as the first line of defense against potential cyber threats.

- Mobile Device Management Solution

A lot of business activity now happens on laptops, smart phones, and tablets. Plus, many people use laptops for their work. The mobile nature of all these devices means they are at high risk for being lost and/or stolen. All mobile devices (including laptops) should be enrolled and managed in a mobile device management (MDM) solution. If a device is lost or stolen, it can be quickly wiped so that unauthorized users cannot access any data

- Regularly Backup Your Data

Regularly backing up your data is essential for recovering from a cyber attack or system failure. Make sure your backup strategy is accurate by keeping copies of your data both locally and online. Be certain to store your backups securely and with encryption. Test your backups often to make sure they can be effectively restored if essential. By having backups in place, you can mitigate the impact of a cyber attack and minimize data loss.

- Secure Your Wi-Fi Networks

Wi-Fi networks can be vulnerable to unauthorized access if not properly secured. Change the default administrator credentials on your wireless routers and use strong, unique passwords for network access. To encrypt data sent over the network, enable network encryption, such as WPA2 or WPA3. Additionally, cover up the SSID (Service Set Identifier) of your network to hide it from view by potential attackers.

- Conduct Regular Security Audits

Regular security audits are crucial for identifying vulnerabilities and weaknesses in your systems and processes. Perform internal and external audits to assess your security posture. Engage third-party security experts to conduct penetration testing and vulnerability assessments. Address the identified issues promptly to maintain a robust security infrastructure

- Stay Informed and Updated

Staying informed about the latest cyber threats and cyber security predictions, along with security best practices, is essential for effectively preventing cyber attacks. Get access to reputable security newsletters like Sprintzeal, follow cyber security blogs and forums, and participate in industry events and conferences. By staying updated, you can proactively adapt your security measures to counter emerging threats and vulnerabilities.

Impact Of cyber Attack on Indian Banking Industry

The international day of banks 2024 which falls on December 4th highlights the indispensable role of trust in banking. However, as banking transitions from physical ledgers to digital platforms, the foundation of trust faces unprecedented challenges from cyber threats, data breaches, and phishing scams which threaten to erode customer confidence, making cyber security not just a technological necessity but a trust enabler. According to check point's threat intelligence report, banking and financial institutions in India experienced an average of 2,525 cyberattacks in the past six months, significantly higher than the global average of 1,674 attacks per organization. This places the financial sector among the most targeted industries in the country. Recently, a ransom ware attack on a technology service provider disrupted payment systems for nearly 300 smaller Indian local banks, causing a temporary shutdown. Over the past two decades, the financial sector has faced more than 20,000 cyberattacks, resulting in losses amounting to $20 billion, as highlighted in the RBI's financial stability report. Furthermore, reports suggest that 69% of reported cyberattacks targeted scheduled commercial banks (SCBS), followed by 19% affecting urban co-operative banks, and 12% involving non-banking financial companies (NBFC). According to data from IMF (international monetary fund) and advisen cyber loss data, in the last 20 years, the financial sector has lost $12 billion as a result of more than 20,000 cases of cyberattacks. India's impressive expansion in online transactions also coincides with an unpredicted hike in cyber frauds. According to data from the reserve bank of India, sent in response to the authors' right to information (RTI) application, □3,207 crore was lost because of 5,82,000 cases of cyber fraud between f.y 2020 and f.y 2024. Maharashtra accounts for more than one-fourth of the amount lost owing to cyber fraud in India, largely because Mumbai, as the country's commercial capital.

Consequences of Cyber-attacks on the Banking sector

- Financial Loss

Banks have to suffer large financial losses due to frequent Cyber attacks. These losses may be from outright financial theft, expenses for containing the assault, court costs, regulatory fines, and payments to impacted clients.

- Reputational Damage

A bank's reputation can be seriously harmed by cyberattacks. If banks are not able to protect the

money and data of customers then its adversely affact their loyalty and faith.

- Operational Disturbances

Banking operations may be interrupt by cyberattacks. These interruptions may result in lost business continuity, inconvenience to clients, and transaction halts as well as restricted access to online services and daily banking operations.

- Regulatory penalties

Strict regulatory standards for cyber security and data protection apply to banks. Successful cyber criminal have highlights the violations of these standards, which lead to imposition of penalties, fine and legal proceeding on the part of regulatory authorities.

- Huge Amount of Security overheads

Banks have to put huge money investments to strengthen their cyber security infrastructure. This entails carrying out extensive security assessments, introducing new security measures, updating systems, and giving employees more training.

- Legal Consequences

Sometimes after losing money and personal data in cyber attacks Customers may sue banks in court. Suits can lead to high settlements and legal costs, which put extra burden on banks financial resources.

- Decrease in customer Base

When Customer suffers loss, it directly shrink their confidence and loyalty. As a result customers decide to shift their accounts to other banks that they believe have stronger security infrastructure, which leads to decrease in customer base of particular bank in market.

- Decreases in Stock Prices

As a result of cyber attack, stock prices of banks shows a declining trend. The market cap of the bank drop due to lower trust of investors in the operation of banks.

- Psychological Effects on Staff Members

The emotional and psychological impact on individuals following losses related to cyber crime can range from mild to severe and lead to symptoms of depression, anxiety, panic attacks, stress, and even suicide, which lower their morale and reduce productivity.

- Reduction of Competitive Edge

A bank may lose its competitive edge if their strategies, Sensitive or confidential data is leaked out. Competitor may use this data to take advantage on the cost of other bank enhance their customer base in market.

CONCLUSION

Cyber issues are global issues now and increasing at a fast rate with new technological advancements. These attacks are not boundary restricted. It can be concluded that banks as a financial institution contain higher cyber risk as compare to other institutions. The increasing reliance of millions of people on online banking presents a significant challenge to cyber professionals in developing a cyber security infrastructure. But it's not only a duty of bank to keep watch but also on the part of public as well to be remain vigilant. They should adhere the cyber security protocols while performing banking transactions and used protective measures. People should not share their credentials with anyone. Any suspicious activity in any form must be reported immediately to the concerned authority to avoid undue hardship. Banks must educate their customers about potential threats and provide them with the tools and resources they need to protect their accounts. Therefore, it can be said that while it may not be able to completely eradicate cybercrime from the internet, it is still possible to keep an eye on banking transactions and activities on a regular basis. By adopting these strategies, banks can reduce the risk of cybercrime and ensure the security and integrity of their operations in the digital age.

REFERENCES

[1] Agrawal, S. (2016). Cyber Crime in Banking Sector*. Udgam Vigyati, 3, 1-19

[2] Bakshi, V.K., Neeta, M.S. (May 2019). Cybercrime in banking sector. Aayushi International Interdisciplinary Research Journal (AIIRJ). ISSN 2349-638X.

[3] Geeta, D. V. (2011), Online identity theft-an Indian perspective, Journal of Financial Crime, Vol. 18 No.3, pp. 235-246

[4] Goel, S. (2016). Cyber-Crime: A growing threat to Indian banking sector. International Journal of Science Technology and Management, 5(12), 552-559.
[5] Kumar, S., Koley, S., &Kuamr, U. (2015). Present scenario of cybercrime in India and its preventions. IJSER, 6(4), 1972-1976
[6] Mayur Abhyankar, Ketan Patil (2019),"A study of Frauds in Banking Industry", Indian Journal of Applied Research, Vol- 9(5).
[7] Reserve Bank of India, Department of Banking Supervision, Central Office, Mumba, Guidelines on Information Security, Electronic Banking, Technology Risk Management & Cyber Frauds
[8] Shah, I. (2020). Analysis of Cyber Crime in Banking Sector.
[9] http://www.cyberlawsindia.net/
[10] https://cybercrime.gov.in/
[11] https://i4c.mha.gov.in/