INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN(O): 2456-6683
Monthly Peer-Reviewed, Refereed, Indexed Journal [Impact Factor: 9.241]
Volume - 9, Issue - 4, April - 2025

DOIs:10.2017/IJRCS/202504011 --:-- Research Paper / Article / Review

Cyber Security in Banking Sector: Best Practices & Solutions to Avoid Cyber Attacks by Cybercriminals

Dasaka VSS Subrahmanyam
Prof. Dept of CSE,
Keshav Memorial Engineering College, Hyderabad, Telangana, India
Email – subrahmanyam.dvss@gmail.com,

Abstract: *Financial secutor, especially Banking sector, has become more vulnerable instrument when it comes to cyber attacks. Some of the world most ingenious unhethical hackers have been targeting Indian Banks regularlyto steal customers' hard earned money and sensitive data and also tracking ttheir financial operations regularly. Some important practices and solutions are necessiated to avoid threats (cyber-attacks) by cybercriminals.*

Key Words: *AePS, Banking Sector, Cyber-attacks, Cybercriminals, Cyber Security, Password, UPI Transactions.*

1. INTRODUCTION:

In this digital world, our bank is in our mobile phone. No customer needs to visit its bank physically for any kind of financial transactions. Every banking need is being done on mobile phones. Banks have been providing their apps for mobile phones. Customers are supposed to download their corresponding bank apps. The world has shifted to online banking with all technological developments taking place from time to time. It has become an ocean of opportunities for cybercriminals for their illegal activities. Different kinds of cyber threats and attacks were identified and corresponding and suitable measures were taken by the cyber-crime department, Government of India, from time to time. But cybercriminals have been adopting various kinds of novel methods to cheat public money from banks. They always try to commit financial frauds online and rob customers' money by sending fake messages, phishing emails, SMSs and malicious bank links. A report on cybercrime, which was published on 17 July 2024, says that cybercriminals have been on 24 x 7 work to call to bank customers pretending as bank officials, making communication with customers, gathering information by means of providing loans with very less interest, cheating customers by the name of OTP verification, verification of their KYC documents etc., There will be huge financial losses to banks and their customers, if customers were not educated on cyber threats and attacks. General public as well as customers have to take care of their personal information with careful measures. But every time cybercriminals have been changing their ways and inventing new tricks to dupe people online. So, much care is to be taken for online transactions. It has only been few years, that our law enforcement agencies have become vigilant in tracking and preventing various kinds of cybercrimes by cybercriminals online.

Bank frauds have seen a dramatic increase with reported cases more than tripling from 8,752 in the Financial Year 2021-2022 to 32,363 in the Financial Year 2024, resulting in losses exceedingly more than Rs. 2,700 crores. Indians have lost Rs. 485 crores to frauds on UPI (Unified Payments Interface) across 6,32,000 reported incidents during the Financial Year 2024. So, customers should be smarter for their online banking transactions. The awareness needs to be spread around the emerging cyber threats in the banking sector. At the same time all banking personnel should be given thorough training on how to detect cyber threats and attacks swiftly without happening any financial losses to banks. Thus, awareness programs from customers side and technical training programs from bank employees' side, are needed. It should be done in a holistic 360^0 approach.

Table 1: Online Bank Frauds (cyber-attacks) (in India):

S. No.	Financial Year	Nature of transactions	No. of reported cases	Financial loss in crores
1	2021 – 2022	Banking	8,752	
2	2022 – 2023	Banking	32,363	Rs. 2700

3	2023 – 2024	Banking		
4	2024 - 2025	UPI	6,32,000	Rs. 485

2. A NOVEL METHOD OF SCAMMING, BY CYBERCRIMINALS:

A novel method of scamming bank customers, to steal their hard-earned money illegally, has come to the notice of bank authorities, very recently. Now cybercriminals can rob customers' money from their respective bank accounts without using OTPs, making fake calls, sending SMSs, malicious links, and phishing emails. Now they are stealing money from bank accounts by using a system called AePS (Aadhar card Enabled Payment System). This new method has been adopted by cybercriminals. Cybercriminals/unethical hackers have always been lookout for flaws in systems' administration. AePS has been a new service, recently, introduced by the Central Government for public convenience. Now it has become a powerful weapon in the hands of fraudsters/cybercriminals, which further strengthens their teeth to steal money form customers' bank accounts. AePS enables users to withdraw money from their bank accounts by using their Aadhar card numbers and Biometrics (Finger prints) (without using their ATM cards and PIN numbers). Here in this system, customers who have their Aadhar cards linked to their mobile phones are only allowed to utilize this unique service. AePS service is not possible to utilize, for those customers whose mobile numbers are not linked with their Aadhar cards. Thus, unethical hackers can attack only Aadhar enabled mobile numbers.

AePS system = Aadhar card (linked with mobile number) + Biometrics ---------- (1)

All AePS enabled bank customers can now withdraw their money without using any chequebook or even an ATM card. But there is a transaction limit on withdrawing money from ATMs, where the transaction limit (upper limit) is imposed by the Reserve Bank of India (RBI). Now, cybercriminals are using this AePS method to withdraw money from customers' bank accounts without their knowledge. It has been an online method to commit financial frauds easily from customers' accounts. Two steps are involved in this cyber-attack:

Step I : For getting customers' mobile numbers: ---------- (2)

- Scammers are using customers' Aadhar card numbers.

Step II: For getting customers' Biometrics: ---------- (3)

- Scammers first concentrate on Land Allotment Records of targeted customers from the Sub-Registrar offices (which are Government offices of the concerned state Governments) of their locations.
- It is Because of the fact that all Land Records contain Bio-metrics (Finger prints) of the corresponding land owners.
- Scammers are collecting Fingerprints from the concerned Land Records easily.
- These are used for Biometric verification.

Thus, scammers collect required details of Aadhar card and Biometrics (Finger prints) of bank customers, easily. Then it will be a cakewalk for them to steal money from customers' bank accounts (without the knowledge of the concerned customers). No personal information on online seems to be protected from scammers. Otherwise, the pitfalls of being online will be increased non-linearly. It is not just to address the growing concerns of cyber security threats in banking sector but to make all general public to be aware of the impacts of cyber-attacks on financial domains. All banks have to provide the increased degree of cyber security to all of its customers and have to make on-hands technical training to its staff from time to time. In this novel method, all customers may not get affected but customers with available Biometric details will definitely be affected. It will have a severe negative impact on both sides of banks as well as customers. But customers' financial bases will severely be damaged. It is very difficult to recover money from cybercriminals, once cyber-attack takes place on customers' accounts. So, all primary measures are to be taken pre-cautiously in an order to avoid all kinds of cyber-attacks.

3. BEST PRACTICES & SOLUTIONS TO AVOID CYBER THREATS:

Best Practices:

Cyber security begins at the leaf node level of the tree structure of security measures. Primary security measures to begin at gross-root levels. These security measures (tips) will outsmart cybercriminals. The following measures are to be followed by banking sector for their financial, infrastructure (computer systems and software) and database protection as well as for protection of their customers too with respect to financial transactions and privacy aspects.

Measures to be undertaken to outsmart cybercriminals:

- OTP, CVV and PIN numbers are not to be shared with anyone.
- Use correct customer care numbers.
- Don't click on unknown/malicious links sent by emails or SMSs or Phone calls.
- Don't download banking apps (or any kind of apps) from unknown sources. Always use banking websites only.
- Don't share personal/confidential details over social media networks.
- Beware of submitting/updating KYC documents where cybercriminals send fake messages/emails saying that your bank account will be blocked unless send your latest KYC documents immediately.
- Be careful with UPI payment requests where fraudsters send fake payment requests asking to "accept" to receive money.
- Be cautious of trading scams- fraudsters promise "guaranteed high returns" in crypto currency, stock market, online betting etc.,
- One of the most recent scams is "Digital Arrest", where fraudsters posing as police or cybercrime officers or CBI officers call and claim that you are involved in illegal activities and demand huge amount of money to "clear your name from the list fraudsters" or ask you to stay on a video call for sharing an OTP number. Don't accept any video call from any unknown/suspicious mobile numbers. In most of the cases. Fraudsters make video calls. So, beware of video calls.
- Be aware of insurance policy frauds, where scammers pose as RBI/IRDAI officers and say that you are supposed to get more money from your previous insurance policy and pay amount to release the bonus insurance money immediately.
- Don't consider for Lottery money prizes, which are phishing mobile calls to lure innocent customers/public into trap to steal their money.
- Most recent scam has been emerged as "Gold and Silver Biscuits for low investment of money". Don't prey to these scams. All these calls are from the databases they acquired from retail shops, super markets, and from other shopping malls.
- Recently, in Hyderabad, one person got a mobile phone call that "5 acres of fertile agricultural land for only Rs. 10 lakhs as the land owner is moving abroad and the sale must be done by today itself and you are supposed to your details online and our person will meet you at a particular place for money. It is a kind of "Real Estate" scam. And also says that the land owner has an account in State Bank of India, that is why preference will be given to SBI account holders only.
- Password protection is very important. Don't share passwords with others. Don't use your date of birth/nick names/religious names as your passwords. These will be easily cracked by fraudsters by using Brute force password recognize software. Be careful with this. Don't share any kind of your personal information on social media.
- Our mobiles have become our world. Nothing could be done without mobile phones. So, more care is needed for mobile phones. Update mobile software periodically. Purchase mobile phones from branded companies. Previously, more data scams were happened by using China made mobile phones. These kinds of data breaching scams were revealed and very stringent actions were taken by the Central Government. Now these types of scams are reduced to a minimum level as they are being tracked and monitored by the Central Government agencies.
- Usage of mobile phones is to be restricted. Don't always be active on social media. Don't go for downloads always. Verification and authentication of links/URLs is always needed. Unnecessary downloading of links/URLs may download spy software/Ransomware/Malware into mobile phones. They are all hidden software and are as a part of free downloads. Once a mobile phone is inflicted by any kind of spyware/malware, then information of every financial and other important data will be in the hands of scammers. All information whether it is personal/financial/passwords everything will be revealed to others.
- So, beware of scammers and take all possible precautions in order to avoid any kind of cyber threats.

Best Solutions:

Cyber-attacks, sometimes, accidentally/without our knowledge, may happen even though utmost care is taken on banking transactions. The following actions are immediately needed in those incidents to avoid serious impact on financial transactions:

- Report online, immediately, to: www.cybercrime.gov.in

- Call the Cybercrime Number: 1930
- Report suspected fraud communications received through phone calls/SMS/WhatsApp calls to www.sancharsaathi.gov.in/sfc/
- Report to the concerned branch of the bank immediately.
- Block your concerned bank account and alert the Banking staff about your cyber-attack.

4. CONCLUSION:

In this digitalization era, everything being on mobile phones, life has become easy in all aspects. At the same time more online cybercrimes/frauds have been taking place on general public customers of financial institutions and the number of cyber-attacks is being increased non-linearly from time to time to rob money from banks and its customers by adopting various kinds of novel methods. Major unexpected cyber-attacks have been emerging from all corners of the globe. Most of the cyber-attacks are targeting Indians on their financial activities. In order to avoid any kind of novel cyber-attack by cybercriminals, all Governmental agencies, banking sector, insurance sector etc., and general public and customers of various organizations are to be protected. It is the time to educate and making general public known about various types of cybercrimes and their financial and privacy impacts on society and nation. The future belongs to cyber knowledge and its advancement.

REFERENCES:

1. Newspaper: The New Indian Express: Hyderabad Edition: Sunday Magazine: March 30, 2025.
2. Newspaper: The New Indian Express: Hyderabad Edition: Thursday: February 20, 2025.
3. Newspaper: The New Indian Express: Hyderabad Edition: Sunday Magazine: February 16, 2025.

Web References

1. www.cybercrime.gov.in
2. https://www.sancharsaathi.gov.in/sfc/
3. https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_2/IJCET_16_02_015.pdf