Cyber Threats and Implications: A Study from the Perspective of E-Banking

Dr. N.K. Pradeep Kumar

Department of Commerce, SVU College of CM&CS, S.V. University, Tirupati – 517 502

ABSTRACT

E-banking refers to electronic banking. E-banking is a generic term for the delivery of banking services and products through the electronic medium. Internet banking allows a customer to perform banking transactions without visiting physically to the bank. At present, E-banking system is widely accepted because cost of transactions and cost of delivering in E-banking are significantly lower than in the traditional banking system. At the same time, E-banking enables to increase the efficiency of a banker that lowers the cost of operation. In India, the share of transaction volume was 15.6 per cent in the year 2020, whereas online payments and other electronic activities were registered 22.9 per cent in the same year. It is expected to reach 71% by 2025. Digitization is expanding and advancing forward in banking sector. While challenges are also mounting in securing the online banking transaction and financial information. E- banking shoulders to get the work done easier and fast. But simultaneously cybercrime paved the way for itself and has become a security threat. The study mainly emphasizes on cyber frauds in bank, online transaction, challenges in e-banking, impact of cybercrime. It also offers ample of useful suggestions on cyber security to avoid e-banking fraud.

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

Backdrop

Banking Industry have been delivering services since 18th century. The revolution of Information and technology (IT) had a great impact on the banking sector. Nowadays banks have their daily operations based on the information and data processing confirming the impact of information technology on banks. At present, E-banking system is widely accepted because cost of transactions and cost of delivering in E-banking are significantly lower than in the traditional banking system. At the same time, E-banking enables to increase the efficiency of a banker that lowers the cost of operation. The corporate world and ordinary customer have been largely benefitted through the spread of E-banking. This has led to the need of safeguarding the confidential information of customers. Thus, satisfaction of consumer on E-banking services provided assumes a great significance.

Research Problem

It is evident that there is a sea changes in the operations of banking sector. In order to strengthen banking sector, information technology is more effectively used for customer friendly transactions. This is one side of aspect whereas another side has its own challenges like online crimes, internet frauds, misuse of technology etc. In this context, it is felt that there is a great need to look into the cyber threats and preventive measures of E-banking in order to create awareness and smooth functioning of online banking.

Objectives

1. To study E-banking and its advancement;
2. To identify the challenges involved in E-banking and its impact on banking sector; and To understand the impacts of cybercrime and its
3. To suggests safety measures that help to create crime free E-banking.

Data Collection

The present data is based on secondary source. Data has been collected from books, journals, websites of cybercrime portal and other related websites.

Need for E-banking

Increased volume of business transactions, high competition and cost control forced all the banks to adopt the information technology and serve the people in better way with low transaction cost. Thus, the internet banking has become a base to more than 80 per cent of customers worldwide due to the fact that it caters banking services in economical way.

E-banking Services

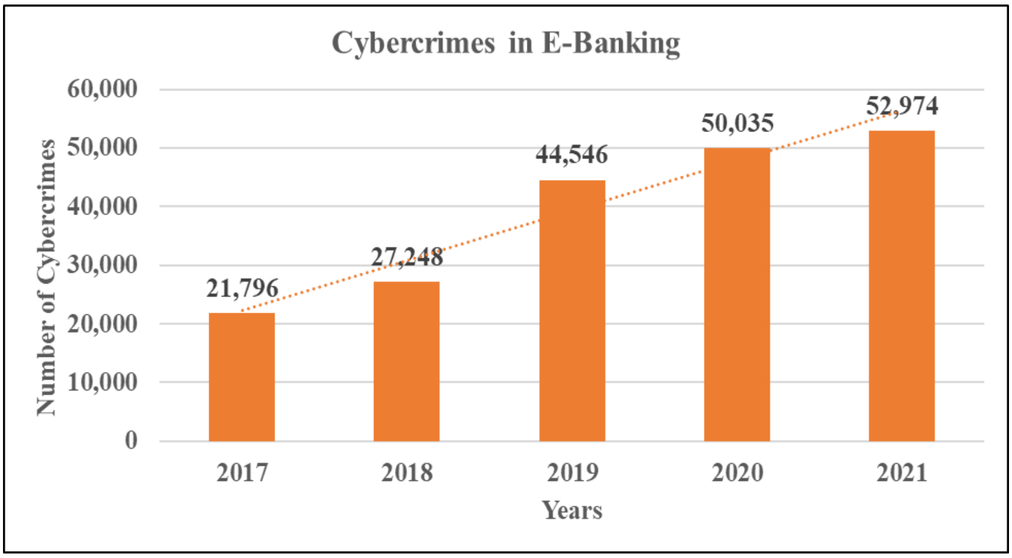
Internet banking facilitates faster access to bank transactions and available round the clock. On the other hand, it increases efficiency of the banker and saves transaction cost to the banker. Debit card, Credit card, Automated teller machine (ATM), National electronic fund transfer (NEFT), Point of sale (POS), Mobile banking, Internet banking and Statement of the account are some of the popular services offered by E-banking.

Cybercrime in Banking Industry

The banking industry provides various services and products to the consumers, for instance internet banking, online payment, mutual funds, loans and like. Customers from any place can easily access their accounts and do transactions using the internet in computer systems and mobile phones. However, these services also have an adverse side, which includes hackers and robberies. Cybercrime refers digital misconduct where the criminal performs a number of offences like transfer of money and unauthorized extraction of money by using the internet, computer, mobile or other electronic devices. Criminals break into customers account through web banking site, execute crime by stealing money and other sensitive information.

It is evident from the Table that, cybercrimes have rapidly aggravated in last five years. Cybercrime has recorded an overall rise from 21,746 cases in 2017 to 52,974 cases in 2021, which is more than the double. It indicates that measures catered by the Government and banking industry to avoid E-banking crimes had not been effective in controlling crimes.

Number of Cybercrimes related to E-banking



Source: www.statista.com

E-banking Challenges

E-banking crime is committed with internet technology. Currently, internet banking is widely used for many purposes like fund transfer, account details, shopping, payment of bills and so on. In the age of online banking and remote working, the threat of cybercrime has grown. Due to ignorance and negligence customers have gone into the clutches of cyber criminals. Securing the data of just one computer is not enough but of multiple accounts accessing cloud services from many different locations. Some important and most frequent cyber frauds are:

1. **Hacking:** It's an illegal access to a system by hacking into customers' accounts or home banking sites. The purpose can be achieved through malicious links, or any other virus sent by fraudsters using different methods to internet access devices.
2. **Keyboard Capturing:** In key logging, keyboard keys are captured secretly when the keys are pressed during the banking activity and the activities of the person is tracked without his knowledge. These are very dangerous as confidential information like banking details, financial details can be easily stolen.
3. **Spyware:** It operates by assembling or transmitting data between systems and websites. Spyware is used for fraudulent purposes. It is installs by itself or by pop up advertisements asking to download software to record and steal web banking credentials like login id, password, credit card and debit card details etc.
4. **Phishing:** In this type of crime an email is sent to online banking customers that seem to be from an authentic source by envisaging that the organization offering electronic services is a genuine one. And through this confidential data such as client identity, debit card and credit card numbers, card expiry date, CVV number and like is stolen. Sometimes, phishers impersonate as bank officials and send a link to the select bank customers that directs them to a counterfeit site which looks identical to the real bank page and acquire personal information for fraudulent transactions. These days phishing crime is also done through SMS (smishing) and mobile (voice phishing).
5. **ATM scanning and POS crimes**: This cybercrime is mostly carried out in ATM machines and POS. Here, scanners are installed above the machine keypad to give the impression of a real keypad

or a device made to be affixed to the card reader to appear as a part of the machines to retrieve PIN number and card numbers, which are then copied to perform deceitful transactions. It is a ploy for compromising ATM machines and POS systems.

6. **Social Networks:** Fraudsters through WhatsApp, Facebook, Twitters and other social network platforms deceive the users by sending a link. Users through the link provided by the fraudsters could be redirected to some other website from where the fraudsters can access information shared by the account holders for unauthorized purposes.
7. **Domain Name System (DNS) Cache Poisoning:** DNS servers are attacked by poisoning through an error in DNS software. As a result, the server authenticates DNS responses mistakenly to ensure that they are from an authoritative source. Incorrect entries will be cached locally by the server and served to all users who make the same request. Eventually an attacker can capture clients by spoofing an IP address, DNS entries for a bank website on a given DNS server and replace them with the IP address of a server they control enabling attackers to hijack customers. DNS servers are used in a company's network to increase resolution response times by caching query results previously received.
8. **Theft of Identity:** It is a most common strategy applied by cyber attackers when dealing with E-businesses mainly online banking services. It is an art of using someone else identity such as name, date of birth, and address for deceitful activities. Information obtained through identity theft can later be used for many unlawful activities.
9. **Malware:** These days banking industry is facing a huge rise in malware attacks. It is a serious threat from cyber criminals and computer fraudsters. A malicious code is created by attackers through various banking malware to steal user's financial information and other sensitive data which can later be used for unauthorized purpose. The rapid growth in mobile devices such as Smartphone and Tablet PCs is paving way for more development of the malicious software of malware.
10. **Denial of Services (DoS):** It is referred to the attack carried out by cyber criminals in denying network service to the users. DoS is so dangerous that fraudster can intervene in any service provided to the target customer and making it inaccessible by flooding with traffic, or sending information that triggers a crash.

Impact of Cybercrime

The average number of cybercrimes was registered at 3.9 per lakh population in 2021. As per National Technical Research Organization (NTRO) 3,855 cybercrimes are committed for financial gain and as per Indian Computer Emergency Response Team (CERT-In), 534 phishing incidents were recorded in the year 2020. Some of the motives for cybercrimes are revenge, extortion and political causes. The advancement of IT and mobile networks have played a significant role in the expansion of financial services to the masses. Nowadays, mobile phones are used for several activities such as online shopping, internet banking, payment of bills etc., making them more vulnerable as they are continuously watched by criminals to steal the confidential information of customers. Though, the banking industry is providing feasible and economical services through the advancement of IT, the chances of becoming a victim of cyber- attack has increased enormously. Banks have to review, re-engineer and reset their prevailing banking practices in order to appraise and reduce the risks. Risk management has become the core force.

Suggestions

A very renowned industry research organization has made a study that nearly all the cybercrimes are the part and parcel of human negligence. Thus, the awareness on cybersecurity has become vital to all the bank customers. To mitigate the cyber fraud, one has to be alert while using technology.

Safeguarding the identity

Users have to safeguard their confidential data like personal details, information of family, address, mobile number, identity proofs to unknown person or organization. If such information is required, it is advisable to take double thought and carefully understand the fraudsters strategies and social engineering to acquire the information. It is further suggested that username and password should not be saved in the web browser accessed in public platforms like cyber cafe. Never forget to sign off from account after using it.

Safe banking activities

Link mobile number and personal mail with respective bank accounts. Avail message alert services of bank transaction and online banking account. Be watchful and regularly change passwords of online banking accounts. If cybercriminals have hacked online account, then log in immediately into the account and change the account password preventing the criminal from further fraudulent use.

Social media and mobile security

Fake profiles are frequently created by fraudsters in social media with an intention to share harmful things and can use it for illegal purposes. It is advised to be careful and avoid friend request from unknown on social media platform. Never install or download malicious software/applications or malicious updates in existing applications rather use trusted and certified sources for the purpose. To ensure strong security regularly update and upgrade mobile apps and software. Always ignore and restrict pop-up advertisements claiming to earn money quickly or about winning a lottery. It could be a scam and security can be compromised. It is recommended that no financial details of bank account should be shared to a stranger person met on social media instead safeguard it through encryption.

Protection from skimming

To avoid cloning or unauthorized copying of card information, it is very vital to ensure that payment receiver swipes credit and debit cards in the presence. It is advised to avoid disclosing of information such as personal identification number (PIN), one time password (OTP), card number, card verification value (CVV) number etc., to any person as cyber criminals sometimes fake their identity and call impersonating as bank officials and try to obtain debit, credit, PIN, CVV, expiry date etc. Always set strong PIN and change the PIN often for more safety and security.

Securing the device

Cybercrimes can be triggered through a malicious links or malwares. Cybercriminals use this devise to steal the data for fraudulent transactions. It is highly endorsed to install best anti-virus and always being protected with firewall that block and removes the hazardous software from further action. Regularly update software and applications to protect data from new cyber threats.

Vigilance to doubtful message and calls

It is recommended to be cautious and not to respond to suspicious e-mails, messages, fake calls requesting the details of debit card, credit card, account info or any other financial data, even though they assure credit or debit of money. Moreover, block and report the same to the concerned officials for immediate action.

Conclusion

E-banking has become prominent because of its convenience and flexibility. Customers could access their bank accounts with ease and comfort. While this approach of access to the banks is on high, an adverse impact too is hitting on banking sector. Cybercrimes like hacking, malware, phishing, spyware, theft of identify and so on are perpetrated through internet to accomplish their malicious object of financial gains. If a bank has to introduce any financial products or services it need IT as the task can be reached to the customers with technology only. Banking industry for expansion of its services has adopted many technological innovations which in turn became risk and gave rise to many cybercrimes. Fraudsters through this vulnerability in the banking system are exploiting the customers.

The necessity of prevention of cybercrime has given rise to various techniques where a person whenever processes the E-banking transaction is asked for identification and verification. Failing to which the user will be prohibited from further online transaction process. The present study has provided a conceptual framework of E-banking and cybercrimes, present in the banking sector. The study has highlighted the security measures through which cyberthreats can be subsided and prevented.

Further, to combat cybercrimes, the banking industry is recurrently using various tools and techniques for the enhancement of safety and security in the banking system. It is coordinating with national authorities to create awareness among the people as a part of risk management process to eliminate cybercrime from the cyber space and to provide a haven for the users of online banking.

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.