ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 1, Mar 2022

A Study on Cyber Crimes with Special Reference to E-Banking Services

Amanpreet Kaur
GNDU Research Scholar, aman_batala15@yahoo.in

ABSTRACT

Cybercrime is an illegal criminal activity conducted by fraudsters with the use of computers and networks. It is unapproved access of sensitive information of individual or group of people's data and information is one side. In today's digitalization in banking system access banking services through electronic mode anywhere any time banking facilities. Customers are using online and offline modes for access services open in private websites for payments for buying and selling activities. The one face side is advantages and convenience and the other side with knowing or unknowingly without awareness threat to their account information from hackers and theft. The paper will provide information about cyber-crime, types of cybercrimes in the banking sector, IPC sections towards cybercrimes, and cyber-crimes trends through cases reported in recent years. Further, it will expand the study on cyber laws related to preventing cyber-crimes in the banking sector and strengthen the framework for E-banking growth. Finally suggests some safeguards to be maintained by banks and precautions to be taken by customers while accessing banking services electronically.

Keywords: ***Cyber-Crime, E-Banking, IT Act, IPC, Cyber Laws, Cyber Security***

Introduction

The banking sector is the main pillar of the economic growth of the country. Economic growth is mainly influenced by the demand for goods and services in the economy. Financial institutions like banks play a vital role in creating demand for goods and services by providing loans and other banking services. They also act as a medium for transactions. The banking sector's efficient functioning is a prerequisite for sustainable growth of the economy. In search of efficiency in functioning and improving service quality, e-banking has come and is more efficient than the traditional banking system. Through this, banking activities are made available for 24*7 days. It provides great opportunities for banks as well as customers to use it anywhere and anytime and work across the boundaries.

Cybercrime is a fraudulent activity where fraudsters use computers and network devices to steal data, money, or vital information without legal authorization to use or access the information or computer system. A person who is well-versed in the use of technology, such as electronic devices

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 1, Mar 2022

or computers, will trap, hack, and access the information of an individual without his or her consent or knowledge. Cyber-crimes in the banking sector are increasing as e-banking is still of recent origin and customer awareness about precautions and safety measures to be followed is still low. There is a shortage of skilled human resources in the banking sector and as new technologies are developed in the information technology sector, everyday fraud committers use this new technology to commit fraud.

Review of Literature

Shewangu Dzomira's (2014) study is conducted in Zimbabwe found that most of the cyber frauds are related to the banking industry. Major challenges are faced like lack of technology and detection tools, inadequate cyber-related laws, lack of awareness towards technology and researcher suggest addressing the cyber security issue and improving the technology to safeguard against cyber-attacks. **Jaro Jasmine and et al (2018)** internet banking witnessed a drastic change in the banking sector. The young generation has adopted the technology and using the same. IT Act, 2000 plays an important in preventing and securing E-banking practices in India. **Harshita Singh Rao (2019)** many of the cybercrimes are not reported due to protection-related issues and not any unified cybercrime announcing instrument. Need to revise the IT to be easily understood and user-friendly. **Mrs. Vinaya Chaturvedi's** study reveals that the use of internet service provides a greater opportunity to access information worldwide and helps to a large base for communication. The author suggests that while using the internet take precautionary measures to avoid data theft.

Objectives of the Study

- To study the various categories of cyber-crimes in the banking sector.
- To know the present scenario of cyber-crimes in e-banking
- To investigate E-banking cybercrime activities and related sections of the IPC.
- To suggest preventive measures to control cyber-crime in e-banking
- To offer valuable suggestions to improve cybercrime in e-banking

Research methodology

The present study is mainly based on secondary sources which are collected from the research articles, journals, and NPCI website, etc., and collected data were presented with help of chat.

Types of Cyber-Crimes

1. **Phishing:** phishing is a type of cyber fraud activity that fraudsters use to steal customers' personal information, like login details, credit or debit card numbers, and other details needed to commit fraud. Phishing involves creating a fake website for a bank or well-known company and asking customers by e-mail to open the link and fill in the details or update their information as requested in the link.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 1, Mar 2022

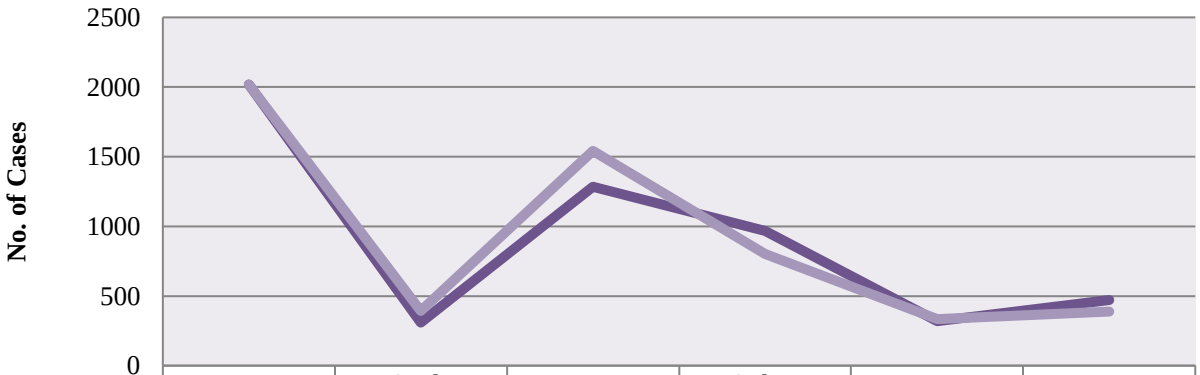
2. **Vishing:** is an electronic fraud activity that is used to collect the personal and financial information of the customer by unauthorised entities. In vishing, a fraud committer acts like a government official or bank official and obtains customers' personal information through phone calls, SMS, or mail services. Vishing also works like phishing. The main difference between them is that phishing is carried out through e-mail, while in vishing, different modes like mobile calls or SMS are also used.

3. **A Trojan** is a virus that, without the knowledge of the user, loads itself into the computer or mobile phone and executes its task of collecting personal data and forwarding this data to fraudsters/hackers. In the beginning, the hacker or fraudster sends a link to the victim. When the user opens the link, the Trojan virus loads and installs itself on the user's computer or mobile phone without his/her knowledge, opening the back door for the hacker to access the computer or mobile phone.

5. **Money Mule: The** money mule term is related to the innocent victims who are acting according to the fraudster's instructions. A money mule, also called a surfer, is a person who works for fraudsters and transfers money from his account to other accounts, thinking the money or transaction is legal, but it is illegal. With this money, transactions continue between money mule accounts till they reach the scam operator.

6. **Spyware:** Spyware is software that is used to monitor a device's activities and transfer data to the fraudster**.** It captures the information from the computer while transmitting it between the websites and the computer.

Cyber crime Cases in E-banking reported during the year 2016-2018



	Frauds	Credit card/Debit card	ATMs	Online Banking frauds	OTP frauds	Others
Series1	2018	309	1284	968	319	473
Series2	2017	395	1543	804	334	390

Source: National Crime Report Bureaus Report

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 1, Mar 2022

Interpretation: The number of cyber-crime cases related to credit/debit card has increased by the growth rate of 27% and atm related fraud cases reported has increased by the growth rate of 20% over the period of two years. The online banking fraud cases reported have a negative growth rate of 16%, and OTP frauds have increased by the growth rate of 4%. Other cyber-crime cases reported related to banking have decreased by a negative growth rate of 17%.

Information Technology Act, 2000: As amended by IT (Amendment) Act, 2008

The IT Act 2000 is the primary law in India and it was passed mainly to deal with electronic commerce and cyber activities. IT has transformed the way of doing business by changing operational environments in every field and reducing or eliminating the distance between the service provider and the user. Since the use of ICT in trade and commerce activities, the paper mode of transactions is being replaced by the electronic mode of transactions. The IT Act provided the legal framework for electronic commerce activities. This act is not applicable to the negotiable instruments, trusts, power of attorney, contracts for the sale of immovable property, wills, and other transactions notified by the Central Government.

In cyber-crimes, fraudsters hack into the electronic devices of the user and steal their personal and sensitive information and use that information to commit fraud in financial transactions or sell the stolen information to third parties.

Cyber-Crimes related to banking activities are charged under-

Sec.43 of the IT act provides that if any person introduces any computer contaminant or computer virus to a computer resource without the owner's permission, he/she is liable to pay damage by way of compensation to the person so affected, and may also be punished with imprisonment for a term of up to three years or with a fine of up to five lakh or with both.

Sec.65 of the IT Act states that anyone who knowingly or intentionally conceals or destroys any computer source code when it is required by law for the time being is punishable by up to three years in prison, a fine of up to two lakhs, or both.

Sec. 70 of the IT act authorises the government to declare a computer resource as a protected system and prohibit its access by the general public. Securing access or attempting to secure access to a protected system imposes imprisonment of up to 10 years with a fine.

Sec. 66C of the IT Act provides penalties for fraudulently or dishonestly making use of the electronic signature, password, or any other unique identification feature of any other person. Such a person is punished with imprisonment of up to three years and a fine of up to one lakh rupees.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 1, Mar 2022

Sec. 419 of the Indian Penal Code 1860 provides punishment of imprisonment for up to three years or a fine or both, for cheating by personation.

Sec. 66D of the IT Act specifically provides for the offence of cheating by personation using a computer resource. This attracts imprisonment of up to three years and a fine of up to one lakh rupees.

Sec. 72 of the IT act provides for a breach of confidentiality and privacy. It provides that if any person who has access to any electronic record, document, or other material, discloses such documents or other materials to any other person; they are punished with imprisonment of up to two years or up to one lakh rupees, or with both.

Generally, the above provisions of the IT Act 2000 and IPC 1860 are used to charge cybercrimes which are concerned with banking activities like phishing, hacking, ransom ware, viruses, spyware, and identity fraud or electronic theft.

Indian Penal Code (IPC) 1860:

Table 4: Indian Penal Code, 1860(IPC) is often invoked along with the IT Act, 2000

Frauds	**Sections**
Forgery	Section 464
Making the sale of documents	Section 465
Forgery for the purpose of cheating	Section 468
Reputation	Section 469
Using as genuine a forged document	Section 471
Possession of a document known to be forged and intending to use it as genuine	Section 474

Preventive Measures to control cybercrimes in E-banking.

1. Create awareness programs about the fake websites and advertisements that pop up when using the internet.
2. Raise awareness about how hackers can attack or infect a user's account or computer without the user's knowledge.
3. Users should be educated on how to use the internet safely, how to determine if their computer is infected with malware, and how to deal with it if it is.
4. Create awareness among bank customers not to share their card number or OTP with anyone.
5. Create awareness about the procedure that has to be followed by the user if and when he finds he is a victim of cybercrime.
6. Strict and stringent norms have to be put in place for the banks by the government and RBI to protect customers so that banks do not share mobile numbers or any other information

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 1, Mar 2022

about their customers, and they also do everything from their side to seal off any way that it is possible to commit fraud on their customers.

Challenges

1. It is difficult to identify or track the fraudsters and investigate them, and the origin of fraud activity is traced to a place because of VPN or other technology to hide IP addresses and because internet activity itself is borderless by nature.
2. Day by day, underground cybercrimes are increasing due to the new and advanced ways technologies are being innovated to commit fraud.
3. There is a shortage of skilled manpower in the banks' IT sections to encounter the cyber-crime activities or seal the loopholes in the system.
4. One of the major challenges in preventing cybercrime is software piracy; it aids in the spread of malware, viruses, and Trojans.
5. Lack of awareness among the bank's staff and customers
6. Lack of adequate and fast fraud detection tools
7. Failure to manage potential risk assessment tools

Suggestions to secure online transactions

1. Before making any online transactions, first check the network connectivity. It helps to avoid entering details again and again.
2. Before doing any transactions in digital mode, check whether the website is secure or not. Unsecured websites are used to hack and steal information like debit and credit card numbers, CVV numbers, expiry dates, etc., and also get malware into the system for other sensitive information.
3. Delete the spam e-mails and empty the trash box, as it helps to prevent accidentally clicking on the provided same link, which is normally used to get malware into the system.
4. Do not open unauthorised e-mails and/or give replies to those e-mails.
5. Do not share the OTP, ATM card, and other related information like card number, PIN, CVV number, expiry date, online banking registered used ID, password, registered phone number, date of birth, etc. with anyone who asks them.
6. Do not save the e-mail ID and password on any website, authorised or unauthorized, and after they complete the transaction, never forget to log out. While doing online shopping, never save the debit or credit card details, CVV number, and expiry date.
7. Do not share the contact number that is given to the bank.
8. By creating a strong password for logging into your account, you can avoid the account being accessed by fraudsters by making assumptions from the stolen information they have accessed. Do not use passwords like your date of birth or names that are easy to guess.
9. Beware of the false messages and avoid clicking on those links which offer prizes, money, gifts, or lottery tickets, as fraudsters use these to infect malware or use the information one provides here for their benefits.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 1, Mar 2022

References

1. Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah - A brief study on Cyber Crime and Cyber Laws of India. International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06 | June -2017
2. Jigar Shah - A Study of Awareness about Cyber Laws for Indian Youth. International Journal of Trend in Scientific Research and Development, Volume 1(1), ISSN: 2456-6470.
3. Yougal Joshi, Anand Singh - A Study on Cyber Crime and Security Scenario in INDIA. International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013 ISSN No.: 2250-0758
4. A.R. Raghavan & Latha Parthiban - The Growing Case of Cybercrime and Types of Cybercrime on a Global Scale. Journal of Computer Science Engineering and Information Technology Research (JCSEITR) ISSN (P): 2250-2416; ISSN (E): Applied Vol. 4, Issue 2, and Apr 2014, 1-6.
5. Ms. Anisha - Awareness and strategy to prevent Cybercrimes: An Indian Perspective. INDIAN JOURNAL OF APPLIED RESEARCH, Volume - 7 | Issue - 4 | April-2017 | ISSN - 2249-555X.
6. https://www.researchgate.net/publication/282281593 Electronic fraud cyber fraud risk in the banking industry Zimbabwe. DOI: 10.22495/rgcv4i2art2.
7. Jaro Jasmine and Aswathy Rajan, 2018 - A Critical Study on Concept of E-Banking and Various Challenges of IT in India with Special Reference to RBI"S Role in Safe Banking Practices. 135. Pdf (acadpubl.eu).
8. Harshita Singh Rao. (2019). "Cyber Crime in Banking Sector." International Journal of Research - Granthaalayah, 7(1), 148-161. https://doi.org/10.5281/zenodo.2550185.
9. Mrs. Vinaya Chaturvedi - Cyber Crime: Technological Blight in Digital Banking in India. 10. 55-62.pdf (iosrjournals.org).
10. Suresh V. Nadagoudar, Chandrika m p – Law relating to e-banking in India-An outreach challenge. International Journal of Current Research Vol. 5, Issue, 11, pp. 3508-3512 November 2013.