CYBER CRIME: A GROWING THREAT TO INDIAN E-BANKING SECTOR

Author 1: Mrs. S. KALPANA

Research Scholar, PG & Research Department of Commerce(CA), Hindusthan college of Arts and Science(A), Coimbatore, Tamilnadu, India.

Author 2: Dr. M.MAHALAKSHMI

Professor, , PG & Research Department of Commerce(CA), Hindusthan college of Arts and Science(A), Coimbatore, Tamilnadu, India.

ABSTRACT: Information and communication Technology has become an integral part of our day to day life. With the cheap availability of broadband and smart phones, almost everyone has access to the cyber space, connecting virtually at millions of online users across the globe. Increasing use of cyber space has also made us vulnerable to cybercrime threats. A minor laps/ negligence in managing our digital life can open doors for cybercrimes and hence can lead to financial loss. So, we must be vigilant and careful while connecting digitally to the outside world whether for financial transactions, social networking, playing games or searching things on the internet etc. This paper provides an overview of cyber crimes in E- banking sector and general tips to prevent themselves from becoming a victim of cybercrime.

KEYWORDS: *Cybercrime, E- Banking, preventive measures.*

I. INTRODUCTION

Banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking. The banking industry has enjoyed the ride of emerging technology to undergo significant changes and has witnessed expansion of its services and strives to provide better customer facility through technology with the swift expansion of computer and internet technologies, on the other hand, there have been risks involved in it as well. Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks.

Electronic Banking or e-banking refers to a system where banking activities are carried out using informational and computer technology over human resource. In comparison to traditional banking services, in e-banking there is no physical interaction between the bank and the customers. E-banking is

the delivery of bank's information and services by banks to customers via different delivery platforms that can be used with different terminal devices such as personal computer and a mobile phone with browser or desktop software, telephone or digital television.

II. REVIEW OF LITERATURE

RBI, Cybercrime fraud 2019, The total value of bank frauds more than doubled in 2019-20. Total cases of frauds have increased 159% by value to Rs 1.85 lakh crore, compared to Rs 71,543 crore in 2018-19.Similarly, the frauds increased 28% by volume to 8,707 cases in 2019-20, compared to 6,799 instances in the previous year, as per data released by Reserve Bank of India (RBI) in its annual report.

Balasubramanian et al, (2014) analysed the success of Information System in internet banking and its security challenges. 52 respondents were surveyed customers have fear that information sent by them through internet is not protected also have threat of their banks website getting hacked. The customers also have the fear of the malware attacks. The customers have the doubt about the security system of being reliable for internet banking services.

III. STATEMENT OF THE PROBLEM

Today, web technology has emerged as an integral and indispensable part of the Indian Banking sector. The enlargement of non-cash based transactions around the globe has resulted in the steady development of robust online payment systems.

The last few years have seen a significant increase in cybercrime across all sectors and geographies. Given the proliferation of this technological crime, organizations face a significant challenge to be resistant against cyber-attacks. Digital India may have become a soft target for criminals as country recorded a huge increase of 63.5 percent in cyber-crime cases in the year 2019, showed the National Crime Record Bureau data. The NCRB's data stated that 44,546 cases of cyber-crimes were registered in 2019 as compared to 28,248 in 2018.

This research attempts to analyses the concerns of cybercrimes in E-banking sector by highlighting the various wrongdoings are reported on a regular basis in the Indian Banking Sector. There is a need to analyses the nature of such crimes so that appropriate preventive measures may be devised.

IV. OBJECTIVES

- To identify the various cyber crimes in E- banking sector in India.
- To provide the preventive measures to control the cyber crimes in India.

V. RESEARCH DESIGN

The focus of the study has been on describing the various cybercrimes and the preventive measure to overcome these issues. The research design chosen for the study has been descriptive and the secondary data source has been collected through web-sites, books and journals. The period of the study was taken till December 2020.

VI. LIMITATIONS OF THE STUDY

This study focuses on the cybercrimes related only to the Indian E- banking sector. It does not cover the whole financial sector. All aspects area and measures covered are limited to the Mobile and Internet Banking users.

VII. CYBER CRIME IN E-BANKING SECTOR

In general cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime".

Cyber fraud cases in banks have become quite common which cause heavy loss of money to the customers every year. Cybercrime can be described as any criminal activity done using computers and the Internet. This includes anything from illegally downloading files to stealing millions of rupees from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. More than half of the population is connected to web these days and every individual has easy access of internet for their daily routine purposes like banking, entertainment, education etc. The availability and use of smart phones have really added weight age to the remarkable growth in the internet. The demand of online services has made a challenge for providing security to the customers, mainly due to increase in cybercrimes, which is serious threat to the financial institutions and banks. Cybercrimes can take many forms like E-laundry, ATM fraud, credit card fraud, etc. There have been significant changes in banking industry due to emerging technologies and IT revolution.

However, from the aspect of financial cybercrimes committed electronically, the following categories are predominant:

- **Hacking:** It is a technique to gain illegal access to a computer or network in order to steal, corrupt, or illegitimately view data.

Preventive measures:

- Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches and Protect systems/devices through security software such as anti-virus with the latest version.
- Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.
- Ensure all devices/accounts are protected by a strong PIN or pass code. Never share the PIN or password with anyone.
- Computers/laptops should have a firewall and antivirus installed, enabled and updated with latest versions.
- Never download or install pirated software, applications etc. on your computer, laptops or hand-held devices.
- Always scan external devices for viruses, while connecting to the computer.

- Be careful while browsing through a public Wi-Fi and avoid logging in to personal and professional accounts while using public Wi-Fi systems.

➢ **Phishing:** It is a technique to obtain confidential information such as usernames, passwords, and debit/credit card details, by impersonating as a trustworthy entity in an electronic communication and replay the same details for malicious reasons.

Preventive measures:

- Ensure all devices/accounts are protected by a strong PIN or pass code. Never share your PIN or password with anyone.
- Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.

➢ **Vishing:** It is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward.

Preventive measures:

- Remember bank never asks for card number/CVV number/OTP.
- Never share the ATM card number, CVV, OTP or any other confidential banking credentials with anyone over a phone call/SMS/WhatsApp.

➢ **Spamming:** Unwanted and unsolicited e-mails usually sent in bulk in an attempt to force the message on people who would not otherwise choose to receive it are referred to as Spam E-mails.

Preventive measures:

- Never give out or post your email address publicly
- Think before you click and do not reply to spam messages
- Download spam filtering tools and anti-virus software
- Avoid using your personal or business email address

➢ **Denial of Service:** This attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service by "flooding" a network to disallow legitimate network traffic, disrupt connections between two machines to prohibit access to a service or prevent a particular individual from accessing a service.

Preventive measures:

- Buy more Bandwidth
- Build redundancy into the Infrastructure
- Configure your network hardware against DDos attacks

➢ **ATM Skimming and Point of Sale Crimes:** It is a technique of compromising the ATM machine or POS systems by installing a skimming device atop the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine. Additionally,

malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number (PIN) codes that are later replicated to carry out fraudulent transactions.

Preventive measures:

- Observe the surroundings for skimmers or people observing the PIN before using an ATM and Cover the keypad when entering the PIN.
- Check your bank and credit card statements often
- Enter the PIN yourself taking due care to hide the PIN
- Physically check the keypad to ensure it does not have an overlay device.
- Do not allow anyone to stand beside or behind you while carrying out transaction with ATM/Debit card/Credit card.
- Do not keep a PIN which can be guessed easily. Keep changing the PIN.
- Ensure you get transaction receipt or confirmation through SMS.
- Ensure that any part of the ATM machine is open or loosely attached.

➢ **Virus, worms & Trojans:** Computer Virus is a program written to enter to your computer and damage/alter your files/data and replicate them. Worms is malicious programs that make copies of themselves again and again on the local drive, network shares, etc.A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

Preventive measures:

- Get a good anti-virus
- Be wary of e-mail attachment
- Avoid the Third Party Downloads
- Have a Hardware-based firewall and deploy DNS

➢ **Impersonation and Identity theft:** Impersonation and identity theft is an act of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person.

Preventive measures:

- Never provide details or copy of identity proofs (e.g. PAN Card, Aadhaar Card, Voter Card, Driving License, Address Proof) to unknown person/organization.
- Be careful while using identity proofs at suspicious places.
- Do not share sensitive personal information (like Date of Birth, Birth Place, Family Details, Address, Phone Number) on public platforms.

- Always strike out the photo copy of the identity proof; write the purpose of its usage overlapping the photo copy. This way, it becomes difficult to reuse the photo copy.
- Do not leave your credit, debit or ATM card receipts behind, in places such as a bank/ATM or a store; never throw them away in public.

➢ **Fraud by request money QR code/link on Google pay/Phonepe/Paytm:** Cyber fraudsters send debit links or QR codes to victims to scan and receive money in their bank accounts through Google Pay/PhonePe/Paytm. But instead of receiving money, it actually gets debited from the victim's account as fraudsters actually send a request money QR code/link.

Preventive measures:

- Never accept/click on any link or scan any QR code from unverified sources as they may send you a manipulated one.
- For receiving money, there is no need to enter MPIN or UPI PIN.

VIII. CONCLUSION

In present scenario, Indian banking sector cannot avoid banking activities carried out through electronic medium but Cyber crime is more serious offence than the real life crimes, in order to overcome this problem the victims should report these cases to the nearest police station and cyber fraud council in banks. In order to stop these issues, the legislature should keep a track on the working system of banks and law implementation should strict to monitor such wrongdoings and moreover banks should educate the customers regarding the awareness of cyber crimes often.

REFERENCES

1. Mayur Abhyankar, Ketan Patil (2019),"A study of Frauds in Banking Industry", *Indian Journal of Applied Research*, Vol- 9(5).

2. Harshita Singh Rao (2019)," cyber crime in banking sector", *International Journal of Research – Granthaalayah*, Vol- 7(1) PP.148.

3. India Banking Fraud Survey, Edition-II,(April 2015),www.deloitte.com/in

4. http://www.cyberlawsindia.net/

5. https://cybercrime.gov.in/Webform/CrimeCatDes.aspx