THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22- Issue-14-December-2019

A Study On Cyber Security Threats In Banking Industry

K. Jeevan Kumar
Assistant Professor
Vidya Jyothi Institute of Technology (Autonomous)
Hyderabad
Jeevan786kumar@gmail.com

Abstract:
In Present global scenario technology is playing a vital role be in all aspects of human life be it banking, business, education, sports and games. With the advancement in technology the banking industry is continuing to grownon cash based transactions around the globe and resulted in the online banking. In the present world Internet crimes is making huge losses to many people and they have been victims of cyber related crimes like hacking, identity theft, cyber virus and losing their money.Online related crimes represent huge risk to the financial institutions. This paper focuses on various forms of cyber-crimes and trying to provide measures to control cyber-crimes in the present global world.

Keywords: *Banking industry, Cyber Hacking, virus, identity theft.*

(I)INTRODUCTION:

Money is the life blood of all transactions beit business, government but also in an individual's life. Banking sector is playing a important role in the country for the smooth flow of financial transactions and also acting as a backbone of our economy. It accepts deposits from the investor at a lower interest rate and gives loans to the borrower at a higher interest rate, and helps the client in transferring the money from one account to another. In Present global scenario technology is playing a vital role in all aspects of human life be it banking services, business, education, sports, and games, Technology and internet changed the traditional banking services to online banking transactions benefiting the users to do the transactions quickly, easily, by saving time, and providing the services24x7 in all 365 days in ayear. For easy earning of money some group of people are using the technology in unethical manner and committing the cyber-crimeslike hacking, identify theft, cyber virus etc. Online related crimes represent huge risk to the financial institutions and such types of attacks are increasing day by day. Banks are not successful in controlling thesecyber crimes.

(II) LITERATURE REVIEW:

This review gives the information on cyber-crime related to digital transaction on the Banking Industries.

[1] KrishanTuli and Dr. Neenu Juneja (2016) revealed in their study that as long as hacking, identity theft and online frauds are easily accessible to have a financial gain the cyber-crimes will increase. Efforts must be made to eliminate the Anti-fraud activities by providing safety measures.

[2] Sultana Sharmeen Karim (2016) states that the banking industry can avoid cyber-crimes by updating their technologies and also by creating a awareness among the banks and their

customers and also suggested that the IT Act must be amended in such a way to combat cyber crime.

[3] Shubhamkumar, Dr. Santanu Koley, Udaykumar (2015) gave the basic idea how to control the cyber crimes , they opinioned that by learning from the past cyber crimes incidents, we can take safety measures to avoid the future crimes. Cyber Law should be updated from time to time.

[4] Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru (2018)revealed in their studythat cyber crimes are increasing year by year with the help of internet, RBI recommended to develop the software as a precautionary measure to control the cyber crime. Banks have to take quickly suitable measures to control and reduce the cyber crimes, this will help in the overall growth and development of the financial institution in the society.

(III) NEED FOR STUDY:

E – Banking in India is playing a important role in improving the quality service in Commercial banks. Financial institutions are adapting and providing online transactions to the bank customers. Although E – Banking transactions growing, but still customers are having a fear of security problems in their mind. Hence it is important to identify the drawbacks existing in the Banking Sector in order to reduce the fraudulent activities and to take corrective measures to control the cyber crimes.

(IV) OBJECTIVES OF THE STUDY:

1. To understand how the cyber-crime operation work.
2. To study the fraud detection in the financial institutions.
3. To analyze and use the preventive measures available for controlling frauds.

(V) LIMITATIONS:

The study is limited to banking only, issues related to digital transactions prevention are only covered in this paper and does not exceed beyond that.

(VI) RESEARCH METHODOLOGY:

The study is descriptive in nature; data is collected from all secondary sources like Books, Newspaper, Magazines Printed media, Published and journals.

(VII) CONCEPT OF E - BANKING:

E – banking refers to doing the Banking transactions through online. E – banking is known by different names such as online banking, Internet Banking. In comparison to traditional banking services, E – Banking provides 24/7 a day and 7 days a week services to the customers . In order to access the services of E – Banking a client has to register with the Bank website with a username and need to create a password, with the help of a computer, mobile or other device customer can access his account and conduct many transactions. All Commercial banks are providing almost similar type of online services to their customers they are as follows.

E- banking provides the following services to the customers

- Downloading Bank statements
- Checking Account balances
- Viewing Previous transactions

ISSN:0971-1260

Vol-22- Issue-14-December-2019

- Payment of all bills such as (Internet bills, Water bills , Electricity bills, Telephone bills etc)
- Viewing images of paid Cheques
- Transfer of funds
- Applying for a loan or credit card
- Ordering a Cheque book
- Changing contact details

The first initiative in the area of bank computerization was stemmed out of two successive Committees on Computerization (Rangarajan Committee). The first committee was arranged in 1984 which made the plan of process of banking activities by using the computers. The second committee was made in 1989 taken the measures of using online banking transactions.

(VIII) CYBER CRIME IN BANKING SECTOR:

Cyber crime: Cyber crime is a fraudulent activity committed through online by using the computer as a tool or computer as a target. Cyber attacks are committed in different ways on the financial institutions few of them are as follows:

(1) **Hacking:** Hacking generally refers to breaking into the computer system and steals valuable information (data) from the system without any permission.

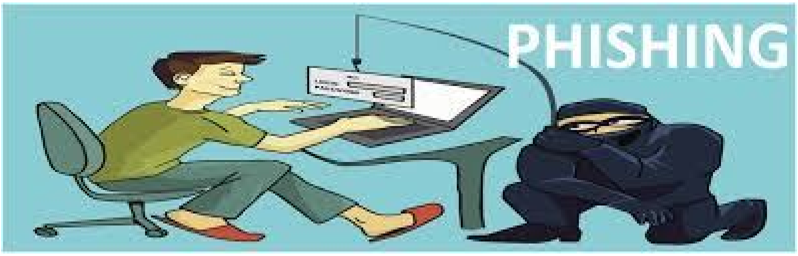
(2) **Credit Card Fraud:** Credit card fraud refers to the misusing the card use by the third parties, when a customer is using for online transactions hackers steal the card details such as password and use the card for their personal benefits.

(3) **Phishing or Identity Theft:** Phishing is the deceptive attempt to acquire the information of the banking customers relating to the username, password over the internet. This practice

ISSN:0971-1260

Vol-22- Issue-14-December-2019

will be done by disguising oneself as reliable entity in an electronic communication.



Spreading computer virus: Virus will damage the database and effect the smooth functioning of the computer software programmes. The hacker will develop some set of instructions through online for effecting the system virus attack.

(4) **E mail Spoofing:** It is a method of cheating the users where emails will be sent to the users with a fake id address in such a way that the user could not able to identify the original sender. This practice will leading tothe fraudulent activities over the internet.

(5) **ATM's Crimes:** It is a Process of committing the crime by installing a additional devices at the swiping point of the ATM machine. When the customer uses the card for transaction purpose it will record the card details and used for malpractices purpose.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

(IX) PRECAUTIONARY MEASURES TO CONTROL CYBER CRIMES IN BANKING SECTOR:

1.If the network is not properly secured- Then try to avoid online banking, shopping, entering credit card details, etc Check your online account frequently and make sure all listed transactions are valid.

2. Education to Customer- The customer should be educated and made aware about various bank frauds and precautionary measures should be informed to them to avoid the cyber crime victim.

3.Training of Bank Employees - Training and Orientation programs must be conducted for the employees by the banks for detecting the online fraud and solving the cyber threats quickly and easily.

4. Do not share the Card details to any unknown persons/ phone calls – Bank customers should not share the card details to any unknown persons while making the shopping and they should not share the pin number to any unknown phonecalls.

5. Checking the website is genuine or not – Fake websites are created by the hackers for cheating the online users, so before doing any online transactions check the website is secure or not.

(X) CONCLUSION:

This paper states the information relating to the cybercrime in financial institutions. Cyber crimes are gradually increasing year by year, whereas banks are not able to control such activities with the present policies, they should update their policies, technology in order to detect the frauds quickly and should hire employees with strong IT background with proper

ISSN:0971-1260

Vol-22- Issue-14-December-2019

training and knowledge to prevent the cyber crimes.

1. ***REFERENCES*:**
2. KrishanTuli and Dr. Neenu Juneja (2016) "Cyber Security challenges & online frauds on internet", International Journal of Advanced Research inISSN: 2278-6244 volume.5 no.2 Feb 2016.
3. Sultana SharmeenKarim (2016) "Cyber – Crime Scenario in Banking Sector of Bangladesh, The Cost and Management" ISSN 1817-5090, Volume-44, Number-2, March - April 2016.
4. Shubhamkumar,Dr.SantanuKoley, Udaykumar (2015) "Present scenario of cybercrime in india and its preventions", International Journal of Scientific & Engineering Research, Volume 6, Issue 4, April-2015 1971 ISSN 2229-5518 IJSER © 2015 http://www.ijser.org.
5. Simran, AkshayManvikar, Vaishnavi Joshi, Jatin Guru(2018) "Cyber - Crimes: A Growing Threat to Indian Banking Sector" ,International Journal of Engineering Technology Science and Research IJETSR ISSN 2394 – 3386 Volume 5, Issue 1January 2018.
6. Books:
   a. Intellectual Property Rights – Deborah, E. Bo Choux.
   b. Intellectual Property Rights – PrabuddhaGanguli.

AUTHOR PROFILE :

K. Jeevan Kumar M.B.A & M.COM presently working as Asst. Professor of MBA Department in Vidya Jyothi Institute of Technology , Hyderabad, Telangana, India.