CYBER CRIMES IN BANKING SECTOR LAWS AND REMEDIES

SUBMITTED TO PARTIAL FULLFILMENT OF

THE REQUIRMENT FOR THE DEGREE OF

(LL.M)

Batch: 2019-2020

SUBMETTID TO:

Miss. Trishla Singh

(Assistant Professor)

SUBMITTED BY:

Lakhte husain rizvi
Roll No: 1190990013

Corporate and Commercial Law

LL.M. IInd Sem.

BABU BANARASI DAS UNIVERSITY

LUCKNOW

CERTIFICATE

This is to certify that **LAKHTE HUSAIN RIZVI**, LL.M(Corporate and Commercial Law) student of Legal Studies, BABU BANARSI DAS UNIVERSITY, LUCKNOW has completed his dissertation, titled **“CYBER CRIMES IN BANKING SECTOR-LAWS AND REMEDIES”** under my supervision, for the award of degree of Master of Law . He has completed all the formalities as required under the ordinance and the dissertation is forwarded for evaluation.

(**Assistant prof. Ms. TRISHLA SINGH)**

SOLS , B.B.D.U

ACKNOWLEDGEMENT

This dissertation is the outcome of the study by the author. Any material used from different sources has been thoroughly acknowledged. After the successful completion of my work, I would like to thank number of people.

I would like to give my heartfelt gratitude to assistant professor Ms. TRISHLA SINGH, school of legal studies who understood the role of supervisor, mentor and guide for the successful preparation of this dissertation. This work is an outcome of an unparalleled infrastructural support that I have received from staff and employees of Institute of legal Studies. It Would never have been possible to complete this study without an untiring support from my father and family.

Finally, I must express my very profound gratitude to my father for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this dissertation. This accomplishment would not have been possible without him. This is study bears testimony to the active encouragement and guidance of a host of friends and well wishes.

LAKHTE HUSAIN RIZVI

LL.M Semester 2

Roll No:1190990013

DECLARATION

I hereby declare the Dissertation entitled " CYBER CRIMES IN BANKING SECTOR-LAWS AND REMEDIES" Submitted by me in the fulfillment of the requirements for the award of the degree of "Masters of Law" of BABU BANARSI DAS UNIVERSITY , is a record of my own work carried under the supervision and guidance of Assistant Professor, Ms. TRISHLA SINGH Institute of legal studies.

To the best of my knowledge this Dissertation has been submitted to BABU BANARSI DAS UNIVERSITY for the award of LL.M. Degree.

LAKHTE HUSAIN RIZVI

LL.M Semester 2

Roll No:1190990013

ABSTRCT

In the era of globalization Internet banking or online banking has revolutionized an integral activity of our modern twenty first century. The man developed various ways for communication to the exchange of information, ideas and knowledge which is of great importance to him as a social being. The evolution of e-banking technology makes the task very easy, banking transactions becomes very fast within a click. Online and mobile banking make daily banking fast and convenient. The misuse of information technology in the cyber space is clutching up which gave birth to cyber crimes at the national and international level. The percentage of risks and the challenges associated with it is increased. However online and mobile banking is never 100 per cent safe. The purpose of this research is to review current scenario of online banking and cyber attack. In this research we focused on cyber crimes related to online banking and new tricks and techniques used by hackers. This research also gives the details on Indian cybercrime Statistics. The latest cybercrime news related to online banking is also identified in this research. The study totally based on the secondary data. To review and analyze the current scenario of cybercrimes, we focused on the annual reports *of National Crime Record Bureau, Indian Computer Emergency Response Team, Internet Crime Complaint Center ,the Global Information Security Survey 2014-15, Press Information Bureau English Releases, Reserve Bank of India publications. The findings of this research shows that the IT usage and cybercrime related to online banking in India are on the rise. Majority of the cybercrimes have been committed by young people in the age group 18-30and are male gender. Our law enforcement agencies need to be adequately equipped to overcome and prevent the cyber crime. Finally researcher has given some suggestions for the prevention and safety use of online banking services.*

Table of content

LIST OF ABBREVIATIONS

AIR	All India Reporters
Anr	Another
NCR	National Crime Record
S	Section
IPC	Indian penal code
Cr.P.C	Criminal procedure Code
I.T Law	Information technology Law
NCRB	National Crime Record Bureau
CERT	Indian computer emergency - - Response Team
IC3	Internet crime complaint center

INTRODUCTION

The world is fast moving online with 46.1% of total world population now connected to the web according to internetlivestats.com . A remarkable instance of this phenomena has been experienced in India with a notable increase in the past three years 18% of the Indian population online in 2014, 27% in 2015 and 34.8% in 2016 .

Today, web technology has emerged as an integral andindispensable 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. While paper-based transactions cleared through cheques amounted to Rs 85 lakh crore in 2015, paperless transactions, including retail electronic transactions such as ECS (electronic clearing system) debits and credits, electronic fund transfer, card transactions, mobile transactions and prepaid instruments were to the tune of Rs 92 lakh crore in the same. India has seen an upsurge in the volume of debit/credit cards due to increased online acceptance through alternative channels, including internet, ATM and mobile banking. In the days to come, this volume will gain traction as the youth generationwill enter the economic gyration. The last few years have seen a significant increase in cybercrime across all sectors and geographies. Given the proliferation of these technological crime, organizations face a significant challenge to be resistant against cyber attacks. As per Motive-wise Cases Reported under Cyber Crimes during 2015 statistics by National Crime Records Bureau, Greed / Financial Gain is the prime motivation for committing Cyber Crimes.

Online transactions have grow fast since demonetization took place in India. The Indian government revision a vision of digital India to grow the Indians to online transactions and online banking . But in India, yet people are not understood about this new technology. Due to which crimes in online banking is increasing. A services says, Scam of 251 crores has occurred in online banking from 2014 to 2015. In which credit card scam of 130 crores around of 90 crores from ATMs card and also they are having many cases like **Jamtara's credit card scam and Cosmos Bank's online robbery** etc.

As an increasing number of users are demanding online services, the background mission of providing balanced security and convenience is seeming to be a tough challenge due to numerous obtrusive actors collectively referred to as “Cyber-Crime”. Simply stated, “Cyber-Crime” is crime that involves a computer and a network. Cyber-Crime is being considered a serious threat to all the aspects of a nations economic growth as maximum instances of the same are being observed in financial institutions. Cyber-Crime incidents include but are not limited to credit card fraud, spamming, spoofing, e-money laundering, ATM fraud, phishing, vishing, identity theft and denial of service.

OBJECTIVES OF THE RESEARCH

1. To understand how cybercrime operations work and why they make money

2.To study cyber crimes and it simplications on the Banking Sector

3.To understand fraud\fraud detection in the sector under study

4.To identify the complaints received, solved and pending

5.To analyze and use the preventive measures available to control frauds

Historical background of the research

Until mid-1990s, banking sector in most parts of the world was simple and reliable; however since the advent of technology, the banking sector saw a paradigm shift in the phenomenon (Jaleshgari, 1999). Banks in order to enhance their customer base introduced many platforms through which transactions could be done without much effort . These technologies enabled the customer to access their bank finances 24*7 and year around through, ATMs and Online banking procedures.

However, with the enhancement in technology, banking frauds have also increased likewise . Cybercriminals are using different means to steal ones bank information and ultimately their money as well. The results of a study revealed that globally, the banks have incurred billions of dollars in losses; and provides details of cybercrimes conducted across the globe in banking sector due to direct and indirect losses, criminal revenue and indirect costs. It is therefore, a collective consensus of banks and regulators to make policies and adopt measures in order to protect banking platforms from cyber threats. A number of technical defence and control measures like increased real time supervision on transactions have been undertaken by the banks, however, even today the problem persists . The reason behind this is that the defence measures currently available with banks are often reactive, time consuming and available in public domain which can be accessed even by the cybercriminal who in turn adopts measures to combat from these defences. The attackers allocate their time in developing new means for cybercrime and also simultaneously work on finding the solutions to bridge these defence measures. One of the ways to mitigate the problem of cybercrimes in banking sector is to identify the factors related to banks that are generally targets of such cyber-attacks, and why some banks have never faced such a situation. According to the empirical study conducted by Moore and Clayton (2007), some banks are targeted more frequently than others, generally by a financial malware. Banks which are generally targets of cybercrimes suffer from various malware attacks in form of online phishing, keystroke-loggings malwares, identity theft, etc. Some of key factors which were identified in the study which reflects the pattern why some banks are targeted more than other include their size (market share), the number of clients, their authentication system is weak, their money transfer policies are not safe and the country in which these banks are located is also an important pre-requisite for the cyber criminals. Studies conducted recently concluded that some of the malware used to attack these banks are becoming more specific. However, more such researches will have to be conducted to conclude if indeed cyber criminals are selecting their target specific tools or not.

Hypothesis

In spite of the I.T act 2000 in India, If money is withdrawing from his account by the Cyber fraud with individual, That the person does not receive any remedies against the fraud because in cyber crime the convict to used this kinds of tools to prevent the police from tracking him. So it is rather difficult task to control cyber crime in the digital India.

Problem Statement

Cybercrime is a growing threat in the virtual world because individuals and organizations are relying more on internet at an increasing rate. The use of internet and other technologies have enhanced the risk of attack from cyber criminals across the globe. With the number of incidents of theft, phishing, computer viruses, hacking, on the rise, there is a need to explore the cybercrime scenario. Although, with the advent of technologies, the banking sector has been able to reach more customers however, it has also enhanced the risk for customers who often feel reluctant and insecure in opting for such services. There is a need for the banks to evaluate their current operating practices. In this paper, the researcher makes and attempt to study the cybercrime scenario and its impact on banking sector.

RESEARCH METHODOLOGY

This study is based on secondary data. To fulfill the first objective of the study the category of Cyber crime in banking sector- laws and remedies analyzed by Information Technology Act 2000 as well as the web site of cyber crime investigation cells . To review the tricks and techniques used by cyber criminals to hack the banking systems and make the cyber frauds various case studies in various news channels are referred. To review the status of cyber crimes in India and the data is gathered from annual reports of National Crime Record Bureau (NCRB).

Chapter=1

Cyber crime in banking sector

Cyber crime, computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties. In the banking sector, the cybercrimes which are committed using online technologies to illegally remove or transfer money to different account are tagged as banking frauds The cybercrimes according to Wall can be categorized into four major categories i.e. cyber-deceptions, cyber-pornography, cyber-violence and cyber-trespass. The banking frauds are sub-categorized in cyber-deception which can be defines as an immoral activities including stealing, credit card fraud, and intellectual property violations. There are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the frauds are executed with the ultimate goal of gaining access to users bank account, steal funds and transfer it to some other bank account. In some cases the cyber criminals uses the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts As a lot of vulnerabilities exist in the defense system of banking sector, thus there is a need to investigate the ways to increase awareness about the measures that can be undertaken to combat cybercrimes in the banking sector. However, not many studies in the past have been conducted in this area which would suggest ways to mitigate the risks and combat such crimes . In order to understand the fraud system in banking sector we will have to understand and describe the attackers and defenders in this environment. The next section therefore describes the different actors which are involved in cybercrimes.

Cyber space and cyber world

A cyber world and cyber space broadly refers to a world full of light, filament and signals , data or its microcosm or similar elements. This is a virtual space, where a lot of activities you cannot see and many things you can see but cannot touch. This virtual world has directly transformed the real world.

What is cyber Crime?

It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

In the case Debarati Holder and K. Shankar Court held that-

Offenses that are committed against individuals or groups or individuals with a criminal motive to intentionally harm the reputation of the victim or causes physical or mental harm or loss to the victim directly or indirectly, using modern telecommunication networks such as Internet , mobile phone and computer etc.

Nature of the crime-

These crimes are relatively new, having been in existence for only as long as the computer have, which explains how unprepared society and the world in general is toward combatting these crimes.

There are numerous crimes of this nature competitive daily on the Internet.

Cyber law versus information technology law.

Cyber law refers to law that is literally a set of Several Law viz computer law, Internet law, and information technology law. Internet law and information technology law is often used as a synonym. Computer law is a dissimilar law, through there is no denying the presence of common element of this and in the northeast laws. That is why, when we study computer technology law or only computer law, We study the method related to layout design patent etc . So for as it has application in the computer and its normal working system. On the other hand, when we are talk about information technology law, our aim is to consider the computation Technology and the legal aspect that application creates on such devices. It is concerned with identification of data, accredition, conservation, transmission and communication and such other matters.

Thus, it can be said that cyber law is aggregate collective noun where as the other laws are individuals, but at time ever without such distinctions, the work goes on For example, when we speak of cyber abuse or cyber crimes, It covers all those offenses which are committed with respect to a computer or computer system or computer network or Internet.

- **<u>Some cyber words</u>**

We shall consider certain words to advance our discussion , which is a part of the cyber world, is just a banner of words used in information technology. To keep this somewhat brief, we shall focus only on the meaning of the terms, which are given to them by the information Technology Act 2000 of India. According to the IT act of India, Some of these words have meaning as under:-

1. **Communication Device**

Communication device refers to the cell phone or private digital assistance, or the mechanism of both or any device used to compress or transmit visual or audio, test or images.

2. Computer

Computer refers to any electronic, magnetic or optical or other high speed data processing device or process. Which are conducts logical, arithmetic or memory functions by conductions of electronically, magnetic or optical impulses. It includes all cost , product, processing, collections, computers software or communication facilities related to a computer system or computer network.

3. Secure system

secure system refer to the software or hardware and procedure of a computer that invites for unauthorized entrances and abuse. Provide reasonable levels of integrity and flawless operations, Suitable for making intended application, and adhering to generally accepted security procedures.

4. Cyber security.

Cyber security refers to protecting any information furnishment , equipment, computer. Computer resource, Communication equipment and the information stored therein against unauthorized entercity , use, barrier modification or destructions

5. Data

Meaning of data is a mapping of information, knowledge, facts, resolution, instructions, processed, or whether something is going on a typical manner and purports to be rendered or . processed in a computer system or computer network; and that can be in any form including the printed print, magnetic or optical transmission medium of a computer punched card or. Punched tape, or stored internally in computer memory.

- **E-banking in India**

In India, since 1997, when the ICICI Bank first offered internet banking services, today, most new-generation banks offer the same to their customers. In fact, all major banks provide e-banking services to their customers**.**

Electronic banking is a form of banking in which funds are transferred through an exchange of electronic signals rather than through an exchange of cash, checks, or other types of paper documents. Transfers of funds occur between financial institutions such as banks and credit unions. They also occur between financial institutions and commercial institutions such as stores. Whenever someone withdraws cash from an automated teller machine (ATM) or pays for groceries using a debit card, the funds are transferred via electronic banking.

Electronic banking relies on intricate computer systems that communicate using telephone lines. These computer systems record transfers and ownership of funds, and they control the methods customers and commercial institutions use to access funds. A common method of access (or identification) is by access code, such as a personal identification number (PIN) that one might use to withdraw cash from an ATM machine.

There are various electronic banking systems, and they range in size. An example of a small system is an ATM network, a set of interconnected automated teller machines that are linked to a centralized financial institution and its computer system.

Electronic banking laid the groundwork for speed and convenience in individual and commercial (business) banking. The spread of personal computer use has added another layer of convenience and speed to the process. Electronic banking allows customers of most banks to do their banking at any hour of the day, regardless of the bank’s operating hours. If customers choose to do such things as transfer funds or pay bills, they can usually do so from anywhere Internet access is available.

Online banking typically offers bank statements, electronic bill payment, funds transfers between a customer’s checking and savings accounts (or to another customer’s account), loan applications and transactions, and purchasing or sales of investments, all of which allow customers to maintain their accounts without making a trip to the bank itself.

- **<u>Types of e banking</u>**

Banks offer various types of services through electronic banking platforms. These are of three types:-

Level 1 – This is the basic level of service that banks offer through their websites. Through this service, the bank offers information about its products and services to customers. Further, some banks may receive and reply to queries through e-mail too.

Level 2 – In this level, banks allow their customers to submit instructions or applications for different services, check their account balance, etc. However, banks do not permit their customers to do any fund-based transactions on their accounts.

Level 3 – In the third level, banks allow their customers to operate their accounts for funds transfer, bill payments, and purchase and redeem securities, etc.

Most traditional banks offer e-banking services as an additional method of providing service. Further, many new banks deliver banking services primarily through the internet or other electronic delivery channels. Also, some banks are ‘internet only’ banks without any physical branch anywhere in the country.

Therefore, banking websites are of **two types:-**

1. **Informational Websites** – These websites offer general information about the bank and its products and services to customers.
2. **Transactional Websites** – These websites allow customers to conduct transactions on the bank's website. Further, these transactions can range from a simple retail account balance inquiry to a large business-to-business funds transfer. The following table lists some common retail and wholesale e-banking services offered by banks and financial institutions.

Importance of e-banking

We will look at the importance of electronic banking for banks, individual customers, and businesses separately.

Banks

1. **Lesser transaction costs** – electronic transactions are the cheapest modes of transaction
2. **A reduced margin for human error** – since the information is relayed electronically, there is no room for human error
3. **Lesser paperwork** – digital records reduce paperwork and make the process easier to handle. Also, it is environment-friendly.
4. **Reduced fixed costs** – A lesser need for branches which translates into a lower fixed cost.
5. **More loyal customers** – since e-banking services are customer-friendly, banks experience higher loyalty from its customers.

Customers

1. **Convenience** – a customer can access his account and transact from anywhere 24x7x365.
2. **Lower cost per transaction** – since the customer does not have to visit the branch for every transaction, it saves him both time and money.

3. **No geographical barriers** – In traditional banking systems, geographical distances could hamper certain banking transactions. However, with e-banking, geographical barriers are reduced.

Businesses

- **Account reviews** – Business owners and designated staff members can access the accounts quickly using an online banking interface. This allows them to review the account activity and also ensure the smooth functioning of the account.
- **Better productivity** – Electronic banking improves productivity. It allows the automation of regular monthly payments and a host of other features to enhance the productivity of the business.
- **Lower costs** – Usually, costs in banking relationships are based on the resources utilized. If a certain business requires more assistance with wire transfers, deposits, etc., then the bank

charges it higher fees. With online banking, these expenses are minimized.

- **Lesser errors** – Electronic banking helps reduce errors in regular banking transactions. Bad handwriting, mistaken information, etc. can cause errors which can prove costly. Also, easy review of the account activity enhances the accuracy of financial transactions.
- **Reduced fraud** – Electronic banking provides a digital footprint for all employees who have the right to modify banking activities. Therefore, the business has better visibility into its transactions making it difficult for any fraudsters to play mischief.

Popular services under e-banking in India

- ATMs (Automated Teller Machines)
- Telephone Banking
- Electronic Clearing Cards
- Smart Cards

- EFT (Electronic Funds Transfer) System
- ECS (Electronic Clearing Services)
- Mobile Banking
- Internet Banking
- Telebanking
- Door-step Banking

Further, under Internet banking, the following services are available in India:-

- **Bill payment –** Every bank has a tie-up with different utility companies, service providers, insurance companies, etc. across the country. The banks use these tie-ups to offer online payment of bills (electricity, telephone, mobile phone, etc.). Also, most banks charge a nominal one-time registration fee for this service. Further, the customer can create a standing instruction to pay recurring bills automatically every month.
- **Funds transfer** – A customer can transfer funds from his account to another with the

same bank or even a different bank, anywhere in India. He needs to log in to his account, specify the payee’s name, account number, his bank, and branch along with the transfer amount. The transfer is effected within a day or so.

- **Investing** – Through electronic banking, a customer can open a fixed deposit with the bank online through funds transfer. Further, if a customer has a demat account and a linked bank account and trading account, he can buy or sell shares online too. Additionally, some banks allow customers to purchase and redeem mutual fund units from their online platforms as well.
- **Shopping** – With an e-banking service, a customer can purchase goods or services online and also pay for them using his account. Shopping at his fingertips.

E-commerce payment system

An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. Also known as a subcomponent of Electronic Data Interchange, e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

OTP

A one-time password (OTP), also known as one-time pin or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device.

ATM MACHINE

Automated Teller Machine—a machine in which you insert a special kind of plastic card to take out money from your bank account

ATM CARD

An ATM card is a payment card or dedicated payment card issued by a financial institution which enables a customer to access automated teller machines (ATMs). Most payment cards, such as debit and credit cards can also function as ATM cards, although ATM-only cards are also available.

ATM PIN

An ATM PIN or Personal Identification Number is a 4 digit code that is unique to every account holder's ATM cum debit card and is provided to ensure that all the cash withdrawals, POS transactions and online transactions are secured

Debit card

A debit card is a plastic payment card that can be used instead of cash when making purchases. It is similar to a credit card, but unlike a credit card, the money is immediately transferred directly from the cardholder's bank account when performing any transaction.

Credit card

A credit card is a payment card issued to users (cardholders) to enable the cardholder to pay a merchant for goods and services based on the cardholder's promise to the card issuer to pay them for the amounts plus the other agreed charges. The card issuer (usually a bank) creates a revolving account and grants a line of credit to the cardholder, from which the cardholder can borrow money for payment to a merchant or as a cash advance.

(Chapter = 2)

Tools of cyber crimes and preventive Measure to control Cyber crimes in Banking Sector

Offences that are committed against individuals or groups of individual with a criminal motive to intentionally harms the reputation of the victim or causes physical or mental harm or loss , to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones.

Crimes that primarily target computer network or device including

- *computer virus*
- *Denial-of-service attacks*
- *Malware (malicious code)*

1.Various Cyber attacks

Viruses and worms

Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.

Spam emails

Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver — potentially creating a wide range of problems if they are not filtered appropriately.

Trojan

A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk.

Denial-of-service (DoS)

DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.

Malware

Malware is a software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a botnet a network of computers controlled remotely by hackers, known as herders to spread spam or viruses.

Scareware

Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses

Phishing

Phishing attacks are designed to steal a person's login and password. For instance, the phisher can access the victims bank accounts or assume control of their social network.

Fiscal fraud

By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits

State cyber attacks

Experts believe that some government agencies may also be using cyber attacks as a new means of warfare. One such attack occurred in 2010, when a computer virus called Stuxnet was used to carry out an iniible attack on Iran’s secret nuclear program. The virus was aimed at disabling Iran’s uranium enrichment centrifuges.

Carders

Stealing bank or credit card details is another major cyber crime. Duplicate cards are then used to withdraw case at ATMs or in shops

Hacking

It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.

Cracking

It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

1.(a)Phishing .

What do you do when you come across emails that seem suspicious? Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (voice phishing) and SMS (Smishing).

How do fraudsters operate?

Fraudsters pose as Bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

Clicking on the link diverts the customer to a fake website that looks like the official Bank website – with a web form to fill in his/her personal information.

Information so acquired is then used to conduct fraudulent transactions on the customer’s account.

How to identify fake Phishing website:

Verify the URL of the webpage. The ‘s’ at the end of ‘https://’ stands for ‘secure’ - meaning the page is secured with an encryption. Most fake web addresses start with ‘http://’. Beware of such websites!

Check the Padlock symbol. This depicts the existence of a security certificate, also called the digital certificate for that website.

Establish the authenticity of the website by verifying its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of your browser window.

How to protect yourself from Phishing:

Always check the web address carefully.

For logging in, always type the website address in your web browser address bar.

Always check for the Padlock icon at the upper or bottom right corner of the webpage to be ‘On’.

Install the latest anti-virus/anti spyware/firewall/security patches on your computer or mobile phones.

Always use non-admin user ID for routine work on your computer.

DO NOT click on any suspicious link in your email.

DO NOT provide any confidential information via email, even if the request seems to be from authorities like Income Tax Department, Visa or MasterCard etc.

DO NOT open unexpected email attachments or instant message download links.

DO NOT access Net Banking or make payments using your Credit/Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones. The number of phishing attacks against banking systems is constantly growing. Practically every sector of society is targeted by cyber criminals with various techniques. Phishing attacks make large use of social engineering techniques to fool the user and steal sensitive information and banking account credentials.

In a typical phishing scheme, spoofed emails lead users to visit infected websites designed to appear as legitimate ones. The websites are designed to coax customers to divulge financial data, such as account credentials, social security numbers and credit card numbers.

In the classic attack scheme, fraudsters send e-mails or advertisements to the victims with content that looks like they were sent by a bank or by a credit card company. The emails request victims to click on a link to go to a website that replicates a bank's website

The malicious email could contain a link to the fake website or could include an attachment that once opened, involves exactly the same task. Phishing attacks use social engineering techniques mixed with technical tricks to fool the user and steal sensitive information and banking account credentials. Phishing messages usually take the form of fake notifications from banks, providers, e-payment systems and other organizations. They request the user to submit sensitive information such as passwords, credit card numbers and bank account details

In literature, there are several variants of phishing, many of them involve the use of malware specifically designed to steal credentials from victims while hiding evidence of an attack.

Case Under the Study: (Official Website of Maharastra G hackedmember 2007 — IT specialists were attempting yesterday to reestablish the official site of the administration of Maharashtra, which was hacked in the early long periods of Tuesday. Rakesh Maria, joint chief of police, said that the state's IT authorities stopped a formal objection with the Digital Wrongdoing Branch police on Tuesday. He included that the programmers would be found. Recently the site, http://www.maharashtragovernment.in, stayed blocked. Vice president Pastor and Home Priest R.R. Patil affirmed that the Maharashtra government site had been hacked. He included that the state government would look for its assistance and the Digital Wrongdoing Branch to examine the hacking. "We have taken a genuine perspective of this hacking, and if require be the legislature would even go further and look for the assistance of private IT specialists. Dialogs are in advancement between the authorities of the IT Office and specialists," Patil included. The state government site contains nitty gritty data about government offices, handouts, reports, and a few different subjects. IT specialists taking a shot at reestablishing the site disclosed to Middle Easterner News that they expect that the programmers may have decimated the majority of the site's substance. As indicated by sources, the programmers might be from Washington. IT specialists said that the programmers had recognized themselves as "Programmers Cool Al-Jazeera" and asserted they were situated in Saudi Arabia. They included this may be a red herring to divert specialists from their trail. As per a senior authority from the express government's IT division, the official site has been influenced by infections on a few events before, however was never hacked. The authority included that the site had no firewall. Three individuals held liable in on line Visa trick Clients Visa subtleties were abused through online methods for booking air-tickets. These guilty parties were gotten by the city Digital Wrongdoing Examination Cell in Pune. It is discovered that subtleties abused were having a place with 100 individuals. Mr. Parvesh Chauhan, ICICI Prudential Extra security officer had griped for the benefit of one of his client. In such manner Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and

Ahmead Sikandar Shaikh were captured. Lukkad being utilized at a private foundation, Kale was his companion. Shaiklh was utilized in one of the parts of State Bank of India. As indicated by the data given by the police, one of the clients got a SMS based alarm for buying of the ticket notwithstanding when the Master card was being held by him. Customer was caution and came to realize something was fishy; he enquired and came to know about them isuse. He reached the Bank in such manner. Police watched association of numerous. Banks in this reference - The tickets were book through online methods. Police asked for the log subtleties and got the data of the Private Establishment. Examination uncovered that the subtleties were gotten from State Bank of India. Shaikh was working in the Visa division; because of this he approached charge card subtleties of a few clients. He gave that data to Kale. Kale consequently passed this data to his companion Lukkad. Utilizing the data acquired from Kale Lukkad booked tickets. He used to pitch these tickets to clients and get cash for the equivalent. He had given couple of tickets to different establishments. Digital Cell head DCP Sunil Pulhari and PI Mohan Mohadikar A.P.I Kate were associated with eight days of examination lastly got the offenders. In this respects different Banks have been reached; additionally, four carrier businesses were reached. DCP Sunil Pulhari has asked for clients who have fallen in to this snare to advise police experts on 2612-4452 or 2612-3346 on the off chance that they have any issues. UTI Bank snared in a phishing attack(14 February 2007) Fraudsters of the internet have raised its revolting head, the first of its sort in the year 2007, by propelling a phishing assault on the site of Ahmedabad-based UTI Bank, a main private bank advanced by India's biggest budgetary organization, Unit Trust of India (UTI).A URL on Geo Cities that is just about a copy form of the UTI Bank; s landing page is accounted for to flow among email clients. The website page not just requests the record holder's data, for example, client and exchange login and passwords, it has additionally beguilingly set up disclaimer and security peril articulations. On the off chance you have gotten any email from a deliver having all the earmarks of being sent by UTIBANK, educating you concerning any progressions made in your own data, account subtleties or information on your client id and secret phrase of your net managing an account office, kindly don't react. It is UTI Bank policy not to look for or send such data through email. In the event that you have effectively uncovered your secret word please transform it quickly, the notice says. The dubious connection is accessible on http://br.geocities/If any clueless record holder enters his login id, secret phrase, exchange id and secret phrase so as to change his subtleties as exhorted by the bank, a similar information is sent vide mailform.cz (the phishes database). After examination, we found that Mail shape is an administration of PC Svet, which is a piece of the Czech organization PES Counseling. The Website admin of the webpage is an individual named PetrStastny whose email can be found on the site page. Top authorities at UTI Bank said that they have revealed the case to the Monetary Office Wing, Delhi Police. The bank has additionally drawn in the administrations of Melbourne-based Extortion Watch Worldwide, a main antiphishing organization that offers phishing checking and bring down arrangements. We are currently during the time spent shutting the site. A portion of these activities require significant investment, however clients have been kept on the up and up about these activities, said V K Ramani , President - IT, UTI Bank according to the discoveries of UTI Bank's security office, the phishers have sent in excess of 1,00,000 messages to account holders of UTI Bank and also different banks. Despite the fact that the organization has commenced harm control activities, none of the activities are penny percent idiot proof. Presently there is no chance to get for banks to know whether the individual signing in with exact client data is a cheat, said Ramani. In any case, dependable sources inside the bank and security offices affirmed that the misfortunes because of this specific assault were nada. The bank has sent alarms to every one of its clients illuminating about such malignant sites, other than expanding their caution and extortion reaction framework; Drawing in expert organizations like Misrepresentation Watch help in decreasing time to react to assaults; said Sanjay Haswar, Right hand VP, System and Security, UTI Bank.

1.(b) Pharming and Credit Card Redirection

Pharming occurs when attackers are able to hijack a bank's URL so that when users try to access their bank's website, they get redirected to a fake site that looks like the real thing.

The term "pharming" is a neologism based on the words "farming" and "phishing." Despite that it's difficult to carry out, it’s technically possible with following techniques:

DNS Cache Poisoning- DNS servers are deployed in an organization’s network to improve resolution response performance by caching previously obtained query results. Poisoning attacks against a DNS server are made by exploiting a vulnerability in DNS software. That causes the server to incorrectly validate DNS responses that ensure that they’re from an authoritative source. The server will end up caching incorrect entries locally, and serve them to other users that make the same request. Victims of a banking website could be redirected to a server managed by criminals who could use it to serve malware, or to induce bank customers to provide their credentials to a copy of a legitimate website. If an attacker spoofs an IP address; DNS entries for a bank website on a given DNS server, replacing them with the IP address of a server they control, makes an attacker able to hijack customers.

Hosts File Modification- The HOSTS file maps domain names to IP addresses, entries in the file override DNS entries maintained by the ISP. Malware authors are increasingly using the HOSTS file to redirect users on website they manage.

Credit card redirection is new technique we're seeing being used on compromised e-commerce websites to steal credit and debit card information, by compromising legitimate web services .

Security experts note that websites implementing e-commerce services are under attack, the most hit open source e-commerce system is Magento. In one case observed, the file used for payment handling was altered to replace every occurrence of paymentexpress.com for paymentiexpress.com, that's a domain managed by cyber criminals.

Credit cards are valuable in the underground market. An attacker modifies the flow of the payment process, so that instead of just processing the card, they redirect all payment details to a domain they manage, so they can steal card details.

The user that accesses the compromised e-commerce site is stealthily redirected to a well designed phishing site, so that the website could acquire card information, and send it back to the attackers.

Redirection is possible also by modifying the credit card processing file, giving the criminals access to all transaction data, including credit card details (name, address, CC and CVV.)

"The attackers modify the flow of the payment process so that instead of just processing the card, they redirect all payment details to a domain they own so they can steal the card details .

Case Study: India's First Atm Card Fraud The Chennai city police have busted a universal posse associated with digital wrongdoing, with the capture of Deepak prem manwani (22), who was caught in the act while breaking into an ATM in the city in June last, it is dependably learnt. The elements of the city cops' accomplishment can be ganged from the way that they have gotten a man who is on the needed rundown of the considerable FBI of the US. At the season of his detainment, he has with him Rs 7.5 lakh knocked off from two ATMs in T Nagar and Abirami puram in the city. Preceding that, he has left with Rs 50,000 from an ATM in Mumbai.   While researching Manwani's case, the police discover a digital wrongdoing including scores of people over the globe.   Manwani is a MBA drop-out from a pune school and filled in as a promoting official in a Chennai-based firm for quite a while.   Strikingly, his daring wrongdoing profession began in a web bistro. While perusing the net one day, he got pulled in to a sire which offered him help with breaking into the ATMs. His contacts, sitting some place in Europe, were prepared to give him charge card number of a couple of American banks for $5 per code. This site likewise offered the attractive codes of those cards, however charged $200 per code. The administrator of the site has concocted an interesting plan to get the individual ID number (Stick) of the card clients. They skimmed another site which looked like that of a presumed telecom organizations.   That organization has a huge number of supporters. The phony site offered the guests to return $11.75 per head which, the site advertisers stated, has been gathered in overabundance unintentionally from them. Trusting that it was an authentic offer the telecom organization being referred to, a few lakh supporters signed on to the site to get back that minimal expenditure, yet in the process separated with their PINs. Outfitted with every single essential datum to hack the bank ATMs, the posse began its orderly plundering. Evidently, manwani and numerous others of his kind went into an arrangement with the pack behind the site and could buy any measure of information, obviously on specific terms, or basically go into an arrangement on a goods sharing premise. In the interim, manwani additionally figured out how to create 30 plastic cards that contained important information to empower him to break into ATMs. He was enterprising to the point that he had the capacity to offer away a couple of such cards to his contacts in Mumbai. The police are vigilant for those people as well. On receipt of huge scale protestations from the charged Visa clients and bank in the US, the FEI began an examination concerning the undertaking and furthermore alarmed the CBI in New Delhi that the universal pack has built up a few connections in India as well. Manwani has since been developed safeguard after cross examination by the CBI. In any case, the city police trust this is the start of the finish of a noteworthy digital wrongdoing.

1.(c) Mobile

Security researchers are observing the increasing interest of cybercriminals in new platforms, including cloud, mobile and social networking. The reason is the capability of these infrastructures to reach a wide audience, and the lack of awareness in cyber threats.

Mobile platforms, due to their high penetration level, are the technology most used to provide banking services. For that reason, it’s a popular target for cyber crime.

When we speak about mobile, we cannot ignore that Android is the OS that has the greatest market share. The downside is that Android malware has monopolized the mobile scenario, as showed in a picture extracted by the last F-Secure Threat Report.

It’s evident that the cyber criminal black market is specializing its offer in malware that targets Android, exactly as for any desktop PC. In the underground market, it’s possible to acquire various exploit kits specifically designed for mobile devices that allow for criminals to recruit machines for botnet architecture, or to organize prolific scam, typically premium SMS and click fraud.

How they work

The mobile phone worked as cyber a cyber café for them. A few years ago gangs such as his used to operate from one of the dozens of cyber cafes in and around Jamtara. The cops have made that difficult with cyber cafe owners being co-opted into police informer networks. Every morning they gather in the barren fields close to the dry jungles bordering the village. One of them brings updates from an underground network of phone number database sellers, new phone connection resellers and general buzz about who could be on the radar of Jamtara's cyber police. The localized of there, they don't allow to take the pictures. They normally chase away people with cameras trying to enter the village. They even pelt stones on police teams who come into our villages sniffing around," the friend says boastfully, picking up a small stone as he talks. After shortlist the phone numbers of people from different parts of India to call posing as bank managers, the action begins. The most common tactic is impersonation. They make calls posing as bank managers, getting their victims to share bank account and card details, and then use the information to move the money to their accounts. Typically, targets are told that their ATM card has been blocked and that if it’s not renewed soon, it will remain inactive. India has over 1.6 billion savings and current banking accounts and some 29 million credit cards and 820 million debit cards approx. - and the chances of someone believing the call to be a genuine one are high. They provide so many offers, such as heavy loan with low interest, credit card with higher limit, or they scared the victims that your account or ATM would be closed. Then they asked for the 16-digit card number and its details. While on the call, self or one of them feed that information in an e-wallet, including the CVV number, and expiry date of the card. Then, they ask the victim to share an OTP message they would be receiving from the bank, which is essential for the criminals to transfer money from the victim’s account to an e-wallet such as Paytm or Oxigen. This e-wallet is already linked with a bank account opened only for this purpose. Mostly a fake bank account opened with fraud KYC documents.

Very Soon, the money is withdrawn and distributed among everyone involved in the crime. Not all involved in the crime have e-wallets; the ones that do become the centrepiece of this entire chain. They told sometimes it's difficult to transact through e-wallets, especially the more established ones such as Paytm because accounts require KYC documentation. But Jharkhand's digital-savvy criminals won't give up so easy. They have discovered a bunch of e-wallets including Tapzo, TMW, Kitecase and so on. They always try to find new e-wallet, for this they take account on lease from the respective users & for that they pay some amount to that user. Police team have been tightening the noose around the networks of SIM card sellers, e-wallet companies and bank accounts involved in this chain and have aggressively moved on the local cybercrime networks. "We act on the leads and information mostly suomoto. Based on local inputs, we conduct regular raids. This year we have done so far 60 arrests.

Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement.

How do fraudsters operate?

Step – 1

Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.

Step – 2

The fraudsters then transfer the illegal money into the money mule’s account.

Step – 3

The money mule is then directed to transfer the money to another money mule’s account – starting a chain that ultimately results in the money getting transferred to the fraudster’s account.

Step – 4

When such frauds are reported, the money mule becomes the target of police investigations.

1.(d) Watering Hole

“Watering hole” attacks are considered an evolution of spear phishing attacks. They consist of injecting malicious code onto the public web pages of a website that that a small group of people usually visit.

In a “watering hole” attack scenario, the attackers wait for victims to visit the compromised site instead of inviting them with phishing messages. The efficiency of the method could be increased with exploitation of zero-day vulnerabilities in many large-use software programs such as Internet Explorer or Adobe Flash Player.

Cyber criminals could easily compromise an improperly configured or updated website using one of the numerous exploit kits available on the black market.

Usually attackers hack the target site months before they actually use it for an attack.

The methods are very efficient. It’s very difficult to locate a compromised website. “Watering hole” is a considerably surgical attack that allows hackers to hit only specific community, comparatively, classic phishing is less noisy.

“Targeting a specific website is much more difficult than merely locating websites that contain a vulnerability. The attacker has to research and probe for a weakness on the chosen website. Indeed, in watering hole attacks, the attackers may compromise. Once compromised, the attackers periodically connect to the website to ensure that they still have access…”

watering hole” attack against the banking sector was observed in March 2013 when several South Korean banks were hit by a widespread attack that wiped data and shut down systems. Internet banking servers went down causing an interruption of their services, including online banking.

1.(e) Man In The Browser

Financial service professionals consider “Man In The Browser” to be the greatest threat to online banking and cybercrime increases, due to its efficiency. In the classic MITB schema, attackers integrate social engineering methods with the use of malware that infects the browser of the victim’s client machine. It appears in the form of a BHO (Browser Helper Object), Active-X control, browser extension, add-on, plugin, or API–hooking. “Man In The Browser” attacks are based on the presence of proxy malware that infects the user’s browser, exploiting its vulnerabilities on the victim’s machine. The malicious code resides in the browser and it’s able to modify the content of a banking transaction or to conduct operations for victims in a completely covert fashion. The agent also hides transactions from victims, altering the content presented to the browser with injection techniques. It’s important to state that neither the bank nor the user can detect the attack. That’s despite when a bank has implemented a multifactor authentication process, CAPTCHA, or any other forms of challenge response authentication.

1.(f) Malware based-attacks

Malware based attacks are among the most dangerous cyber threats related to online banking services. The number of families of malicious code specifically designed for financial attacks are constantly increasing. Some of the most popular banking malware are Zeus, Carberp, Spyeye, Tinba and the recent KINS. But surely, the first three agents are considered to be the most by the security community. Zeus is the oldest of them. Numerous variants were detected during the last five years, and they have been often used to commit cyber fraud on a large scale. The first version of the Zeus trojan was detected in July 2007, when it was used to steal information from the United States Department of Transportation.

Almost every banking Trojan presents a group of shared capabilities, including backdoor and credential stealing features, and form grabbing. The majority of malware use has methods of attacking the "Man In The Browser."

Cosmos bank cyber attack

Cosmos Bank became the victim of a major cyber-attack. Hackers breached the bank's ATM switch server in Pune, stealing details of multiple Visa and Rupay debit card owners. The details were then used to carry out around 12,000 fraudulent transactions across 28 countries on August 11 – with a further 2,841 transactions taking place in India.

The attack didn't stop here. Two days later, on August 13th, in another malware attack on the bank's server, a SWIFT transaction was initiated – transferring funds to the account of ALM Trading Limited in Hanseng Bank, Hong Kong.

The total losses from the attack stand at INR 94 crore, or 13.5 million USD. Cosmos Bank was forced to close its ATM operations and suspend online and mobile banking facilities.

How did the attack happen?

Malware attack: The core banking system (CBS) of the bank receives debit card payment requests via a 'switching system'. During the malware attack, a proxy switch was created and all the fraudulent payment approvals were passed by the proxy switching system.

ATMs compromised: When depositors withdraw money at ATMs, a request is transferred to the respective bank’s CBS. If the account has sufficient balance, the CBS will allow the transaction. In the case of Cosmos Bank, the malware created a proxy system that bypassed the CBS. While cloning the cards and using a ‘parallel’ or proxy switch system, the hackers were able to approve the requests – withdrawing over INR 80.5 crore in approximately 15,000 transactions.

Reserve Bank of India (RBI) guidelines: RBI has clear guidelines to protect against incidents such as the Cosmos Bank attack which must be followed. The security measures across Indian banks are moderate and given the high level of coordinated international attacks, all banks need to upgrade their security mechanisms.

Why is this attack more serious?

Just a few days prior to this attack, the American FBI had warned banks of a major hacking threat to ATMs worldwide. According to Krebs On Security, the influential cyber-security blog run by journalist Brian Krebs, a confidential alert to international banks informed them that criminals were plotting an imminent, concerted global malware attack on ATMs.

Smaller banks with less sophisticated security systems were believed to be most vulnerable to attack – with a scheme known as 'ATM cash-out' as the likely approach that the criminals might take. This is where crooks hack a bank or payment card processor and use cloned cards at ATMs around the world to fraudulently withdraw millions of dollars in just a few hours.

Banking experts and industry players fear this could be a 'pilot run' unless the authorities take the attack seriously. Essentially, this malware attack was not against any bank but rather, the banking system. It was carried out at international scale in a meticulously coordinated manner.

1.(j) The Zeus Trojan

Zeus is a Trojan used to steal banking credentials by “Man In The Browser” keystroke logging, and form grabbing. It’s spread mainly through drive-by downloads and phishing schemes. To give an idea on the use Zeus within the cyber crime ecosystem, consider that 9 million of those phishing e-mails have been sent since 2009.

Zeus was first detected in July 2007, when it was used to steal information from the United States Department of Transportation. the then current version of Zeus’ source code was leaked, and in October, the abuse.ch blog reported a new custom build of the trojan that relies on more sophisticated peer-to-peer capabilities.

In reality, the availability on the Zeus source code online has made it possible to develop a model of sale known as “malware-as-a-service.” Many groups of cyber criminals have started to offer customization of malicious code underground, according to the specific requests of their clients. In a short time, numerous customized variants of Zeus were found on the black market, including a version to work with social media, or to be able to be controlled by C&C servers hidden in Tor network. A Trojan is a harmful piece of software that users are typically tricked into loading and executing on their computers. After it is installed and activated, Trojan attacks the computer leading to deletion of files, data theft, or activation/spread of viruses. Trojans can also create back doors to give access to hackers.

How do fraudsters operate?

Step – 1

Fraudsters use spamming techniques to send e-mails to numerous unsuspecting people.

Step – 2

Customers who open or download the attachment in these emails get their computers infected.

Step -3

When the customer performs account/card related transactions, the Trojan steals personal information and sends them to fraudsters.

Step – 4

These details will then be used to conduct fraudulent transactions on the customer’s account.

How to protect yourself from fraud:

Never open e-mails or download attachments from unknown senders. Simply delete such emails.

Installing antivirus helps. It scans every file you download and protects you from malicious files.

Enable automatic OS updates or download OS patch updates regularly to keep your Operating System patched against known vulnerabilities.

Install patches from software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan.

Download and use the latest version of your browser.

If your computer gets infected with a Trojan, disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system If necessary, get your computer serviced.

1.(k) DDoS attacks

Another insidious cyber threat for online banking services are DDoS attacks. Security experts and law enforcement warned the banking sector of a possible rise of DDoS attacks, both financially and politically motivated. In late 2012 and early 2013, the self-proclaimed Muslim hacktivist group Izz ad-Din al-Qassam

Cyber Fighters conducted Operation Ababil. That caused the destruction of banking websites of the US top banks including U.S. Bankcorp, JPMorgan Chase & Co, Bank of America, PNC Financial Fervices Group, and SunTrust Banks.

Security experts noted that the hackers adopted an anomalous strategy for DDoS attacks. Instead of using botnets, they hit targets involving a network of volunteers that deliberately have participated in the operations. While a classic botnet, although is very efficient, is quite simple to detect due the presence of anomalous traffic to and from the Command and Control servers, in this case the presence of volunteers complicates the mitigation of the attack.

The DHS and FBI have reportedly been liaising with cyber security officials in 129 other countries, and shared details of a total of 130,000 IP addresses that have been used in the attacks. The attacks have resulted in customers sometimes being unable to access online or mobile banking services, due to the extension of the attack.

Main categories of DDoS attacks are:-

Volume Based Attacks- The attacker tries to saturate the bandwidth of the target's website by flooding it with a huge quantity of data.

Protocol Attacks- The attacker's goal is to saturate the target servers' resources or those of intermediate communication equipment (e.g., load balancers) by exploiting network protocol flaws.

Major trends that DDoS mitigation solution providers are observing are:-

Larger and larger network attacks- These large-scale attacks often use SYN flood and DNS amplification as their tools of choice.

Hit and Run attacks- These are smaller scale application layer attacks that don't last very long, but occur every few days.

DDoS attacks are also used for the purposes of extortion, or as a diversion to hide the effects of an ongoing attack. The latest trend observed for recent offensive operations against numerous US banks is that fraudsters are targeting wire payment switches, instead to hitting directly into the banking accounts of individuals and businesses.

1.(l) SIM Swap

Under SIM Swap, fraudsters manage to get a new SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account.

How do fraudsters operate?

Step – 1

Fraudsters gather customer’s personal information through Phishing, Vishing, Smishing or any other means.

Step - 2

They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing asng the customer.

Step – 3

The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

Step – 4

Fraudster then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

1.(m)Vishing

Vishing is one such attempt where fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

How do fraudsters operate?

Step – 1

The fraudster poses as an employee from the bank or a Government / Financial institution and ask customers for their personal information.

Step – 2

They cite varied reasons as to why they need this information. For e.g. reactivation of account, encashing of reward points, sending a new card, linking the Account with Aaddhar, etc.

Step – 3

These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer’s account without their knowledge.

1.(n)Smishing

Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

How do fraudsters operate?

Step – 1

Fraudsters send SMS intimating customer’s of prize money, lottery, job offers etc. and requesting them to share their Card or Account credentials.

Step – 2

Unaware, the customer’s follow instructions to visit a website, call a phone number or download malicious content.

Step – 3

Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on customer's account, causing them financial loss.

(2).Preventive Measures to Control Cyber Crimes in Banking Sector.

Challenges Fighting and preventing cyber criminals from damaging infrastructures are is very serious challenge to our law and enforcement agencies. It is often difficult to determine the cyber criminal and their community. The techniques used by cyber criminals are continuously evolving and making it more challenging. The following are some challenges of cyber crimes related to mobile and online banking.

2 (a). Tracking the origin of crime- Tracing cyber criminals is very difficult because criminal investigations and criminal activity itself is borderless by nature.

2 (b). Growth of the underground cyber crime economy -the fight against cyber crime is the growth of an underground cyber crime economy. The underground economy attracts many digital experts and talented individuals with a specialty around cyber initiative.

2 (c). Shortage of skilled cyber crime fighters- skilled manpower is requiring implementing cyber security measures and encountering such cyber attacks.

2 (d). Widespread use of pirated software- the most important challenge is preventing the cyber crime. The prevalence of software piracy, as pirated software is more prone to attacks by viruses, malware and Trojans.

(3).Safety Tips for Online Secure Transaction:-

3(a). If the network is not properly secured- avoid online banking, shopping, entering credit card details, etc Check your online account frequently and make sure all listed transactions are valid

3(b). Never ever click on a link- Be extremely wary of e-mails asking for confidential information they could be phishing e-mails from fraudsters. Donot click on link given in a spam e-mail.

3(c). Always delete spam-delete spam e-mails immediately and empty the trash box to prevent clicking on the same link accidentally.

3(d). Beware of lotteries- please beware of lotteries that charge a fee prior to delivery of your prize. Do not respond to lottery messages or call on the numbers provided in the text messages.

3(e). Check if the website is secure- While using a credit card for making payments online, check it if website is secure as the CVV will also be required for online transactions, is printed on the reverse of credit card. Do not provide photocopies of both sides of the credit card to anyone .It can be misused by the fraudsters for online purchases.

3(f). Notify your bank/credit card issuer - if you do not receive the monthly credit card statement on time, if a credit card is misplaced or lost, immediately inform to your bank/ credit card issuer. Do not share bank credentials in public or over phone

Secure Net-Banking Tips

- Keep your Customer ID and password confidential and do not disclose it to anybody.

- Change your password as soon as you receive it by logging into your Net Banking account. Memorize your password, do not write it down anywhere.

- Avoid accessing internet banking from shared computer networks such as cyber cafes or public Wifi network like hotel/airport etc.

- Do not click on links in the emails or sites other than the genuine net banking site of your Bank to access your Net Banking webpage.

- Always visit the Bank's Net Banking site through Bank's home page by typing the bank's website address on to the browser's address bar.

- Always verify the authenticity of the Bank's Net Banking webpage by checking its URL and the PAD Lock symbol at the bottom corner of the browser.

- Disable "Auto Complete" feature on your browser.

- Uncheck "User names and passwords on forms", click on "Clear Passwords"

- Click "OK"

- Use virtual keyboard feature while logging into your internet banking account.

- Do cross check your last login information available on Net Banking upon every login to ascertain your last login and monitor any unauthorized logins.

- Always type in your confidential account information. Do not copy paste it.

- Monitor your transactions regularly. Use Bank's Alerts service and bring any fraudulent transaction to the notice of the bank.

- Always logout when you exit Net Banking. Do not directly close the browser.

Secure ATM Banking

- Memorize your PIN. Do not write it down anywhere, and certainly never on the card itself.

- Do not share your PIN or card with anyone including Bank employees, not even your friends or family. Change your PIN regularly.

- Stand close to the ATM machine and use your body and hand to shield the keypad as you enter the PIN. Beware of strangers around the ATM who try to engage you in any conversation.

- Do not take help from strangers for using the ATM card or handling your cash

- Do not conduct any transaction if you find any unusual device connected to your ATM machine.

- Press the 'Cancel' key and wait for the welcome screen before moving away from the ATM. Remember to take your card and transaction slip with you.

- If you get a transaction slip, shred it immediately after use if not needed.

- If your ATM card is lost or stolen, report it to your bank immediately

- When you deposit a cheque or card into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report it to your bank.

- Register your mobile number with the Bank to get alerts for your transactions

- If your card gets stuck in the ATM, or if cash is not dispensed after you keying in a transaction, call your bank immediately

- If you have any complaint about your ATM/Debit/Credit card transaction at an ATM, you must take it up with the bank

Secure Phone Banking

- While talking to the Phone Banking officer, never disclose the following

  o 4 digit ATM/IVR PIN

  o OTP

  o Net Banking password

- CVV (Card Verification Value)

- Ensure that no one sees you entering you PIN (personal identification number).

- Avoid giving verification details to the Phone Banking officer while in public places.

- The Phone Banking channel is meant to be used by the account holder only. Do not transfer the line or hand over the phone to any other person after you complete self-authentication.

Secure Online Shopping tips

- Always shop or make payments through trusted/reputed websites.

- Do not click on links in emails. Always type the URL in the address bar of the browser.

- Before entering your private details, always check the URL of the site you are on!

- If you are a frequent online shopper, signup for Verify by Visa and Master Card secure code program.

- Check your account statements regularly and bring any fraudulent transaction to the notice of the bank.

- Check for PAD LOCK symbol on the webpage before starting to transact.
- Do not click on

Chapter=3

Laws and remedies against cyber Crimes in Banking sector

--

In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term ‘Cyber’ became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cyber crimes at the domestic and international level as well.

Though the word Crime carries its general meaning as “a legal wrong that can be followed by criminal proceedings which may result into punishment” whereas Cyber Crime may be “unlawful acts wherein the computer is either a tool or target or both”.

The world 1st computer specific law was enacted in the year 1970 by the German State of Hesse in the form of ‘Data Protection Act, 1970’ with the advancement of cyber technology. With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system. It is under these circumstances Indian parliament passed its “INFORMATION TECHNOLOGY ACT, 2000” on 17th oct to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes.

Impact of Cybercrime on Banks Finances

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions. The banking sector is forced to evaluate its current practices in order to analyze and manage their risks effectively. Technology driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in everyday life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services affordable and accessible . However, this has also increased the risk of becoming targets of cyber attacks. Cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the banks finances. Globally, USD 114 Billion is lost nearly every year due to cybercrimes, and the cost spend to combat cybercrimes is double is amount i.e. USD 274 billion (Symantec Cyber Crime Report, 2012). On an average, banking facilities take 10 days to fully recover from a cyber act which further adds to the cost of operation. Comparing the financial losses faced by the Indian Banking Sector, it is nearly 3.5% of the loss in cash in comparison to global loss. USD 4 billion is lost in recovering from the crime and USD 3.6 billion is spent to combat such crimes from happening in future. The average time taken to resolve the crime in Indian banking sector is also higher in comparison to global scenario i.e. 15 days . In order to fight these cybercrimes, the banking sector needs to collaborate with global authorities and watchdog organisations so that a model can be developed which can help in controlling and dealing with such threats. The main issue of concern here is that there is absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks (Stafford, 2013). High profile banks in the UK like Barclays and Santander were targeted by hackers who stole personal information of nearly 2.9 million credit card customers by hacking the software maker system of these banks, which led them to incur huge losses. However, the scenario is not restricted to UK, in US as well such attacks have surfaced in the past years and in order to curb the affect, they launched the program Quantum Dawn 2 which test the efficacy of system installed in banks in response to cyber-attacks (Stafford, 2013). However, the sad truth is that most the systems are one-step behind the tools adopted by cyber criminals which has resulted in demand of development of system which is flexible is meeting and destroying the incoming assaults. A solid defense system to resolve attack is the need of the hour before, during and after the attack.

Who will bear liability in cyber fraud cases banks or customers

The digitization of the financial sector is having unintended, but unavoidable consequences — cyber frauds and ransomware attacks. To assuage the fears of depositors, the Reserve Bank of India (RBI), in its annual report for 2017-18, highlighted the framework for containing the spread of unauthorized transactions and limiting the liability of customers.

The prevailing norms categorize customers' exposure to frauds into two categories — zero liability and fixed liability. Customers can rest assured if the fault is on the part of the bank. Even if the breach can be traced to deficiencies existing in the system, and not on banks, the customers will not have to bear a loss**.**

To claim immunity from liability, customers will have to notify their bank within three working days of the time of breach. In the case of unauthorized transactions attributed to systemic flaws, customers are expected to report the incident between four to seven days of the incident. Depending on the type of account and the circumstances in which the fraud took place, the liability to be borne by customers can range from Rs 5,000 to Rs 25,000.

The central bank's norms restricting the liability of customers places the ball in the court of banks. Cashstrapped lenders will have to compensate depositors who have been defrauded in online scams unless it can provide conclusive proof that the fault lies on the part of the victim. Experts are of the opinion that banks should be slapped with penalties for not adhering to norms laid down by the RBI.

However, many banks continue to disregard the existing guidelines. In the case of small amounts, the length of the investigation can be a deterrent for customers seeking a refund. After following up with banks in the immediate aftermath of the fraud, customer interest may recede if the pendency in settlement is long, and the money in question is relatively small.

According to the RBI’s liability norms, the amount of money constituting the unauthorized transaction has to be transferred to the customer’s account inside 10 working days from the date of notification. Investigations undertaken by the bank’s board are instructed to establish liability within 90 days of the breach being flagged.

Time taken to report fraud	=Customer’s liability
Less than 3 working days	=zero
Between 4-7 working days	=Transaction value or between Rs 5,000 – Rs 25,000, whichever is lower
Over 7 working days	= Dependent on policy of bank’s board

The central bank has not provided a timeline for the implementation of its norms. However, after the guidelines were released, banks have been more responsive in acting against complaints of cyber fraud.

The Economic Times reported on August 3 that around 76 customers from were defrauded to the tune of Rs 20 lakh after their debit and credit cards were skimmed and cloned. In this case, the victims were compensated in a few days, and the fraudsters, nabbed. For customers fighting a lone battle, the prospects of recovery are less promising.

If by error of judgement, customers share their credentials with fraudsters, they will be held liable, allowing the bank to wash its hands off the case. Also, if there is a gap of more than seven days between the time the initial breach took place and when it was reported, the customer will not be able to recover the amount lost from the bank.

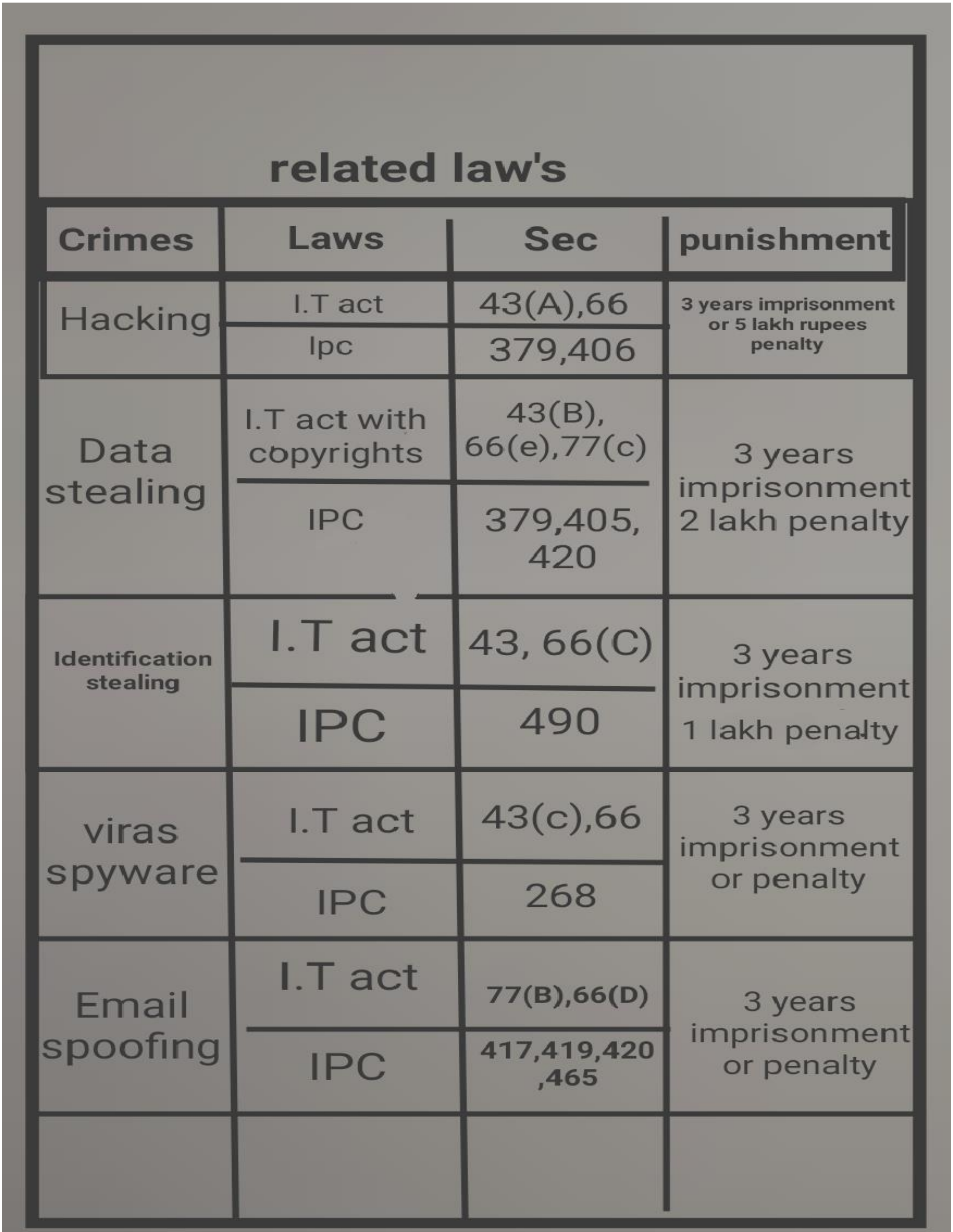
However, if money is siphoned off from their accounts even after the fraud has been reported, the liability is to be borne by the bank**.**

Remedies for financial fraud

Apart from the criminal processes, S.46 IT Act also provides for remedies against data theft, hacking, virus attacks and financial frauds covered under Chapter IX (S.43 to S.45) by filing an application before the adjudicating officer. Presently, the ad-hoc system of the secretary of the IT ministry acting as the said authority continues. This remedy has been very successfully availed of by victims of financial frauds. However, there is clear ignorance about the fact that the jurisdiction of this authority far exceeds claims against banks.

Businesses also have to take into account possibility of being held liable for data protection violations (S.43A & S.72A IT Act). Apart from the possibility of civil and criminal actions being initiated against them, if they fail to report cyber security incidents to the central authority, they would be liable for action. Being themselves victims of cyber crimes will not help them wriggle out of this requirement. Further, businesses which fall within the category of “intermediaries” have very heavy responsibilities

and duties under the IT Act.



related law's

Crimes	Laws	Sec	punishment
Hacking	I.T act	43(A),66	3 years imprisonment or 5 lakh rupees penalty
	Ipc	379,406	
Data stealing	I.T act with copyrights	43(B), 66(e),77(c)	3 years imprisonment 2 lakh penalty
	IPC	379,405, 420	
Identification stealing	I.T act	43, 66(C)	3 years imprisonment 1 lakh penalty
	IPC	490	
viras spyware	I.T act	43(c),66	3 years imprisonment or penalty
	IPC	268	
Email spoofing	I.T act	77(B),66(D)	3 years imprisonment or penalty
	IPC	417,419,420 ,465	

Conclusion

This research has given an outline to the idea of E-saving money by talking about profoundly different digital wrongdoings, distinguished explicitly in the managing an account division. The Saving money framework is the soul and spine of the economy. Data Innovation has turned into the foundation of the saving money framework. It gives an enormous help to the regularly expanding difficulties and managing an account necessities. By and by, banks can't consider presenting money related item without the nearness of Data Innovation. Anyway Data Innovation has an unfavorable effect too on our managing an account division where wrongdoings like, phishing, hacking, falsification, bamboozling and so on are submitted. There is a need to avert digital wrongdoing by guaranteeing validation, recognizable proof and check procedures when an individual goes into any sort of saving money exchange in electronic medium. The development in digital wrongdoing and intricacy of its examination strategy requires proper measures to be embraced. It is basic to expand the collaboration between the partners to handle digital wrongdoing. As indicated by National Wrongdoing Records Agency it was discovered that there has been a tremendous increment in the quantity of digital violations in India in recent years. Electronic wrongdoing is a difficult issue. In instances of digital wrongdoing, there isn't just money related misfortune to the banks yet the confidence of the client upon banks is additionally undermined. Indian managing an account division can't abstain from keeping money exercises helped out through electronic medium as the investigation recommend that there has been an expansion in the quantity of installments in e-saving money. Nonetheless, the adjustment in the saving money industry must be such which suits the Indian market. In conclusion, it very well may be presumed that to dispense with and kill cybercrime from the internet is certifiably not an apparently conceivable assignment however it is conceivable to have an ordinary keep an eye on managing an account exercises and exchanges. The main auspicious advance is to make mindfulness among individuals about their rights and obligations and to additionally making the usage of the laws all the more firm and stringent to check wrongdoing.

The rapid growth to global electronic crime and the complexity of its investigation requires a global presence. Presently, the measures undertaken the banks are not sufficient and therefore it is imperative to increase cooperation among the banks across the world for the development of tools and models which can be applied to counter global banking cybercrimes. According to the National Crime Records Bureau (NCRB), a total of 9,622 cybercrime cases were registered in India in 2014 while, 11,592 and 12,317 cases of cybercrime were registered in 2015 and 2016 respectively. Cyber attacks have become more organised with significant funding, passion, they are sophisticated, they often gain access and they wait for the right time, for the moment of their choice for their attacks. By increasing employment and awareness in these areas such crime can be controlled.

Suggestions

1) As there is no explicit requirement identified with the law, the significant effect of these violations is left unsolved numerous multiple times, a demonstration must be authorized to control this sort of danger.

2) The law implementation ought to be extremely unbending, and refreshed occasionally to monitor such wrongdoings.

3) There ought to be quick track portable courts to explain these cases, to meet the complaints and fabricate certainty among the general population.

4) The legislature ought to likewise keep a track on the working system exercises with the assistance of Huge Information Banks.

5) Disciplines and punishments should be practiced completely so as to limit the effect of these issues and punish the assailants.

6) Mindfulness Projects ought to be started so as to educate the general population about the continuous situation and forthcoming dangers.

7) General society should report these cases to the Digital Wrongdoing Branch in the issues related as opposed to simply alluding it to the banks, to guarantee quick and strict activities.

How to make a complaint

- 1. Collect Bank statement from the concerned bank showing the fraudulent transactions.
- 2. Make a copy of SMSs received related to the alleged transactions.
- 3. Copy of your ID proof and address proof as shown in the bank records

- 4. Lodge a complaint at your nearest Police Station explaining complete incident along with the above mentioned documents.

Bibliography

http://securityaffairs.co/wordpress/17680/cyber-crime/group-ib-threat-intelligence-report-2012-2013-h3-must-read.html

http://securityaffairs.co/wordpress/19010/cyber-crime/online-banking-cybercrime.html

http://securityaffairs.co/wordpress/13991/cyber-crime/apwg-global-phishing-survey-report.html

http://resources.infosecinstitute.com/phishing-dangerous-cyber-threat/

http://securityaffairs.co/wordpress/15379/cyber-crime/carberp-banking-trojan-code-or-sale.html

http://securityaffairs.co/wordpress/16611/malware/kins-trojan-is-threatening-banking-sector.html

http://securityaffairs.co/wordpress/17557/cyber-crime/hesperbot-new-powerful-banking-trojan-found-eset.html

http://securityaffairs.co/wordpress/13771/cyber-crime/new-wave-of-ddos-against-eu-banking-can-hide-a-sinister-mystery.html

http://securityaffairs.co/wordpress/12489/security/mobile-cyber-threats-from-risky-apps-to-black-market-activity.html

http://securityaffairs.co/wordpress/17205/cyber-crime/ddos-to-hide-attacks-against-wire-payment-switch-systems.html

http://securityaffairs.co/wordpress/18772/cyber-crime/atlas-q3-2013-ddos.html

http://securityaffairs.co/wordpress/11113/cyber-crime/group-ib-banking-trojan-carberp-sales-were-reborn-with-bootkit-module.html http://securityaffairs.co/wordpress/15003/malware/facebook-zeus-malware-targeting-bank-accounts.html

https://zeustracker.abuse.ch/statistic.php

http://www.zdnet.com/linux-desktop-trojan-hand-of-thief-steals-in-7000019175/

http://blogs.rsa.com/wp-content/uploads/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf

http://securityaffairs.co/wordpress/12195/malware/threat-report-h2-2012-proposed-by-f-secure.html

http://blog.sucuri.net/2013/07/phishing-2-0-redirecting-credit-card-payments-to-malicious-domain.html