Cyber-Crimes in India

Ankita Pachar

August 6, 2021

CYBER-CRIMES IN INDIA

INDEX

Introduction:

The life of humans is made easier through the invention of computer which is being used for various purposes starting from the individual to large organizations across the globe.

Computers and internet have become very necessary and useful in our daily lives. This gave birth to cybercrime; cyber-crime is any illegal activity which is committed using a computer network (especially the internet). Cyber-crime involves the breakdown of privacy, or damage to the computer system properties such as files, website pages or software. Most of the cases in India were found, crimes are committed due to lack of knowledge or by mistake. Cybercrime is any criminal activity involving computers and networks.

Now comes the term “Cyber Law”. Cyber Law can be described as the laws that deals with legal issues related to use of inter-networked information technology.

Research Objectives:

- To study about Cyber-Crimes.
- To study about Cyber Criminals.
- To study about Cyber Law in India.

Limitations

According to the data collected by a team in the past few months considering the amount of time given to us (3-4 months) is very limited and the information obtained by a research does not cover the whole topic of cybercrime on which we have done our project, considering the fact that the data is only based on cybercrimes committed in India an occurred in certain states.

Research Methodology

1.Primary Data: Our Research has no primary data as it is entirely based on secondary data.

2. Secondary Data: This research is entirely based on the secondary data to study on cybercrimes in India. The secondary data is collected from the reputed newspapers, magazines, journals and various sites on the internet.

Review of Literature:

- Criminals are taking advantage of the fast internet speed and benefit provided by the internet to perform large and different criminal activities, says Agarwal. In her article, she suggested that it becomes the duty of all the active internet users to be aware of the cyber-crime and the cyber law made to deal with cyber-crimes.
- A survey was conducted by the Mehta about the awareness of the cybercrime in India which resulted those men are more aware about the cybercrime than women.

- Another survey by Hasan in 2015 on awareness of cybercrime in Malaysia where female students are more aware than male students.

Objective-1

To study about Cyber-crimes

Introduction:

Cybercrimes are the types of crime that are committed in the cyber world. This type of crimes has expanded its roots very rapidly in every aspect of life. The term cybercrime is a wide term and therefore cannot be explained in one or two sentences. This is a type of crime in which computers and computer networks are put into use or more specifically, abuse and the crime is committed either through them or to them or both.

According to the survey by Ipsos, the frequency of complaints in India is much higher, that is, 32% more than the USA, UK and other advances technology countries where it ranges only about 11-15%. One of the main causes of such rapid increase in the cybercrime cases is the dependency on the internet even for the most basic requirements.

History of Cybercrime:

In the early era, the crime related to computers were to destroy them physically. There was no cybercrime. During 1870's, initial cases of cybercrime appeared where teenagers were known for telephone phrasing. By the 1990s, internet was seen as the fastest medium in human history and increase in technology. In 1992, the first cybercrime case appeared where the first polymorphic virus was released. In India, the first case of cybercrime was of Yahoo V. Akash Arora.

Classifications of Cyber-crimes:

Some types of cybercrimes are:

1.Hacking: Hackers is an unauthorized user who attempts to access the information from a victim's system. Hacking is a crime even if it does not provide any visible damage but attacks the privacy of data.

2. Cyber Stalking: Cyber Stalking involves the use of internet to harass or threat or false accuse someone. It is main done by men and the majority of victims are women.

3. Spamming: This type of cybercrime involves, sending of unsolicited bulk and commercial messages over internet. It causes damages such as overloading networks or negative impacts on consumer attitudes etc.

4. Phishing: It is a criminally fraudsters where they earn huge amount of money by acquiring sensitive information such as username, password and credit card details.

5. Web Jacking: The term refers to forceful taking of control of a website by cracking the password.

6. Spreading Computer Virus: The unauthorized user will provide or make some set of instruction which will perform some malicious operations. The virus may stop the normal function of the system and will ruin the system. This may be done by the following- Emails, CDs, Pen Drives, Multimedia, Internet.

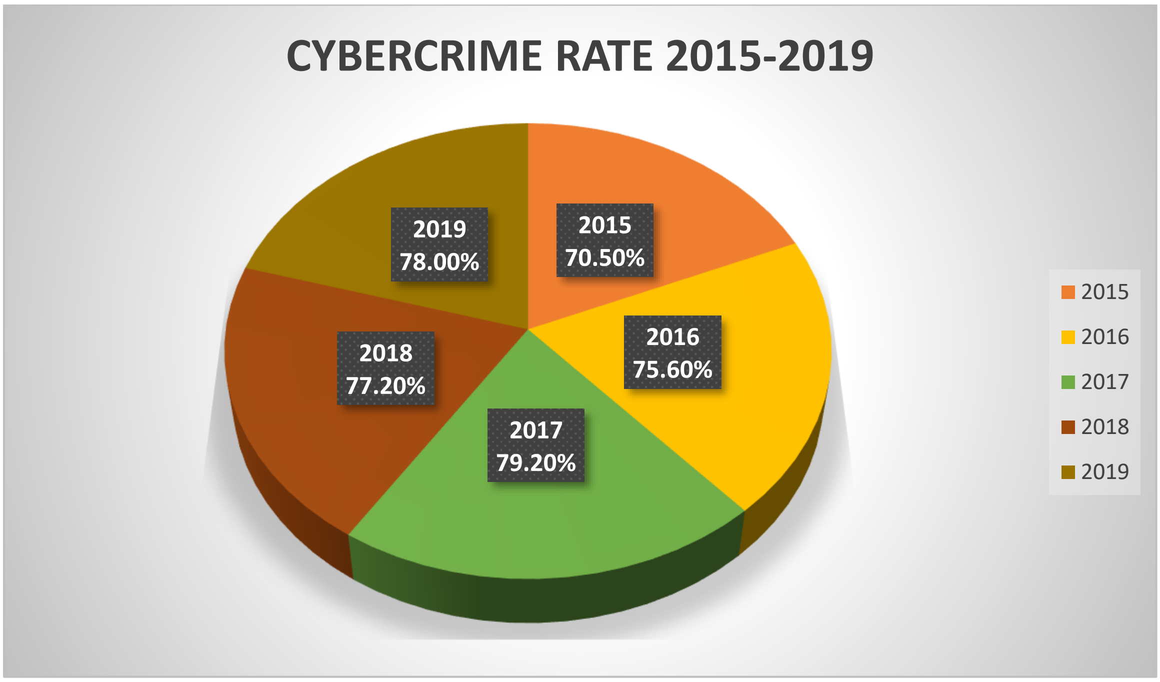


Fig.1 Cybercrime Rate in India.

The rate of cybercrime in above fig has increased from 2015 that is 70.50%. It has constantly increased since 2015 till the year 2017(70.50%-79.20%). After 2017 the cybercrime rate decreased by 2% from 79.20% to 77.20%. As every year the internet users are increasing the rate of cybercrime in 2019 has again increased by 1% that is in 2019 (78.00%).

Objective-2

To study about Cybercriminals

Introduction:

Cyber criminals are individuals or group of people who perform hostile activities on digital systems or using technology to steal the computer information or personal data to generate profit. They are very difficult to identify on both individuals or group level because they use various security measures. Cyber security experts informs that the cyber criminals are using more ruthless methods to achieve their objectives.

The growth of the global cybercriminals network, which increased the opportunities for financial incentives, has created a number of different types of cyber criminals, many of them are threat to the government and corporation.

Types of Cybercriminals:

1.Identity Thieves:

Identity Thieves are those cyber criminals to access the victim's personal information like- Name, Address, Phone number and many more. They use such personals information to make financial information and social security number. Identity theft is one of the oldest cybercrimes during the early year of the internet. Initially, they basic use hacking techniques, to steal the desired information.

2. Internet Stalkers:

Internet Stalkers are individuals who evilly monitors the online activity of their victims to terrorize or acquire personal information. This type of cybercrime is done through the use of social networking platforms. The motives for such attackers are differ depending on other cyber criminals, but many internet stalkers seek to acquire important information that they can be used that they can be used for bribery, slander or both. Businesses should be aware of internet stalkers as well as they strategies that they utilize, their employees become the victims of internet attackers. The internet stalker causes emotional distress to the employees or obtain data for blackmail.

3.Phishing Scammers:

Phishers are cyber criminals who attempt to get the victim's personal or sensitive information from his computer. This is often done with phishing websites that are designed to copy the small-businesses, corporate, firm or government websites. victim's computer often falls in prey to such type of activities by unknowingly providing their personal information. When such personal information is obtained by the frauds, they either use it for personal use or sell it in dark web. It's important for the businesses to be aware of such activities and follow protective measures.

4. Cyber Terrorists:

Cyber terrorism is a well-developed, politically inspired cybercriminal in which he takes the information or government computer systems and networks which results in harming the country, individuals, organization and businesses. The main difference between the cyber terrorism and cyber-attack is that cyber terrorism depends on stealing the data related to government or political to gain financial requirements.

5. Kids (age group 9-16):

As it is hard to believe that kids can also be cyber criminals knowingly or unknowingly. Teenagers are the most amateur hackers. To these teenagers, hacking the computers or websites and stealing information is pride for them. They commit these crimes without knowing that what they are doing is crime.

How to avoid being a victim?

1. Use Strong passwords.

2. Keep Your social media accounts private.

3. Secure your Mobile Devices.

4. Protect your data.

5. Protect your identity online.

6. Keep your computer current with the latest patches and updates.

7. Protect your computer with security software.

Case study

ATM System Hacked in Kolkata:

In July 2018, fraudster had hacked a Caranna Bank ATM server. They were more than 50 victims who lost their money. It was found that they have planned to target more than 300 ATM users in India. The hackers have wiped off the ATM with minimum of INR 10,000 and maximum of INR 40,000. On August,2018, two men were arrested who were the hackers who used skimming method to hack ATM.

Objective-3

To study about Cyber Law in India

Introduction:

India cyber laws carry the information technology act 2000 which came into force on October 17 2000. The main purpose of this act is to provide legal acknowledgement to electronic commerce and to facilitate filing of electronic records.

Cyber law helps protect the users from harm and serious loss of personal information and data by enabling investigation and prosecution of online criminal activity.

Need of Cyber Law:

It was very necessary that cyber laws would come into existence, which helped the country deal with cyber criminals and digital and technical, and internet crimes.

Cyber law plays and very important role in the new approach of technology. Many people might not be aware of it but every action taken in the cyberspace has his own legal and illegal aspects.

It is very important that is cyber law is very important cause it is connected to all the transactions made with the help of internet and all the data shared with the help of internet.

India's legal system in place is extremely detailed and will defined several laws have been enacted and implemented and foremost among them was the constitution of India.

Beginning of the rise of new and complex legal issues have been signaled with the arrival of internet. By keeping in mind the cultural scenarios of the relevant time, it may be pertinent to mention that all the existing laws in place in India where enacted.

All the different activities of cyberspace including all relating aspects could not be interpreted in the light of emerging cyberspace. Hence comedy need for enactment of relevant cyber laws.

Existing laws did not give any legal validity or sanction to the activities in cybercrime. For example, majority of female users use require the internet, email is not “legal” in our country till today.

Key Elements of information technology act 2000:

- Now e-mail is a valid and legal form of communication.
- Legal validity given to digital signatures.
- Notices on internet through e governments is allowed through this act.
- The companies or the company can communicate through the internet.
- This provides remedy in the form of money to the company if in case there is any harm or loss done to the company.

Overview of other laws amended by the IT,2000 are as follows:

SEACTION	DESCRIPTION	PUNISHMENT
65	TEMPTING WITH THE COMPUTER SOURCE DOCUMENTS.	3 YEAR IMPRISONMENT OR FINE OF RUPEES 2 LACS OR BOTH.
66	HACKING WITH COMPUTER SYSTEM, DATA ALTERATION.	3 YEARS OF IMPRISIONMENT OR FINE OF 2 LACS OR BOTH.
66A	SENDING OFFENSIVE MESSAGES THROUGH ANY COMMUNICATION SERVICES.	3 YEARS OF IMPRISONMENT FOLLOWED BY A FINE.
66C	IDENTITY THEFT.	3 YEARS OF IMPRISONMENT OR FINE OF RUPEES 1 LAKH.
66D	CHEATING BY CHARACTERIZATION BY THE USE OF COMPUTERS RESOURCES.	3 YEARS OF IMPRISIONMENT ALONG WITH FINE THAT ALSO MAKE STAND UP TO RUPEES 1 LAKH.
66E	PRIVACY OR VIOLATION.	3 YEARS OF IMPRISIONMENT OR FINE 2 LAKH.

Findings::

1.From the above survey tools found out that there are different ways of committing cybercrimes and every different type of crime there are different set of rules and judgement.

2. According to the data analysis it was found out that there is no specific age group for people who commit cybercrimes even though the data is very limited.

3. There was a significant jump in cybercrimes reported in the year 2019 in India, that year over 44.5 thousand cybercrime cases were reported.

4. There is no reasonable motive behind people who commit cyber-crimes, they are committed mostly with the intent of causing trouble to specific people and society.

5. Over the years the Indian government has introduced a lot of rules and regulations regarding the usage of internet and different ways of finding out the people responsible for committing cybercrimes.

6. The Indian constitution has changed and improved a lot considering the situation over the years 7. The same punishment is given to a single individual or a group involved in committing a cybercrime depending upon the matter.

8. There are certain case studies which help an individual understand how a cyber-criminal think does his work and is an awareness for public.

Suggestions:

There are different types of punishments for people committing cyber-crimes and different types of laws and a number of ways to find out the people committing cyber-crime, in spite of all that people need to be very careful and be aware about the cyber-crimes, the awareness could be spread through different media platforms and awareness performances. The cyber cafe owner needs to be very precise and careful while collecting the data of the internet users and people need to be very much careful with hackers and scammers who tried to obtain your personal data and hijack your personal devices with the help of links pop up ads etc

Conclusion:

The above data is the total information that our group has collected in the time given to us for our project. Cybercrime was a very vast topic a lot of people all over the world have faced this situation. Although the data we have collected does not cover the whole topic as the research has been done on the incidents that have taken place in India and up to certain specific States.

The data we have collected is very accurate even though it is limited and very useful for the people which helps them understand about internet, cybercrime, cyber criminals and cyber law. The judgement is totally based on the laws made by the Indian constitution against the cyber criminals and are not our point of view neither are the point of use of people in India. Cyber-crime is a delicate topic and is one of the major social problems faced by people. The people found of committing the crime either be a single individual or a group will be punished by the court as per the law and every crime has its own punishment.

The above data helps us understand about the cyber-crimes its history and the changes it has been through over the years; it helps us understand about cybercriminals the way they behave the reason for them to commit such crimes and why do they commit such crimes and about the cyber laws which are made for people who have found guilty of committing this crime. All that is based on the data we have collected and not our perspective as project does not go against the laws and the research has been done by putting those laws into consideration.

References:

1. https://en.wikipedia.org/wiki/Internet_in_India

2.https://en.wikipedia.org/wiki/Internet_in_India#Wireless_internet

3.https://www2.ed.gov/pubs/OR/ConsumerGuides/internet.html

4.https://www.tutorialspoint.com/computer_concepts/computer_concepts_introduction_to_internet_www_web_browsers.htm

5.https://telanganatoday.com/when-internet-started-in-india

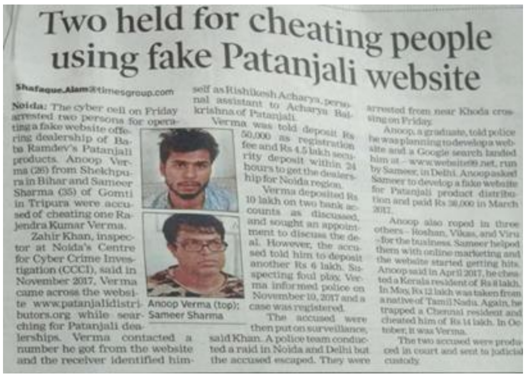
6.http://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html

7.https://asianetbroadband.in/effects-of-the-internet-on-society/

8.https://www.ukessays.com/essays/media/impact-of-the-internet-on-our-society-media-essay.php

9.https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals

10.https://www.researchgate.net/publication/307594049_A_Study_on_the_Cyber_-_Crime_and_Cyber_Criminals_A_Global_Problem



Two held for cheating people using fake Patanjali website

Shafaque.Alam@timesgroup.com

Noida: The cyber cell on Friday arrested two persons for operating a fake website offering dealership of Baba Ramdev's Patanjali products. Anoop Verma (26) from Shekhpura in Bihar and Sameer Sharma (35) of Gomti in Tripura were accused of cheating one Rajendra Kumar Verma.

Zahir Khan, inspector at Noida's Centre for Cyber Crime Investigation (CCCI), said in November 2017, Verma came across the website www.patanjalidistributors.org while searching for Patanjali dealerships. Verma contacted a number he got from the website and the receiver identified himself as Rishikesh Acharya, personal assistant to Acharya Balkrishna of Patanjali.

Verma was told deposit Rs 50,000 as registration fee and Rs 4.5 lakh security deposit within 24 hours to get the dealership for Noida region.

Verma deposited Rs 10 lakh on two bank accounts as discussed, and sought an appointment to discuss the deal. However, the accused told him to deposit another Rs 6 lakh. Suspecting foul play, Verma informed police on November 10, 2017 and a case was registered.

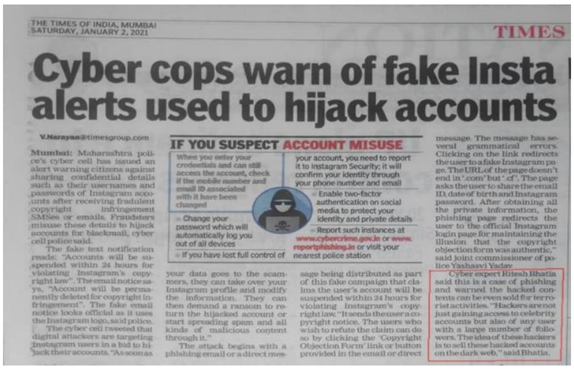
The accused were then put on surveillance, said Khan. A police team conducted a raid in Noida and Delhi but the accused escaped. They were arrested from near Khoda crossing on Friday.

Anoop, a graduate, told police he was planning to develop a website and a Google search landed him at – www.website99.net, run by Sameer, in Delhi. Anoop asked Sameer to develop a fake website for Patanjali product distribution and paid Rs 36,000 in March 2017.

Anoop also roped in three others – Roshan, Vikas, and Viru – for the business. Sameer helped them with online marketing and the website started getting hits. Anoop said in April 2017, he cheated a Kerala resident of Rs 8 lakh. In May, Rs 12 lakh was taken from a native of Tamil Nadu. Again, he trapped a Chennai resident and cheated him of Rs 14 lakh. In October, it was Verma.

The two accused were produced in court and sent to judicial custody.

Anoop Verma (top); Sameer Sharma



THE TIMES OF INDIA, MUMBAI
SATURDAY, JANUARY 2, 2021

TIMES

Cyber cops warn of fake Insta alerts used to hijack accounts

V.Narayan@timesgroup.com

Mumbai: Maharashtra police's cyber cell has issued an alert warning citizens against sharing confidential details such as their usernames and passwords of Instagram accounts after receiving fradulent copyright infringement SMSes or emails. Fraudsters misuse these details to hijack accounts for blackmail, cyber cell police said.

The fake text notification reads: "Accounts will be suspended within 24 hours for violating Instagram's copyright law". The email notice says, "Account will be permanently deleted for copyright infringement". The fake email notice looks official as it uses the Instagram logo, said police.

The cyber cell tweeted that digital attackers are targeting Instagram users in a bid to hijack their accounts. "As soon as your data goes to the scammers, they can take over your Instagram profile and modify the information. They can then demand a ransom to return the hijacked account or start spreading spam and all kinds of malicious content through it."

The attack begins with a phishing email or a direct message being distributed as part of this fake campaign that claims the user's account will be suspended within 24 hours for violating Instagram's copyright law. "It sends the user a copyright notice. The users who wish to refute the claim can do so by clicking the 'Copyright Objection Form' link or button provided in the email or direct message. The message has several grammatical errors. Clicking on the link redirects the user to a fake Instagram page. The URL of the page doesn't end in '.com' but '.cf'. The page asks the user to share the email ID, date of birth and Instagram password. After obtaining all the private information, the phishing page redirects the user to the official Instagram login page for maintaining the illusion that the copyright objection form was authentic," said joint commissioner of police Yashasvi Yadav.

Cyber expert Ritesh Bhatia said this is a case of phishing and warned the hacked contents can be even sold for terrorist activities. "Hackers are not just gaining access to celebrity accounts but also of any user with a large number of followers. The idea of these hackers is to sell these hacked accounts on the dark web," said Bhatia.

IF YOU SUSPECT ACCOUNT MISUSE

When you enter your credentials and can still access the account, check if the mobile number and email ID associated with it have been changed

- Change your password which will automatically log you out of all devices
- If you have lost full control of your account, you need to report it to Instagram Security; it will confirm your identity through your phone number and email
- Enable two-factor authentication on social media to protect your identity and private details
- Report such instances at www.cybercrime.gov.in or www.reportphishing.in or visit your nearest police station