Universe International Journal of Interdisciplinary Research
(Peer Reviewed Refereed Journal)

© UIJIR | ISSN (O) – 2582-6417
JAN. 2021 | Vol. 1 Issue 8
www.uijir.com

VARIOUS KINDS OF CYBER CRIMES & CYBER SECURITY IN INDIA

Author's Name: Shiksha Shreshtha

Affiliation: *Law Student,Kalinga University,Raipur, CG,India*

E-Mail: shiksha272002@gmail.com

DOI No. – 08.2020-25662434

Abstract

This paper talks about the issues and various types of cyber crimes that are happening these days and also the concept of cyber security The twentieth century has brought to reality the idea of a global village, where digital technology has interconnected and enmeshed the world economies, cultures and populations. India is no exception, with over 400 million internet users as of 2018, making it the second-largest internet population in the world. While greater connectivity via the world wide web promises large-scale progress, it also leaves our digital societies open to new vulnerabilities. Cyber crimes know no borders and evolve at a pace at par with emerging technologies.

Keywords: *Cyber Crimes, Cyber Security, Global village, Digital Technology.*

INTRODUCTION

In fact, according to a 2017 report, Indian consumers had lost over 18 billion U.S. dollars due to cyber crimes. In 2018, there were over 27 thousand cases of cyber crimes recorded in the country, marking an increase of over 121 percent compared to the number of cases just two years back. While the nature of crimes ranges from petty online frauds to lottery scams and sexual harassment, the most targeted crimes seem to be in the banking and finance sector.

Even then, it is important to remember that cyber vulnerabilities aren't just limited to private sectors. Some of the most dangerous data breaches have been with respect to government data. One such security breach was that involving India's unique citizen identification system- the Aadhaar, which got hacked in early 2018, compromising extensive personal information including bank details, address and biometrics of over a billion Indians.

Along with economic losses, cyber crimes also impact public safety- especially for minors and vulnerable sections of the society through incidents of cyber bullying and exploitation. In 2018 alone, India recorded over two thousand cases of cyber crimes related to sexual harassment and over 700 cases of cyber bullying against women and minors. Perhaps these high number of cases had led to an increased awareness about the issue of cyberbullying , and a large share of Indians felt that the responsibility for abusive behavior on social media lay with both the users as well as social media platforms.

However, one of the biggest impediments in curbing cyber crimes has been the lack of awareness on cyber hygiene leading to critical digital vulnerabilities. Most cyber crime incidents in India went unreported. And even when crimes were reported to authorities, the infrastructure and process to tackle such cases were largely inefficient. On the bright side, in 2018 the Indian government launched its National Cyber Crime Reporting Portal for citizens to register their complaints online. Under this initiative, cyber cells in various cities across the country have also been training police and government employees how to handle digital security incidents and increase public awareness at the same time.

The advancement of technology has made man dependent on Internet for all his needs. Internet has given man easy access to everything while sitting at one place. Social networking, online

shopping, storing data, gaming, online studying, online jobs, every possible thing that man can think of can be done through the medium of internet. Internet is used in almost every sphere. With the development of the internet and its related benefits also developed the concept of cyber crimes. Cyber crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber crimes, India is also not far behind the other countries where the rate of incidence of cyber crimes is also increasing day by day.

In a report published by the National Crime Records Bureau report (NCRB 2011), the incidence of cyber crimes under the IT Act has increased by 85.4% in the year 2011 as compared to 2010 in India, whereas the increase in incidence of the crime under IPC is by 18.5% as compared to the year 2010. Visakhapatnam records the maximum number of incidence of cases. Maharashtra has emerged as the center of cyber crime with maximum number of incidence of registered cases under cyber crimes. Hacking with computer systems and obscene publication were the main cases under IT Act for cyber crimes. Maximum offenders arrested for cyber crimes were in the age group 18-30 years. 563 people in the age group 18-30 years were arrested in the year 2010 which had increased to 883 in the year 2011.

TYPES OF CYBER CRIMES IN INDIA

- **Hacking**

Hacking is basically gaining unauthorized access to your system profit, protest, information gathering, or to evaluate system weaknesses. The provisions for hacking are given in IT Act, 2000 under section 43-A and 66 and section 379 & 406 of Indian Penal Code. The punishment for hacking is 3 years or shall be imposed with fine up to 5 lakhs.

- **Denial of Service**

It brings down the server (any server). It is known as the flooding machine with requests in an attempt to overload systems. It also uses bots for tasks. The provisions are given under section 43(f) of IT Act with imprisonment up to 3 years or with fine up to 5 lakh rupees.

- **Virus Dissemination**

It involves direct or search unauthorized access to system by introducing malicious programs known as viruses, worms etc. Virus needs host while worms are standalone.

Provisions are provided under the IT Act, 2000 under sections 43-C, 66 and section 268 of the Indian Penal Code.

- **Credit Card Fraud**

Card fraud begins either with the theft of the physical card or with the comprise of data associated with the account. Provisions of such fraud are given under Section 66 C and 66 D of IT ACT, 2000 and section 468 & 471 of Indian Penal Code, 1860.

- **Phishing**

A malicious individual or group who scam users. They do so by sending e-mails or creating web pages that are designed to collect an individual's online bank credit card, or other login information. The provisions to prosecute any person for phishing are given under section 66 C, 66 D and 74 of the IT Act with imprisonment up to 3 years or with fine up to 1 lakh rupees.

- **Cyber Stalking**

It can be defined as the use of electronic communications to harass or frighten someone, for example by sending threatening emails. The provisions are given under IT Act, 2008 under section 72 and section 354 C (voyeurism) of the Indian Penal Code. Also, section 67 provides imprisonment up to 3 years with fine.

MOTIVE OF CYBER CRIMES

Extortion as motive for cybercrime in India 2018 by leading state. ... The country recorded a total of over thousand cases of cyber-crimes motivated by extortion that year. These crimes came under the purview of numerous sections of the Indian Penal Code under Information Technology Act (Cyber-crimes).

DEFFINATION OF CYBER CRIME AND CRIMINAL

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may threaten a person, company or a nation's security and financial health.

Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

IMPACT OF CYBER CRIME IN CURRENT SENARIO

India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a poor track record of cyber security. According to Home Ministry statistics, as many as 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012. There have been 62,189 incidents of cyber frauds till June 2014. In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011. As per the cyber-crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012 and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012 and 2013, respectively. There has been an annual increase of more than 40 per cent in cyber-crime cases registered in the country during the past two-three years, Source-(http://ncrb.nic.in/) According National Crime Records Bureau (NCRB), a total of 288, 420, 966, 1,791 and 2,876 cyber-crime cases were registered under IT Act during 2008, 2009, 2010, 2011 and 2012, respectively. As per the information reported to and tracked by Indian Computer Response Team (CERT-In), a total number of 308, 371 and 78 government websites were hacked during the years 2011, 2012 and 2013 respectively and 16,035 incidents related to spam, malware infection and system break-in were reported in 2013.

HOW TO PROTECT A COMPUTER SYSTEM AGAINST THESE CYBER CRIME

1. **Use a full-service internet security suite**

For instance, Norton Security provides real-time protection against existing and emerging malware including ransomware and viruses, and helps protect your private and financial information when you go online.

2. **Use strong passwords**

Don’t repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.

3. **Keep your software updated**
This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.

4. **Manage your social media settings**
Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

5. **Strengthen your home network**
It's a good idea to start with a strong encryption password as well as a virtual private network. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data. It's a good idea to use a VPN whenever you a public Wi-Fi network, whether it's in a library, café, hotel, or airport.

6. **Talk to your children about the internet**
You can teach your kids about acceptable use of the internet without shutting down communication channels. Make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, or bullying.

7. **Keep up to date on major security breaches**
If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

8. **Take measures to help protect yourself against identity theft**
Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. How? You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal data. A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

9. **Know that identity theft can happen anywhere**
It's smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel's Wi-Fi network.

10. **Keep an eye on the kids**
Just like you'll want to talk to your kids about the internet, you'll also want to help protect them against identity theft. Identity thieves often target children because their Social Security number

and credit histories frequently represent a clean slate. You can help guard against identity theft by being careful when sharing your child's personal information. It's also smart to know what to look for that might suggest your child's identity has been compromised.

11. **Know what to do if you become a victim**

If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future. If you think cybercriminals have stolen your identity. These are among the steps you should consider.

1. Contact the companies and banks where you know fraud occurred.
2. Place fraud alerts and get your credit reports.
3. Report identity theft to the FTC.

12. What leads to the commission of cyber-crime?

There are 4 main causes which lead to the commission of cyber-crime.

Breach Because of Mobile Devices. In 2015, mobile devices had less than 1% infection rate, so they were considered safe. Now, more than three-fifths of IT security professionals report that it is either certain.

Embedding Malware Into Legitimate Applications

Cyber criminals have embedded malware into legitimate applications and they are targeting poorly secured Wi-Fi spots, stealing passwords, and more in their quest to steal information.

Exploiting Unauthorized Products

In many cases, attackers like to exploit unauthorized products having weak security controls in the corporate cloud.

Unlimited Internet Access

By using internet, we have given convenience in accessing without any limitations. This is the foremost factor which causes cyber-crime.

INFORMATION TECHNOLOGY ACT

Intellectual property (IP) is a legal concept which refers to creations of the mind for which exclusive rights are recognized. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyright, trademarks, patents, industrial design rights, trade dress, and in some jurisdictions trade secrets.

CYBER SECURITY

Computer security, cyber security[1] or information technology security (IT security) is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the

"Internet of things". Owing to its complexity, both in terms of politics and technology, cyber security is also one of the major challenges in the contemporary world.

DOCUMENT REQURID TO MAKE A CYBER COMPLEN

In Email related Complaints

- A written Complaint explaining the complete incidence
- Copy of the alleged Email
- Email should be taken from the original receiver. Copy of the forwarded email should be avoided
- Full Header of the alleged Email
- Copy of email and header should be in both hard & soft forms
- Soft copy should be given in a CD-R only

In Social Media related Complaints

- Copy/screenshot of alleged contents/profile
- Screenshot copy of URL of alleged contents
- Contents should be in both hard & soft forms
- Soft copy should be given in CD-R only

In Mobile Apps related complaints

- Screenshot of the malicious app and the location from where it downloaded.
- Bank statement from the victim's account if any transactions made.
- soft copy of all above mentioned documents in soft form

In Business Email Compromise complaints

Brief description of the incident, and consider providing the following financial information:

1. Originating Name
2. Originating Location
3. Originating Bank Name
4. Originating Bank Account Number
5. Recipient Name
6. Recipient Bank Name
7. Recipient Bank Account Number
8. Recipient Bank Location (if available)
9. Intermediary Bank Name (if available)
10. SWIFT Number
11. Date
12. Amount of Transaction
13. Additional Information (if available) - including "FFC"- For Further Credit; "FAV" – In Favor Of

In Data Theft complaints

- Copy of data which has been stolen
- Copyright certificate for the data in question.
- Details of suspected employee who took the data from company.
- Following documents related to suspected employee:
  1. Appointment letter

2. Non-disclosure agreement if any
3. List of duty assigned.
4. List of gadgets assigned to the suspected.
5. List of clients with whom the suspect is in touch.

- Proof of selling of your copyright data to any client.
- Devices used by the suspect while working with the company, if any.

In Ransomware complaints

- E-mail /phone number or any other means of communication through which ransom has been demanded.
- If malware was sent in the attachment of the mail. Screen shots of the mail with full header of first receiver should be provided.

In Net banking/ATM Complaints

- Bank statement from the concerned bank of last six months.
- Copy of SMSs received related to the alleged transactions.
- Copy of your ID proof and address proof as shown in the bank records.

In Fake call frauds

- Bank statement from the concerned bank of last six months.
- Make a copy of SMSs received related to the alleged transactions.
- Copy of your ID proof and address proof as shown in the bank records.

In Lottery scams Complaints

- Bank statement from the concerned bank of last six months.
- Make a copy of SMSs received related to the alleged transactions.
- Copy of your ID proof and address proof as shown in the bank records.

In Bitcoin related Complaints

- Complete facts in brief about the incident.
- Address of Bitcoin.
- Amount of Bitcoin involved.
- Address from/to whom purchase/sale of Bitcoins is done.

In Cheating related Complaints

- Print out of the alleged email along with its full header of the email
- Email should be taken from the original receiver. Copy of the forwarded email should be avoided
- Bank statement from the victim's account.
- Details of the alleged transaction made.
- Soft copy of all above mentioned documents.
- In Online Transactions related Complaints
- Bank statement from the concerned bank of last six months.
- Make a copy of SMSs received related to the alleged transactions.
- Copy of your ID proof and address proof as shown in the bank records.

CONLUSION

Though not all people are victims to cyber crimes, they are still at risk. Crimes done behind the computer are the 21st century's problem. With the technology increasing, criminals don't have to rob banks, nor do they have to be outside in order to commit any crime.

REFRENCES

1. http://www.legalserviceindia.com/legal/article-3042--types-of-cyber-crime-and-its-causes.html
2. India: Cyber security 2020, ICLJ.com(February 22, 2019), https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
3. Information Technology Act2000
4. Chandrima Khare, laws Punishing Cyber Stalking and Online Harassment, iPleaders.in (July 13, 2018), https://blog.ipleaders.in/cyber-stalking/
5. Abhinav Rana, Credit Card Fraud: Penal Provisions and Ways to Deal with it, iPleaders (February 21, 2020), https://blog.ipleaders.in/credit-card-fraud/
6. https://www.myadvo.in/blog/cyber-crime-in-india/
7. https://www.infosecawareness.in/cyber-laws-of-india
8. http://cyberlawindia.com/cyber-crime/