

CYBER CRIMES ARE ON THE RISE IN INDIA

Nidhi Majethia*

ABSTRACT

Cybercrimes are a serious concern in the present times and everyone in society has witnessed heinous attacks which has infringed on several laws and regulations for preventing cybercrimes as well as several sections of the Indian Penal Code; although the government has framed several initiatives and measures to curb these cybercrimes. India is a highly populated country with a large number of internet users cybercrime has become a serious threat due to the increasing number of cybercriminals. In the past few days, there have been multiple cases of cybercrimes including data leakage, and privacy violations, although a vast amount of private data of persons have been leaked, which is an infringement of their rights thus putting them in jeopardy. In the current scenario, there is no such protection provided to internet users as we can witness the rising cybercrime cases. However, this could be prevented if the government takes strict action against cybercriminals. This paper will focus on cybercrimes, types of cybercrimes, how to protect yourself from them, rapid growth, their impact, and laws governing cybercrimes. The author has also discussed the need for awareness of curbing cybercrime incidents.

Keywords: cybercrime, internet, privacy violations, serious threat.

INTRODUCTION

In today's modern era, every individual has become more and more reliant on the computers and internet. With the increasing use of such technologies, cybercrime has become a serious concern for society. The Internet has become a part of our day-to-day lives, including online classes, internet banking, online money transfer, online shopping, social media, online jobs¹, and so on. It has now become a basic need for everyone because no work could be done without the internet in today's era. No doubt the internet has given individuals access to everything from the comfort of their homes although there are many adverse effects of the internet. This digital world of technology has given rise to cybercrimes such as hacking, cyber stalking, phishing, spoofing, cyberbullying, online job fraud, online sextortion, data

*LLB, SECOND YEAR, RIZVI LAW COLLEGE, MUMBAI.

¹Mayuri Shukla, 'Overview of famous cybercrime cases that target people instead of money' (Ipleaders, 12 November 2021) <<https://blog.ipleaders.in/overview-of-famous-cyber-crime-cases-that-target-people-instead-of-money/>> accessed 13 April 2023

breaches, child pornography, sim swap scam, and so on. These crimes are increasing rapidly due to excessive internet use, which is also essential in the present times. However, a lot of people becomes the victims of such crime.

Cybercriminals may target the personal information of any person, business, bank, government, or financial institution. However, recently people are suffering lots of financial losses due to cybercrimes. These include Internet banking, ATM Debit Cards/Credit Cards, spyware, spam calls, etc. People are easily targeted and become victims of such crimes due to a lack of awareness regarding cyber crimes.

WHAT IS CYBER CRIME?

Cybercrime is an illegal activity that involves a computer or internet or any other similar device for the execution of a crime.²These cyber crimes are committed by individuals or organizations for the sake of profit which they gain after the commission of such crimes. These cybercriminals are highly technically skilled persons, they are well-versed in such technology and also know how to target people with little or no knowledge regarding such crimes. However, these people without knowledge are more vulnerable and easily fall victim to such cyber criminals. They also create fake accounts and rob people by stealing their money to generate profits. Cybercriminals are responsible for placing innocent lives in jeopardy. These crimes are increasing rapidly and are causing a serious menace to society.

TYPES OF CYBER CRIMES

1. Phishing

Phishing is a type of fraud in which hackers send malicious emails that contain unauthorized attachments or URLs to the users to get access to their accounts or computer. The purpose of this crime is to gain confidential information of users by duping them. These include stealing the sensitive information of the users such as ATM pin, Debit/Credit Card number, Bank account details, CVV number, OTP, etc through emails that seem to be from an authorized source.³

²Ibid

³Alex Andrews George, 'Cybercrime- Definition, Types and Reporting' (Clear IAS, 03 December 2021) <<https://www.clearias.com/cybercrime/>> accessed 13 April 2023

2. SIM Swap Scam

SIM Swap Scam takes place when fraudsters buy a new SIM and tries to activate it with the same number⁴through the phone's carrier operator by duping him, giving him false excuses that he has lost the older SIM card. Thereafter, when the activation is complete by duping that person to obtain the OTP, the fraudster has complete control over the victim's phone. From then on, all the calls and texts will be forwarded to the fraudster's phone and he will misuse it to rob the victim.

3. Cyber Stalking

Cyber Stalking is a crime where a person menaces the victim through online texts and emails, this creates fear in the victim's mind for his/her safety. This creates apprehension and can have a serious impact on the victim's mental health. Section 354D⁵of the Indian Penal Code, 1860 deals with the offense of stalking.

4. Identity Theft

In this type of theft, the cybercriminal steals the personal information including passwords, and credit card numbers, of the users to commit fraud by impersonating the actual user. This confidential information can be used for several illicit purposes without the consent of the users. Section 66C⁶of the Information Technology Act, of 2000⁷deals with the offense of identity theft.

5. DDoS Attacks

DDoS Attacks often referred to as Distributed denial-of-service aims at closing down online services or internet connections and making them unreachable by overloading the website with traffic affecting online networks and thus intervening in the services. Due to the overloading of the website, the system forces it to shut down or it may even cause the website to crash, thereby the services are inaccessible to legitimate users.

⁴ Divya Bhati, 'SIM swap frauds rising in India, How to protect your SIM by changing it to eSIM' (India Today, 19 January 2023) <<https://www.indiatoday.in/technology/features/story/sim-swap-frauds-rising-in-india-how-to-protect-your-sim-by-changing-it-to-esim-2323582-2023-01-19>> accessed 14 April 2023

⁵Indian Penal Code 1860, s 354D

⁶Information Technology Act 2000, s 66C

⁷ Information Technologu Act 2000

HOW TO PROTECT YOURSELF AGAINST CYBERCRIMES?

- Ensure your software is up to date
- Use strong passwords
- Make children aware of the internet and crimes related to it
- Secure yourself from identity theft
- Install anti-virus software
- Manage your social media settings

RAPID GROWTH OF CYBER CRIMES AND ITS IMPACT

India is the most adversely affected country in the whole world when we talk about cyber fraud, with nearly 31 percent of the victims losing money. People fall victim to these cyber criminals who dupe them to make a profit. Every day we see lots of people who lose their money by tapping on some links or fraudsters trying to obtain the personal details of the victim by tricking them.

The most recent cyber scam occurred in Gujarat where a couple lost a shocking amount of Rs. 1.12 crore and fell victim to a cyber scam. The couple fell for the enticement of earning money after fraudsters told them that their job would be to watch and give ratings for movies. They were introduced to this conspiracy via a Telegram group. They had received a message in the group, “You can earn by sitting at home in your comfort, all you have to do is give ratings to movies”⁸. The couples were assured a daily income of Rs. 2,500 to Rs. 5,000. The couple fell into this trap and they went on spending their hard-earned money. After this the situation turned more adverse and the fraudsters began to coerce the woman if she tried to withdraw a huge amount of money the fraudsters would menace to file a money laundering⁹ case against her. However, the officials are still investigating to find the culprit behind the intricate scam.

Due to these crimes, the women in our society are falling victim to crimes such as blackmailing, cyberpornography, sextortion, cyberbullying, defamation¹⁰, cyberstalking¹¹,

⁸ LingamguntaNirmitha Rao, ‘Gujarat couple falls prey to cyber fraud, lose over ₹1 crore: Report’ (Hindustan Times, 01 April 2023) <<https://www.hindustantimes.com/technology/gujarat-couple-fall-prey-to-cyber-fraud-lose-over-rs-1-crore-report-101680340206485.html>> accessed 14 April 2023

⁹ Ibid

¹⁰ Indian Penal Code 1860, s 499

¹¹ Indian Penal Code 1860, s 354D

posting obscene¹² sexual content, and creating fake profiles these are the most habitual crimes committed against women and placing their lives in jeopardy. As a consequence of this, women are facing hindrances like anxiety, panic, apprehension, and frustration which mentally affect women.

In a recent case where a twenty-six-year-old widow from Nagpur, Maharashtra fell prey to sextortion¹³ and cyber fraud after a fraudster duped her in the guise of love and affection. A woman was working for a private firm, she received a friend request on Facebook on 22nd March. The woman accepted his friend request, and the fraudster called her and addressed himself as Rahul Khanna from a UK marriage bureau. On the 25th of March, the fraudster enticed her emotionally by expressing his feelings for her and stating that he had started loving her and impelled her to undress. The man even recorded her nude video during the WhatsApp call. Thereafter, he enticed the widow by saying that he was sending two lakh US dollars and some diamonds. Subsequently, she received a call from a delivery boy who asked her for cash as government duty charges for handing over the gifts and jewelry. She was made to pay up Rs. 1.5 lakh. Thereafter, the fraudster started asking for more money by menacing to make her nude recordings viral on social media platforms. The widow was frustrated by frequent threatening calls from the fraudster and she tried to end her life. However, the police have lodged an offense against the fraudster and also her in-laws who were also a part of this crime and had shared the victim's obscene photographs with others.

THE IMMENSITY OF CYBERCRIME CASES ARISING IN INDIA

India is the second largest market across the globe with over 692 million internet users in January 2023. And it is expected to have over 900 million internet users in India by 2025. Due to the emerging use of the internet and new technologies, the market is expected to boost rapidly. No doubt the internet is making human lives better and easier but what about the growing concern regarding cyber security? According to Mumbai Crime Report the registration of cyber offenses, including online fraud under the guise of offering jobs, luring for money by providing jobs, insurance, investment, online shopping, etc. Furthermore,

¹² Information Technology Act 2000, s 67

¹³ Soumitra Bose, 'Sextortionist targets 26-year-old widow, extorts ₹1.5 lakh' (Times of India, 05 April 2023) <<https://timesofindia.indiatimes.com/city/nagpur/sextortionist-targets-26-year-old-widow-extorts-1-5-lakh/articleshow/99254618.cms>> accessed 15 April 2023

Mumbai observed a 70 percent rise in cybercrime¹⁴ cases in 2022 compared to the last year. At least 4,286 cybercrime incidents were reported in Mumbai over one year till November 2022, the deputy chief minister said.

Besides this, almost Rs. 1 crore was robbed every day by cyber fraudsters¹⁵ from individuals in Karnataka, in the year 2022. Karnataka lost a staggering sum of Rs. 363 crores in 2022, and since 2019 the fraudsters have arranged to siphon away Rs. 722 crores.

This clearly shows that cyber crimes are on the rise and fraudsters are looting innocent people who have little or no knowledge or awareness regarding such crimes.

LAWS REGULATING CYBERCRIMES IN INDIA

- Information Technology Act, 2000¹⁶: Indian cyber laws are regulated by Information Technology Act¹⁷, which was enacted in 2000. The main objective of this act is to provide legal authorization for electronic commerce and electronic transactions by making it secure and safe to register real-time records with the government and also to prevent cybercrimes.
- Indian Penal Code, 1860¹⁸: Identity theft and related cyber offenses are included in Indian Penal Code (IPC) 1860¹⁹, along with the Information Technology Act, of 2000.²⁰

The primary pertinent section of the IPC covers cyber frauds:

- Forgery (Section 464)²¹
- Fraudulently or dishonestly presenting a forged document as genuine (Section 471)²²
- Harming reputation (Section 469)²³
- False documentation (Section 465)²⁴

¹⁴Mumbai saw 70 pc rise in cybercrime cases in 2022: Devendra Fadnavis, (The Economic Times, 03 March 2023) <<https://economictimes.indiatimes.com/news/mumbai-news/mumbai-saw-70-pc-rise-in-cyber-crime-cases-in-2022-devendra-fadnavis/articleshow/98391667.cms>>accessed 15 April 2023

¹⁵Karnataka lost nearly Rs 1 crore every day to cybercrimes in 2022: Home Department, (The Indian Express, 23 February 2023) <<https://indianexpress.com/article/cities/bangalore/karnataka-lost-nearly-rs-1-crore-every-day-cybercrimes-2022-home-department-8461897/>>accessed 15 April 2023

¹⁶Information Technology Act 2000

¹⁷ Ibid

¹⁸Indian Penal Code 1860

¹⁹Ibid

²⁰Ibid

²¹Indian Penal Code 1860, s 464

²²Indian Penal Code 1860, s 471

²³Indian Penal Code 1860, s 469

- Forgery pre-planned for cheating (Section 468)²⁵

CONCLUSION

As we are aware that in the present day, the internet and computer have become our fundamental requirements but with the evolution of technology cybercrime incidents are arising day by day across the world. The Internet has become a device for wicked acts that are abused by professional criminals for evil causes and at times for monetary gain. Thus, it has become important for every citizen to be aware and not fall into such traps, however, at this moment cyber laws come into play which is essential for every individual. Countries all over are shifting toward digitalization and now at this moment cyber laws and security need to be more rigid. With the increasing technology, cybercriminals don't have to loot banks, nor do they have to be outside their homes to commit a crime. They can simply commit a crime and make profits sitting at their homes. Their weapons aren't pistols or guns anymore, they just need to have in-depth knowledge of the internet and computer.

Therefore, we need greater training facilities and awareness for curbing cyber cases so that we can secure our information, data, and devices by ourselves by taking these preventive measures. In India, the Information Technology Act was initiated to restrain the cybercrime cases which were arising at that time but these laws need to be amended and modified frequently which would help in developing an apprehension among cybercriminals in a consequence of this the cybercrime rate would decline gradually.

To tackle this problem awareness among people regarding cybercrimes should be initiated. Government should make strict laws regarding cybercrimes to create fear in the fraudster's minds so that they would not commit such crimes.

²⁴ Indian Penal Code 1860,s 465

²⁵ Indian Penal Code 1860,s468