



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## RISE OF CYBER CRIMES IN INDIA AND THE LEGAL REMEDIES AVAILABLE TO VICTIMS

*Adesh Kumar Srivastav*

### Introduction

India is on the verge of becoming a digital society. Technology has become a part and parcel of daily life from online banking to UPI payment to social media platforms to e-commerce websites. Implemented digital revolution has contributed to an increase in cybercrimes in the country because communicating and conducting financial transactions are easier than ever before.

Cybercrimes including online fraud, hacking, stalking, identity theft and phishing are prevalent today. There are some people, especially students and senior citizens, who are susceptible to being targeted just because they do not know what to do when using the Internet. In the present context of a fast-growing internet service scenario, there has been a significant surge in complaints of cybercrime in India according to recent government reports<sup>1</sup> and awareness about cyber-crimes and its legal recourse to the affected individuals has come to the fore.

### Reasons Behind the Rise of Cyber Crimes

One of the major reasons behind the increase in cybercrimes is the rapid growth of digital technology in India. The advent and emergence of such systems and policies of government like '*Digital India*' have greatly enhanced the convenience of conducting online transactions

---

<sup>1</sup> Press Information Bureau, *Rise in Cyber Crime Cases in India*, GOV'T OF INDIA, <https://pib.gov.in>.

and using the internet even in rural areas <sup>2</sup>but, at the same time, placed more opportunities in the hands of the cybercriminals.

This is followed by the lack of cybersecurity awareness among Internet users. A common method by which many people are unwittingly subjected to the risks involves them providing OTPs, clicking on suspicious links, or downloading unknown applications unbeknownst. The lack of awareness makes it an easy place for cybercriminals to stage financial crimes and steal identities.

Online banking and UPI payments have also been getting more popular and hence have added to the cybercrimes. Fake numbers are commonly used by fraudsters to trick users into sending money from their customer care services, which are often a part of QR code scams or even fake payment links.

Recently, there was a trend in India of “digital arrest scams” done by cyber criminals posing as police officers/officials via video calls to threaten victims with fake arrest/sentencing. Many people tend to give significant sums of cash to fraudsters out of worry. A number of these have been reported over various states, particularly targeting the elderly or financially vulnerable individuals.

## **Legal Remedies Available to Victims**

To address cybercrime and ensure the safety of victims, India has enacted specific laws or regulatory frameworks. *The Information Technology Act 2000*<sup>3</sup> is the primary legislation that deals with cyber offences. The Act acknowledges electronic records and digital transactions and offers punishment for several cyber offences.

Some important provisions under the Act include:

- **§ 66C – Punishment for identity theft<sup>4</sup>**
- **§ 66D – Punishment for cheating through online impersonation<sup>5</sup>**

---

<sup>2</sup> Digital India Programme, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, <https://www.digitalindia.gov.in>.

<sup>3</sup> Information Technology Act, 2000 India

<sup>4</sup> Information Technology Act, 2000, section 66C (India)

<sup>5</sup> Information Technology Act, 2000, section 66D (India)

- **§ 67 – Punishment for publishing obscene material online<sup>6</sup>**

Victims can also seek remedies under relevant provisions of the Indian Penal Code in cases involving fraud, cheating, criminal intimidation, and harassment.<sup>7</sup>

The Government of India has set up the National Cyber Crime Reporting Portal for reporting online offences.<sup>8</sup>

Users may report incidents of financial fraud, cyberbullying, ID theft and crimes against women and children that involve financial loss through this platform. If someone feels they are the victim of financial fraud linked to the Internet, they can also contact the national helpline number 1930 for immediate assistance.

Nowadays some states in India have cybercrime police stations and cyber cells in place which are dedicated for investigating cases involving cybercrime and online fraud. These institutions can contribute significantly to the enhancement of cyber security and justice for victims.

## **Preventive Measures Against Cyber Crimes**

While legislation is there to protect against cybercrime, prevention is also crucial. Everyone needs to learn how to use the Internet and electronic communications safely to minimize cyber risks to keep personal information safe.

Some useful guidelines are to:

- Do not provide OTPs/passwords to anyone
- Use secure passwords and 2 factor authentication to secure your accounts.
- Double-check links before using the internet to make payments
- Do not download applications that you don't know.
- Keep security software up-to-date and change passwords regularly.
- Report any suspicious activity as soon as it is noticed

There are steps that can be taken that can decrease the likelihood of getting scammed online.

---

<sup>6</sup> *Information Technology Act, 2000, section 67 (India)*

<sup>7</sup> *Indian Penal code, 1860 sections 415 , 419, 503*

<sup>8</sup> *National Cyber Crime Reporting Portal, MINISTRY OF HOME AFFAIRS, <https://cybercrime.gov.in>.*

## **Conclusion**

Cybercrime has been one of the major issues faced during the digital era in India. Cyber scammers are adopting sophisticated tactics as the reliance on technology grows in the world. Millions of people are a common target of various financial frauds, ID theft, phishing and online harassment.

Though the Government of India has enacted legal regulations under Information Technology Act, 2000 and several reporting platforms for cybercrime, there is a need to raise awareness regarding the internet and the internet's usage amongst masses while cultivating a responsible attitude to use the internet. Creating a safe digital environment requires citizens to be careful, educated, and assertive in their interactions in the digital world.

In today's technology driven world cybersecurity is not solely the responsibility of the government or law enforcement agencies. It is a shared responsibility of every internet user.