# Understanding Cybercrime: Key Definitions and Classifications

**Authors: Krishna CV Grandhi, Chandra Lekha**

Cybercrime is defined as any criminal behaviour that employs a computer or the internet to commit the crime. It can encompass everything from online fraud and identity theft to cyberstalking and hacking.

The Information Technology Act of 2000, the IT Amendment Act of 2008, and other Indian legislations do not define cybercrime specifically. However, the Indian Penal Code, 1860, and several other pieces of legislation address offences and crimes that may be committed both online and through traditional offline means in great detail. As a result, cybercrime may be defined as any offence or crime that involves the use of a computer.

Interestingly, even a minor offense like stealing or pickpocketing can fall under the broader purview of cybercrime if the basic data used to commit such offense involves a computer or information stored in a computer that is used (or misused) by the fraudster.

In cybercrime, a computer or data can either be:

- The target or object of the offence.
- A tool for committing another offence, providing necessary inputs for that offence.

All such criminal acts and related acts fall under the broad definition of a cybercrime.

**Types of Cybercrimes**

Cybercrimes may be classified into three categories:

1. Crimes Against Individuals
   - Cyberstalking
   - Cyber bullying
   - Identity theft

2. Crimes Against Property
   - Hacking
   - Virus or malware attacks

3. Crimes Against Society
   - Cyber terrorism
   - Spread of illegal or harmful information online

## Common Cyber Attacks

1. **Hacking**: Hacking is the act of gaining unauthorised access to a network or computer with the goal of damaging it or obtaining confidential data. Such acts are committed by hackers i.e., individuals who use computers, networks or other skills to gain unauthorised access to systems or networks for illegal or unethical purposes.

   *Types of Hackers:*

   White Hat Hacker: A white hat hacker is a person who works for a company to find security flaws and fix them before a security breach happens. They take proactive steps to identify vulnerabilities and support the maintenance of services and data security.

   Black Hat Hacker: A black hat hacker is a person who attempts to enter security networks or websites without authorisation and with malevolent intent. They may be motivated by thrill-seeking, protest, or cyber espionage, but their main objective is typically financial and personal gain.

   Grey Hat Hacker: A hacker that combines black hat and white hat techniques is known as a "grey hat hacker." They reveal all weaknesses and vulnerabilities to law enforcement or intelligence organisations by using networks and computer systems like black hats, but without malevolent intent.

2. **Phishing**: Phishing is the deceptive practice of posing as a reliable organisation in order to obtain private data, including credit card numbers and passwords.
3. **Online Fraud**: Online fraud includes a variety of schemes, such as investment fraud, advance fee fraud, and auction fraud carried out to defraud or take advantage of victims.
4. **Identity Theft**: Identity theft is the theft of a person's personal data in order to perpetrate fraud or other crimes.
5. **Cyberstalking**: Cyberstalking is the threatening or harassing of a person online or through other digital means to incur fear or concern about their safety. It is an invasion of a person's privacy, and manifests in repeated actions over a period of time.
6. **Phishing Scams**: Phishing scams are fraudulent mails that deceive consumers into divulging personal information or login credentials.
7. **Malware Infections**: Malicious software that compromises, interferes with, or eavesdrops on digital systems without the consent of its user, is known as a

malware infection. Such harmful software may vary from viruses, spyware and ransomware.

8. **Ransomware Attacks**: A ransomware attack holds a user's data hostage, locking them out of their system until a certain ransom amount is paid to the hacker.
9. **Distributed Denial of Service (DDoS) Incidents**: It is a cybercrime in which the attacker floods a server with internet traffic thereby preventing the user from accessing online services.

## CYBER CRIME RELATED TO SOCIAL MEDIA

A significant number of people use social networking sites and post images, videos, and comments. However, since personal information can be hacked and misused, most users are unaware of the risks associated with excessive usage of such social networking websites. Some of the common social media offences are:

**(i) Cyber Bullying & Trolling**: While not recognized as statutory crimes, these activities often involve the use of technology or social media to threaten, harass embarrass or target another individual. Such actions may still be prosecuted under criminal laws.

**(ii) Buying Illegal Items**: While conducting legitimate business through social media is legal, connecting with individuals to buy drugs or other regulated, controlled, or banned products is illegal.

**(iii) Vacation Robberies**: Burglars use social media to discover when potential victims are on vacation by monitoring publicly viewable status updates.

**(iv) Creation of Fake Profiles**: Attackers may create fake profiles using publicly available information of an induvial and post offensive content, including morphed photographs and unauthorised status updates.

**(v) Fake Online Friendships**: Fake online friendships involve developing online relationships without real-life familiarity and exploiting emotional connections to transfer money under false pretences.

**(vi) Image and Video Morphing**: It is a form of digital sexual violence wherein photos or videos are morphed and upload online, often to pornographic websites. Such crimes have become more prominent with sophisticated AI capabilities.

**(vii) Deep Fake**: Deep fake is an artificial intelligence that produces realistic-looking phoney photos, films, and audio recordings. Combining the words "deep learning" with "fake," the term frequently refers to replacing one person with another or producing completely bogus content.

## CYBERCRIME STATISTICS IN INDIA

India has seen a record spike in cybercrimes in 2024:

• Average number of complaints per day: 7,000;

• Growth over prior years: 60.9% higher than 2022-2023 and 113.7% higher than 2021-2023

About 740,000 cybercrime incidents were reported on the cybercrime.gov.in during the first four months of 2024 and by September of the same year, there were 1.2 million cases reported with victims losing more than ₹120 crores.

Despite the sharp rice, conviction rates for cybercrime remain staggeringly low. Only 2,706 (1.6%) of the 167,000 cases that were filed between 2020 and 2022 resulted in convictions.

Between 2021-2022, there has also been a 32% rise in crimes against children and a 4% rise in crimes against women. As per reports, more than 19,000 cases were recorded in 2022 involving sexual abuse and exploitation. These statistics highlight the urgent need for effective legislative amendments within the evolving digital landscape.

www.csail.org