



## Cyber Crime

**For Prelims:** [Cyber Crime](#), [Seventh Schedule of the Constitution](#), [Internet of Things](#), [Crypto-Currency](#), [Massive Open Online Courses](#).

**For Mains:** Cyber Crime, Related Challenges and Measures to Deal with it.

**Source:** [PIB](#)

### Why in News?

The Indian government has taken significant steps to strengthen the mechanism for dealing with [Cybercrimes](#) in a comprehensive and coordinated manner.

What is Cyber Crime?

#### ▪ About:

- Cybercrime is defined as a crime where a **computer is the object of the crime or is used as a tool** to commit an offense.
  - Cybercrimes fall under State subjects as per the [Seventh Schedule of the Constitution](#) of India.
- It involves illegal or unauthorized activities that **exploit technology to commit various forms of crimes**.
- Cybercrime covers a wide range of offenses and can affect individuals, organizations, and even governments.

#### ▪ Types:

- **Distributed Denial-of-Service (DDoS) Attacks:** These are used to make an **online service unavailable** and take the network down by overwhelming the site with traffic from a variety of sources.
- **Botnets:** Botnets are networks from **compromised computers that are controlled externally by remote hackers**. The remote hackers then send spam or attack other computers through these botnets.
- **Identity Theft:** This cybercrime occurs when a criminal gains access to a **user's personal information or confidential information** and then tries to tarnish reputation or seek a ransom.
- **Cyberstalking:** This kind of cybercrime involves **online harassment where the user is subjected to a plethora of online messages** and emails. Typically, cyberstalks use social media, websites, and search engines to intimidate a user and instill fear.
- **Phishing:** It is a type of **social engineering attack often** used to steal user data, including login credentials and credit card numbers. It occurs when an **attacker, masquerading as a trusted entity**, dupes a victim into opening an email, instant message, or text message.

### What are the Challenges Related to Cyber Security in India?

- **Profit-Friendly Infrastructure Mindset:**
  - Post liberalisation, the Information Technology (IT), [electricity](#) and [telecom sector](#) have witnessed **large investments** by the private sector.
  - Operators are not investing in protective infrastructure, **rather they are focused on the profitable infrastructure only**, because they think **investment on cyber-attack preparedness** may not generate good profits.
  - All operators are focused on profits, and do not **want to invest in infrastructure that will not generate profits (i.e. protective infrastructure)**.
- **Absence of Separate Procedural Code:**
  - There is no separate procedural code for the **investigation of cyber** or computer-related offences.
- **Trans-National Nature of Cyber Attacks:**
  - Most cybercrimes are **trans-national in nature**. The collection of evidence from foreign territories is not only a difficult but also a tardy process.
- **Expanding Digital Ecosystem:**
  - In the last couple of years, India has traversed on the path of digitalizing its **various economic factors** and has carved a niche for itself successfully.
  - The latest technologies like [5G](#) and [Internet of Things \(IoT\)](#) will increase the coverage of the internet-connected ecosystem.
  - With the advent of digitalisation, paramount consumer and citizen data will be stored in digital format and transactions are **likely to be carried out online which makes India a breeding ground** for potential hackers and cyber-criminals.
- **Limited Expertise and Authority:**
  - Offenses related to [crypto-currency](#) remain **under-reported** as the capacity to solve such crimes remains limited.
  - Although most State cyber labs are capable of analysing hard disks and mobile phones, **they are yet to be recognized as 'Examiners of Electronic Evidence'** (by the central government). Until then, they cannot provide expert opinions on electronic data.

## What Measures Can be Taken to Tackle Cyber Crimes in India?

- **Cybersecurity Awareness Campaign:**
  - The governments at various levels need to conduct massive cybersecurity awareness campaigns, regarding **Cyber frauds**, use strong, unique passwords, **being careful using public wi-fi, etc.**
- **Cyber Insurance:**
  - Develop cyber insurance policies that are **tailored to the specific needs of different businesses** and industries. Customized policies will help ensure that organizations have coverage for the **most relevant cyber risks they face**.
    - **Cyber insurance** provides financial coverage against losses resulting from cyber incidents and by **mitigating the financial impact** of these incidents, organizations can **recover more quickly and continue their operations**.
- **Data Protection Law:**
  - Data is referred to as the new currency, thus is a requirement for **a stringent data protection regime** in India.
    - In this context, the [European Union's General Data Protection Regulation](#) and India's Personal Data Protection Bill, 2019 are steps in the right direction.
- **Collaborative Trigger Mechanism:**
  - For a country like India where the **citizenry is more vulnerable** to cybercrime, there is an urgent need for a collaborative trigger mechanism.
    - This mechanism would bind all parties and enable law enforcers to act quickly and safeguard citizens and businesses from a fast-growing menace.
    - In this context, the Indian **Cyber Crime Coordination Centre will assist in centralizing cybersecurity investigations**, prioritize the development of response tools and bring together private companies to contain the menace.

## What are the Government Initiatives to Cope with Cyber Crimes in India?

- **Indian Cyber Crime Coordination Centre (I4C):** This center coordinates efforts to tackle all

types of cyber-crimes across the country.

- **National Cyber Forensic Laboratory:** It provides early-stage cyber forensic assistance to Investigating Officers of all State/UT Police through both online and offline modes.
- **CyTrain Portal:** A [Massive Open Online Courses \(MOOC\)](#) platform for capacity building of police officers, judicial officers, and prosecutors through online courses on critical aspects of cyber-crime investigation, forensics, and prosecution.
- **National Cyber Crime Reporting Portal:** A platform where the public can report incidents of cyber-crimes, with a special focus on **crimes against women and children.**
- **Citizen Financial Cyber Fraud Reporting and Management System:** It is a **system for immediate reporting of financial frauds** and assistance in lodging online cyber complaints through a toll-free helpline.
- **Cybercrime Prevention against Women and Children (CCPWC) Scheme:** Financial assistance provided to States/UTs for **developing capabilities of Law Enforcement Agencies** in investigating cyber-crimes.
- **Joint Cyber Coordination Teams:** Constituted to enhance coordination among Law Enforcement Agencies of States/UTs, particularly in areas with multi-jurisdictional issues related to cyber-crimes.
- **Central Assistance for Modernization of Police:** Providing financial support to States/UTs for acquiring **modern weaponry, advanced communication/forensic** equipment, and cyber policing equipment.

## Conclusion

- It is of critical importance to ensure global cooperation through information sharing and strengthening joint efforts in cybersecurity research and development as most cyberattacks originate from beyond the borders.
- It is important for the corporates or the **respective government departments to find the gaps in their organisations** and address those gaps and create a layered security system, wherein security threat intelligence sharing is happening between different layers.