

Cybercrime: Notes for UPSC GS-III

Cybercrime, is a crime that involves a computer and a network. The computer may have been used to commit the crime and in any cases it is also the target. Cybercrime may threaten a person or a nation's security and financial health.

Cybercrime is a topic featured in the GS-III section of the UPSC Exams. Candidates attempting the exam will find the details given in the article to be of immense use.

Definition of Cybercrime

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".

Why is Cybercrime considered a grave offence?

There are many privacy concerns surrounding cybercrime when sensitive information is intercepted and leaked to the public, legally or otherwise. Some of those information may include data about military deployments, internal government communications and even private data about high-value individuals . Cybercrime is not confined to individuals alone.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state is sometimes referred to as cyberwarfare.

In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, a leading cybersecurity firm concludes that close to \$600 billion, nearly one percent of global GDP, is lost to cybercrime each year.

Laws against Cybercrime in India?

Ever since the introduction of cyber laws in India, the Information Technology Act (IT Act) 2000 covers different types of crimes under cyber law in India. The following types of cybercrime are covered under the IT Act 2000.

- **Identity theft** - When personal information of a person is stolen with the purpose of using their financial resources or to take a loan or credit card in their name then such a crime is known as Identity theft.

- **Cyberterrorism** - When a threat of extortion or any kind of harm is being subjected towards a person, organization, group or state, it is known as the crime of Cyber Terrorism. Generally, it includes the well-planned attack strategies on the Government and corporate computer system.
- **Cyberbullying** - When a teenager or adolescent harasses, defames, or intimidates someone with the use of the internet, phone, chat rooms, instant messaging or any other social network then the person is said to be committing the crime of Cyberbullying. When the same crime is done by adults it is known as Cyberstalking.
- **Hacking** - The most common cybercrime is Hacking. In this crime, the person gets access to other people's computers and passwords to use it for their own wrongful gain.
- **Defamation** - While every individual has his or her right to speech on internet platforms as well, but if their statements cross a line and harm the reputation of any individual or organization, then they can be charged with the Defamation Law.
- **Copyright** - With the massive surge in internet users, when the data/ information is distributed on all platforms, copyrighting your work aids you to restrict the use of your work. Any use of your copyrighted without your permission is a punishable offence.
- **Trade Secrets** - Internet organization spends a lot of their time and money in developing softwares, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offence.
- **Freedom of Speech** - When it comes to the internet, there is a very thin line between freedom of speech and being a cyber-offender. As freedom of speech enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web.
- **Harassment and Stalking** - Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offence.

IT Act, 2000 went through amendments under the Indian Penal Code in the year 2008. These were made in light of the laws on cybercrime - IT Act, 2000 by way of the IT Act, 2008. They were enforced at the beginning of 2009 to strengthen the cybersecurity laws.