

UNIT - I: Introduction to Cybercrime: Introduction, Cybercrime: Definition and origins of the word, Cybercrime and Information Security, who are cyber criminals? Classifications of cybercrimes, cybercrime: the legal perspectives, an Indian perspective, cybercrime and the Indian IT Act 2000, a Global perspective on Cybercrimes.

Introduction to Cybercrime

What is Cybercrime?

Cybercrime means any illegal activity in which a **computer, computer network, smartphone, or digital system** is used as a tool, target, or both.

Role of technology	Meaning	Example
Computer as a tool	Technology is used to commit a crime.	Sending a fake scholarship message to steal money.
Computer as a target	A system or its data is attacked.	Installing ransomware on a college server.
Both tool and target	An attacker uses a computer to attack another system.	Using an attacker's device to steal records from a college database.

Cybercrime = Crime committed using digital technology or against digital systems

Common examples of cybercrime

Cybercrime	What happens?	Example
Phishing	Fake messages are used to steal information	Fake bank email
Hacking	Unauthorized access to a computer/system	Attacker breaks into a server
Identity theft	Someone uses another person's identity	Using stolen PAN/Aadhaar details
Online banking fraud	Money is stolen through digital methods	Fake banking link
Ransomware	Files are encrypted and ransom is demanded	Hospital computers locked
Cyberbullying	Technology is used to harass someone	Threatening messages on social media
Data theft	Confidential information is stolen	Customer database stolen
DDoS attack	A service is overloaded with traffic	Website becomes unavailable

Origin of the Word "Cybercrime"

The word **cybercrime** is made from two parts:

Cyber + Crime

Cyber

The word **cyber** is derived from **cybernetics**, a term associated with the study of **control and communication in machines and living systems**.

The term *cybernetics* was popularized by mathematician **Norbert Wiener** in his work on communication and control systems.

Over time, **cyber** became associated with:

- Computers
- Computer networks
- Internet
- Digital communication
- Virtual environments

Crime

Crime means an act that violates a law and is punishable by the government.

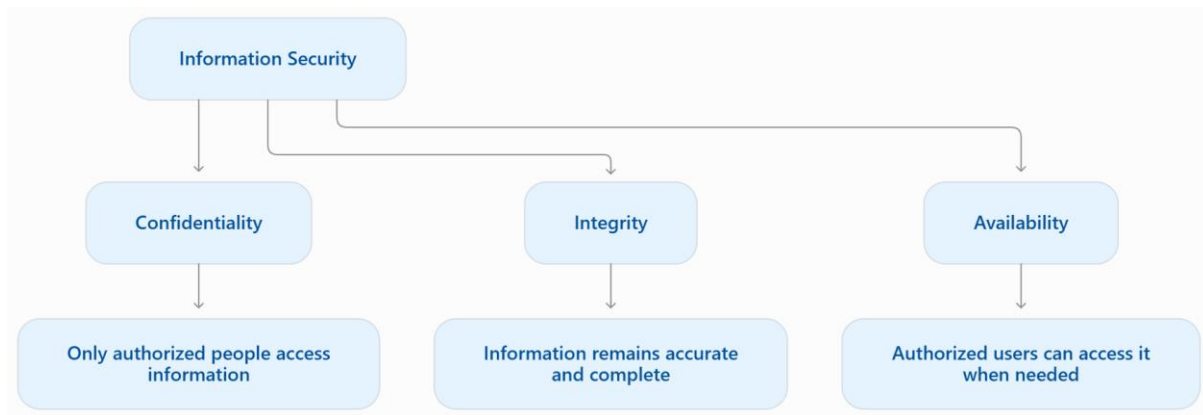
Cybercrime and Information Security

What is Information Security?

Information Security (InfoSec) is the practice of protecting information and information systems from:

- Unauthorized access
- Unauthorized modification
- Unauthorized disclosure
- Destruction
- Disruption

The three fundamental objectives of information security are called the **CIA**



Cybercrime vs Information Security

Cybercrime

Concerned with illegal activities
 Attacks systems/data
 Usually performed by attackers
 Examples: hacking, phishing, ransomware
 Causes loss or damage
 Exploits vulnerabilities

Information Security

Concerned with protecting information
 Defends systems/data
 Implemented by security professionals/organizations
 Examples: encryption, authentication, firewalls
 Attempts to prevent or reduce loss
 Identifies and protects vulnerabilities

Cybercrime involved

Examples:

Phishing Bank Fraud

Social Media Account Theft

Ransomware in a Hospital

Relationship between Cybercrime, Cybersecurity, and Information Security

Aspect	Cybercrime	Cybersecurity	Information security
Main concern	Criminal activity involving digital technology.	Protection of digital systems, networks, and data.	Protection of information in all forms.
Example	Stealing a college portal password.	Detecting and blocking suspicious login attempts.	Protecting both digital marks and printed question papers.

Who are cyber criminals?

Cybercriminals are individuals or groups who use computers, mobile devices, networks, or the internet to commit crimes. They may steal money or information, cheat people, threaten victims, or damage digital systems.

For example, a person who creates a fake scholarship website to collect students' banking details and steal money is a **cybercriminal**.

Common Types of Cybercriminals

Type	What they do	Example
Unauthorized attackers	Enter systems without permission to steal, alter, or destroy information.	An attacker accesses a college database and changes examination marks.
Online fraudsters	Deceive people to obtain money.	A person advertises a fake job and collects an "application fee."
Phishers	Use fake messages or websites to steal sensitive information.	A fake bank email asks a customer to enter their password on a fraudulent website.
Identity thieves	Misuse another person's identity or personal details.	A criminal uses stolen identity documents to impersonate someone.
Malware creators and distributors	Develop or spread harmful software.	A person distributes a fake application that secretly steals passwords.
Ransomware criminals	Block access to systems or data and demand payment.	A group encrypts a company's files and demands money to restore access.
Cyberstalkers	Use digital platforms to repeatedly monitor, threaten, or harass someone.	A person repeatedly sends threatening messages through different accounts.
Malicious insiders	Misuse legitimate access within an organization.	An employee deliberately steals confidential customer records and sells them.
Organized cybercrime groups	Coordinate criminal activities, often with different members performing different roles.	One member steals passwords, another accesses accounts, and another handles stolen money.

Example: A Fake Scholarship Scam

Classifications of Cybercrimes

Cybercrimes can be classified in different ways. These categories overlap: one attack may harm an individual, an organization, and its information simultaneously.

Cybercrime: The Legal Perspective means examining unlawful activities involving computers, digital devices, or the internet **according to the law**. It considers what offence occurred, which law applies, what evidence is required, and what legal action may follow.

Example: A person creates a fake bank website, pretends to represent the bank, and tricks a customer into transferring money.

From the legal perspective:

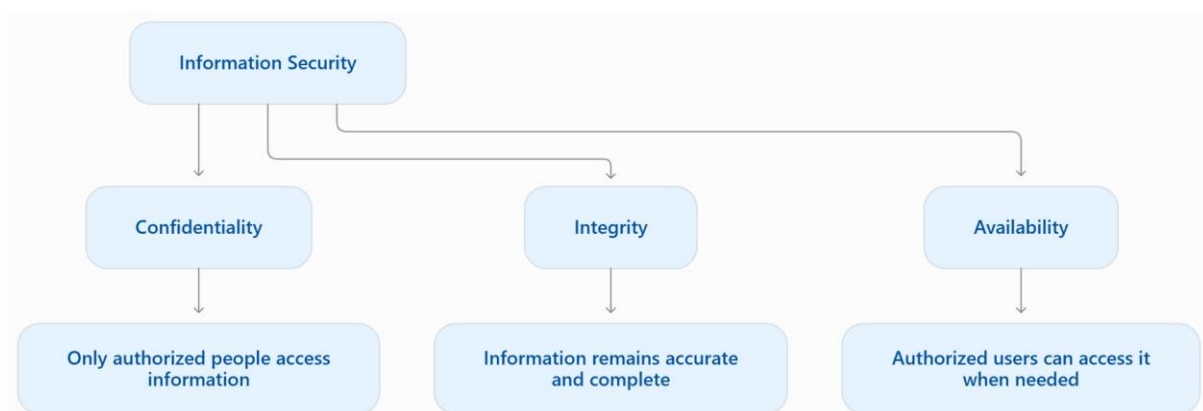
- **Offence:** Cheating by impersonating the bank online.
- **Applicable law:** In India, **Section 66D of the Information Technology Act, 2000** may apply.
- **Evidence:** Fake website details, messages, payment records, and device records.
- **Legal action:** The offender may be investigated and prosecuted when the required legal elements are established.

Cybercrime: An Indian Perspective means understanding crimes involving computers, mobile devices, or the internet **in the Indian context**, including their effects on people and organizations and how Indian laws and authorities address them.

Example: A fraudster creates a fake scholarship website resembling an Indian government portal and collects “processing fees” from students. This is online fraud. Cheating by impersonation through a computer resource may attract **Section 66D of the Information Technology Act, 2000**, depending on the facts.

A Global Perspective on Cybercrimes

Cybercrime frequently crosses national borders. The criminal may operate in one country, use a server in another, and target victims elsewhere.



Example: An Indian student pays a fake overseas internship agency. Investigators may need payment records from an Indian bank, account information from a foreign platform, and assistance from authorities where the offender operates.

Cybercrime and the Indian IT Act, 2000

The **Information Technology Act, 2000** is a foundational Indian law for electronic transactions and computer-related offences. It also recognizes electronic records and electronic signatures. It was substantially amended through the **Information Technology (Amendment) Act, 2008**, whose major provisions took effect in 2009. Thus, several familiar cybercrime provisions were later additions to the original Act.

Section	Main subject	Simple example
43	Compensation for specified unauthorized acts affecting computers or data.	Copying a database without permission.
65	Tampering with computer source documents required by law to be maintained.	Knowingly destroying legally required source code.
66	Section 43 acts committed dishonestly or fraudulently.	Deliberately deleting records to cause wrongful loss.
66B	Dishonestly receiving a stolen computer resource or communication device.	Knowingly receiving a stolen laptop dishonestly.
66C	Identity theft involving specified identification features.	Fraudulently using another person's password.
66D	Cheating by personation using a computer resource or communication device.	Impersonating a bank officer online to cheat someone.
66E	Specified privacy violations involving private-area images.	Sharing such an image without consent in prohibited circumstances.
66F	Cyberterrorism.	Conduct meeting the section's national-security-related conditions.
67 / 67A / 67B	Obscene electronic material, sexually explicit material, and specified child-related sexual material.	Publishing prohibited material online.
75	Extraterritorial application with the required Indian computer-resource connection.	Certain overseas conduct involving a computer resource in India.