

REMEDIES UNDER THE IT ACT FOR CYBER CRIME

Presented by: Advocate Vibhav Srivastava



INTRODUCTION TO CYBER CRIME

What is Cyber crime

Cybercrime refers to any criminal activity that involves a computer, network, or network device. It encompasses a wide range of illegal acts that can target individuals, organizations, or governments.

The United Nations categorizes cybercrime into two main types:

- Narrow sense (computer crime) targeting computer security.
- Broader sense (computer-related crime) involving illegal behavior related to computers and networks



LEGAL FRAMEWORK IN INDIA FOR CYBER CRIME

Primary Law:

The Information Technology Act, 2000 (amended in 2008) governs cybercrimes and data protection.

Supporting Laws/ Guidelines:

- Bhartiya Nayay Sanhita (BNS) addresses crimes like defamation, fraud, and threats.
- CERT-In guidelines assist in cyber incident reporting and response (In India, the Indian Computer Emergency Response Team (CERT-IN) plays a pivotal role in ensuring cybersecurity by issuing guidelines and frameworks that help organizations respond to cyber incidents effectively.)

Objective of Cyber Laws:

To safeguard electronic transactions and penalize misuse of technology.



LEGAL FRAMEWORK FOR CYBER CRIME UNDER IT ACT

Categories of Cybercrimes under IT Act

- 1.Hacking:** Unauthorized access or control over digital systems to manipulate data.
- 2.Identity Theft:** Misuse of personal data (e.g., Aadhaar or bank details) for illegal purposes.
- 3.Cyberstalking:** Repeated online harassment, including threats or intimidation.
- 4.Online Fraud:** Scams involving fake emails, phishing, or false websites.
- 5.Cyberterrorism:** Attacks on critical systems to threaten national security.

HACKING AND UNAUTHORIZED ACCESS

What Constitutes Hacking?

- Gaining unauthorized access to a computer system.
- Modifying or destroying data without permission.

Legal Provision:

Section 66 (IT Act)

Remedies Available:

- Penalty: Imprisonment up to 3 years and/or fine up to ₹5 lakh.
- Example: A hacker infiltrates a company's database and steals sensitive data.



IDENTITY THEFT AND ONLINE IMPERSONATION

What Constitutes Identity Theft and Online Impersonation

- Identity Theft: When someone's personal data is stolen for misuse.
- Impersonation: Pretending to be someone else online for financial gain or defamation.

Legal Provision (IT ACT):

- Section 66C: Addresses theft of personal identifiers such as Aadhaar, PAN, or bank details
- Section 66D: Penalizes impersonation for fraudulent purposes.

Remedies Available:

- Penalty: Imprisonment up to 3 years and/or fine up to ₹1 lakh.



CYBERSTALKING AND HARASSMENT

What Constitutes Cyberstalking and Harassment ?

Persistent online behavior aimed at monitoring, threatening, or intimidating someone.

Legal Provision:

- IT Act: Section 67 is for penalizing harassment involving obscene or offensive online messages.
- Section 78, BNS: Covers stalking, including online.

Remedies Available:

- Under Section 67 of the IT Act, when a stalker sends or posts any obscene content to the victim via electronic media then they will be liable to punish with 5 years of jail and Rs. 1 Lacs fine. If the incidence repeats then they will be liable to punish with 10 years of jail and Rs. 2 Lacs fine both.
- As per the provision provided in the law, when a stalker misuses victim's personal information to post an obscene message or comment on any electronic media, then this action is punishable for defaming and harming a person's reputation with imprisonment of 2 years, fine or both.
- Victims can report directly through cybercrime.gov.in or file a police complaint.

DATA PROTECTION AND NEGLIGENCE

What Constitutes negligence in Data Protection?

When a body corporate fails to use reasonable security practices and procedures in order to protect sensitive personal data and such negligence results in a wrongful gain or loss, it is said as Negligence in Data protection. It Applies when :

- Organizations are liable when they fail to protect sensitive user data.
- Negligence leading to data breaches or unauthorized access invites penalties.

Legal Provision:

Section 43A (IT Act)

Remedies Available:

Financial compensation based on proven damages.



CYBERTERRORISM

What Constitutes Cyberterrorism ?

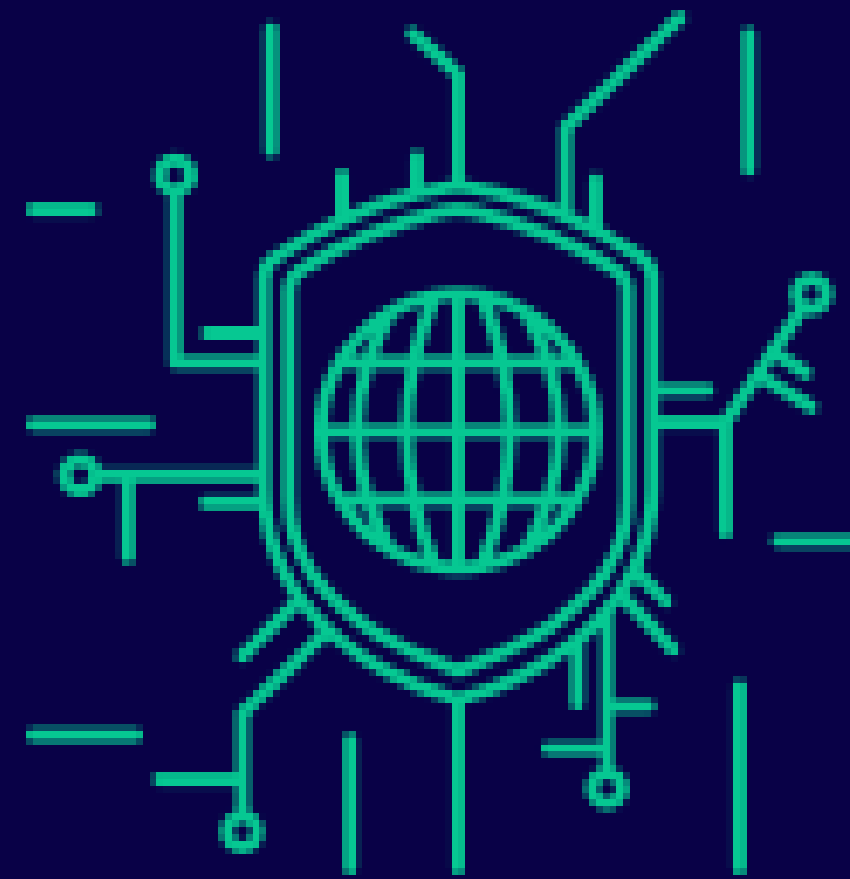
- Any cyber activity that threatens national security, sovereignty, or unity.
- Includes hacking critical systems like defense, power grids, or government databases.

Legal Provision:

Section 66F of IT Act

Punishment Available:

Life imprisonment for offenders.



Section 66F of IT Act defines Cyber terrorism as :

1(1) Whoever,—

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,
commits the offence of cyber terrorism.

ONLINE FRAUD AND PHISHING

What Constitutes Phishing?

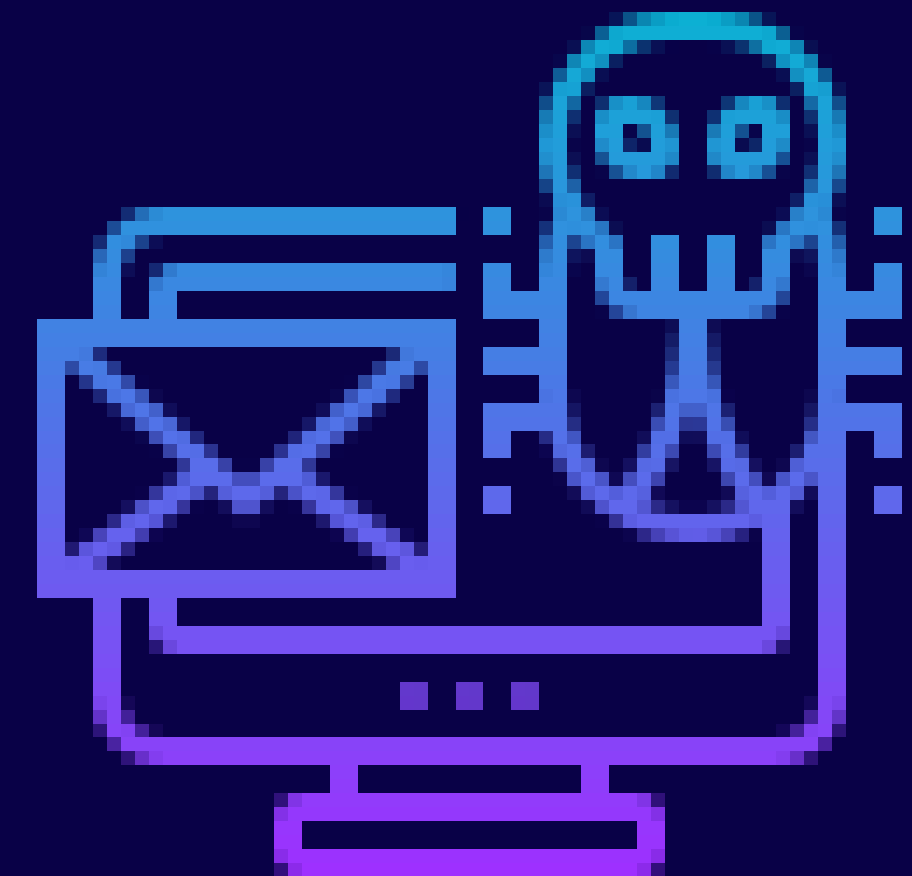
- Deceptive online tactics like fake emails or websites to steal sensitive information (e.g., OTPs, credit card details).
- Common Scams: Fake job offers, lottery scams, or fraudulent e-commerce platforms.

Legal Provision:

Section 66D of IT Act

Remedies Available:

- Imprisonment up to 3 years and fines.
- Victims should report incidents to their bank and the National Cyber Crime Reporting Portal – <https://cybercrime.gov.in/>



REPORTING CYBERCRIMES IN INDIA

Where to Report ?

1. Cybercrime.gov.in: A centralized national reporting portal. The affected party can also lodge complaint on the number 1930
2. Police Stations: Victims can file FIRs under the IT Act and BNS

Pre requisites :

1. For Evidence Collection: Gather all relevant evidence, including:
 - a. Screenshots of suspicious activities or communications.
 - b. Emails, messages, or any digital content related to the incident.
 - c. Logs or records that document the timeline of events.
2. Detailed Description: Provide a clear and concise description of what happened, including dates, times, and affected systems.
3. ID proofs (required during the filling of complaints)



CYBER INSURANCE AS A REMEDY

Cyber Insurance act as safety net if in case person is victim of cyber crime. Lets First understand what is Cyber insurance?

- Cyber insurance provides financial protection against losses resulting from cyber incidents, such as data breaches, cyber extortion, and business interruptions.
- These Policies typically include both first-party coverage (for direct losses incurred by the insured) and third-party coverage (for liabilities to others due to a cyber event).

Types of Losses Covered under Cyber Insurance :

- Financial Loss: Covers direct financial losses from cyber incidents, including theft of funds due to fraud or unauthorized transactions. It Includes costs associated with business interruption resulting from cyberattacks.
- Data Recovery: Expenses for recovering compromised data and restoring systems after a breach. Costs for forensic investigations to determine the extent of the damage and prevent future incidents.



FILING CLAIMS BEFORE ADJUDICATING OFFICER : AO

- **Section 46:** AO has Power to adjudicate any contravention of the Act/rules etc.
- **AO** can direct or order to the guilty person to pay penalty or compensation up to ₹ 5 crores
- **AO:** To be not below the rank of Director to the Govt. of India or an equivalent officer of State Govt.
- **AO:** To consider factors like amount of unfair advantage, loss caused to person, repetitive nature of default (Section 47) before adjudicating quantum of compensation.



APPEAL & OTHER PROVISIONS:

Section 48: Appeal of AO order to TDSAT

Section 62: Second Appeal to High Court


Section 60: Applicability of Limitation Act ,1963 to appeal

Section 61 : Bar on jurisdiction of Civil Court

Section 64: Penalty imposed or compensation awarded shall be recovered as an arrear of land revenue

CHALLENGES IN CYBERCRIME ENFORCEMENT

Key Issues:

1. Cross-border jurisdiction challenges.
 2. Lack of cyber literacy among victims.
 3. Delayed investigation due to technological complexities.
 4. Laws need constant updates to keep pace with evolving threats.
- 
- A decorative graphic in the bottom right corner consisting of several concentric, slightly offset circles in a light blue color, creating a sense of depth and movement.

RECOMMENDATIONS FOR VICTIMS OF CYBER CRIME

Steps Victims Should Take After Experiencing Cybercrime:

1. Report Incidents Promptly to Authorities:

- Victims should report cybercrime incidents to the appropriate authorities, such as the Cyber Crime Cell or local police, as soon as possible.
- Prompt reporting increases the chances of apprehending the offender and mitigating further damage.
- Utilize Online Reporting Portals: Many jurisdictions offer online platforms for reporting cybercrimes, making it easier for victims to file complaints.

2. Gather and Preserve Evidence:

- Document all details related to the incident, including dates, times, and descriptions of events.
- Take screenshots of communications, emails, or messages that are relevant to the case.

3. Preserve Digital Evidence:

- Avoid altering or deleting any digital evidence. This includes saving files, logs, and any other pertinent information that may assist in investigations.
- Consider using forensic tools or seeking professional help to ensure evidence is preserved correctly.

4. Seek Legal Advice from Professionals Specializing in Cyber Law:

- Victims should seek advice from lawyers who specialize in cyber law to understand their rights and options for pursuing justice.
- Legal professionals can provide guidance on filing civil lawsuits for compensation and navigating the complexities of cybercrime cases.



FOLLOW WHATSAPP CHANNEL

CYBERDOST

THANK YOU