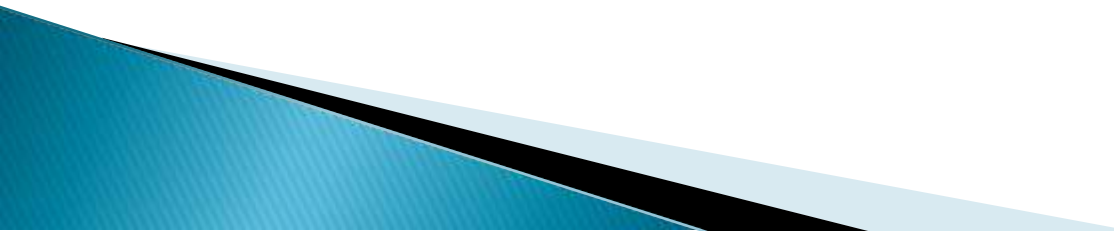


# CYBER LAWS (23CY512)

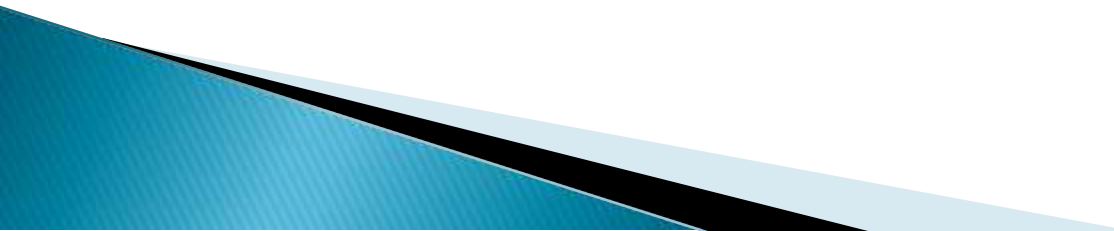
PPT PREPARED BY  
Mrs. P ARUNA  
Asst. Professor  
Computer Science and Engineering

# UNIT-I

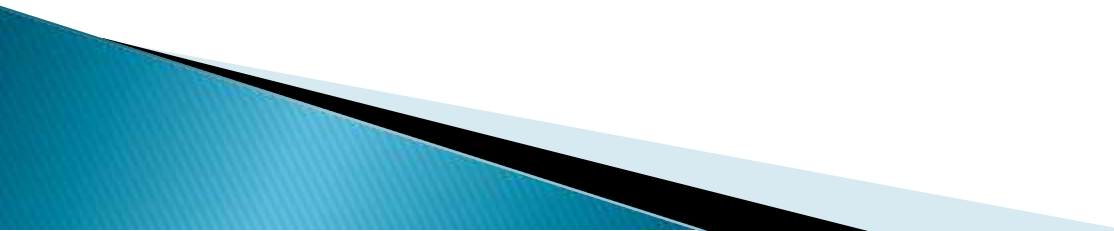
# History of Internet: Early Development

- ▶ 1960s: ARPANET project funded by the U.S. Department of Defense.
  - ▶ ARPANET connected research universities and defense contractors.
  - ▶ Used packet switching technology to enable data transmission.
  - ▶ Email became popular in the 1970s among academic and military users.
- 

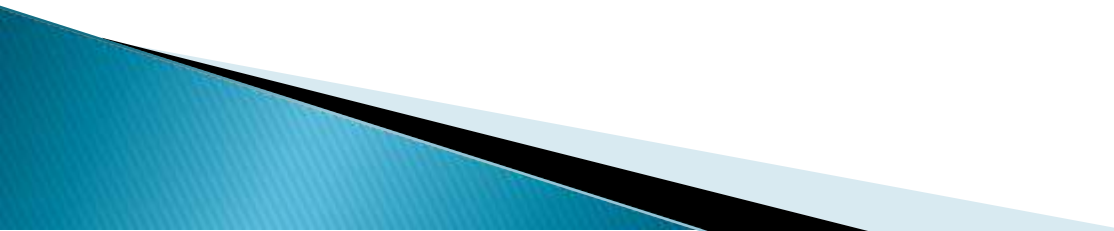
# History of Internet: Commercialization

- ▶ 1980s: TCP/IP protocol standardized and adopted widely.
  - ▶ 1989: Tim Berners-Lee proposed the World Wide Web.
  - ▶ 1991: WWW made public, changed the way people accessed data.
  - ▶ 1990s: Internet Service Providers (ISPs) began offering access to the public.
  - ▶ Rapid expansion through the 1990s led to the dot-com boom.
- 

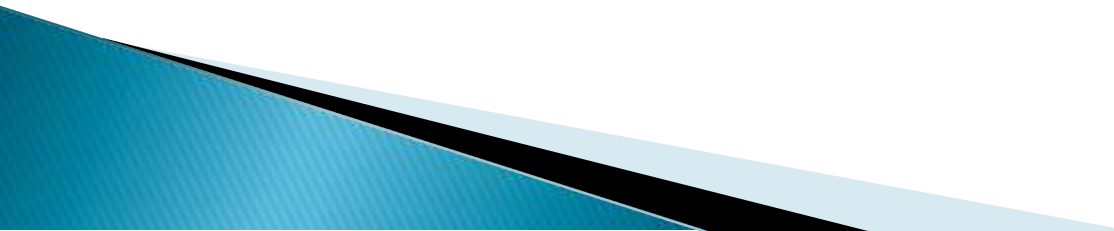
# History of the World Wide Web

- ▶ Developed by Tim Berners-Lee at CERN in 1989.
  - ▶ 1991: First website launched ([info.cern.ch](http://info.cern.ch)).
  - ▶ Browsers like Mosaic (1993) and Netscape Navigator (1994) fueled web adoption.
  - ▶ HTML, URLs, and HTTP became the foundation of the Web.
  - ▶ E-commerce, social media, and streaming transformed online experiences.
- 

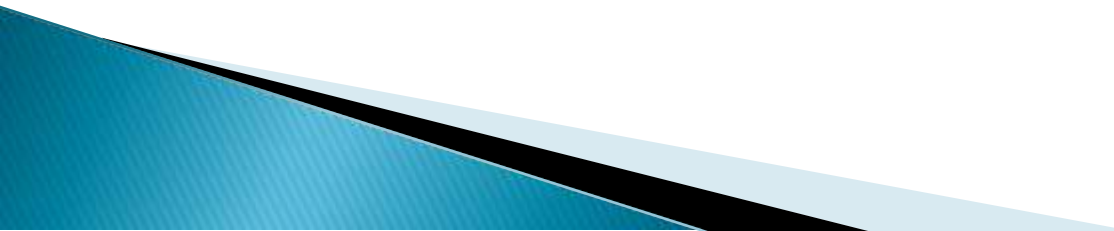
# Need for Cyber Law: Overview

- ▶ The rise in internet use has led to increase in cybercrimes.
  - ▶ Conventional laws were insufficient to address digital issues.
  - ▶ Cyber laws regulate online behavior and protect digital rights.
  - ▶ Provide a legal framework for e-commerce and online contracts.
- 

# Need for Cyber Law: Key Reasons

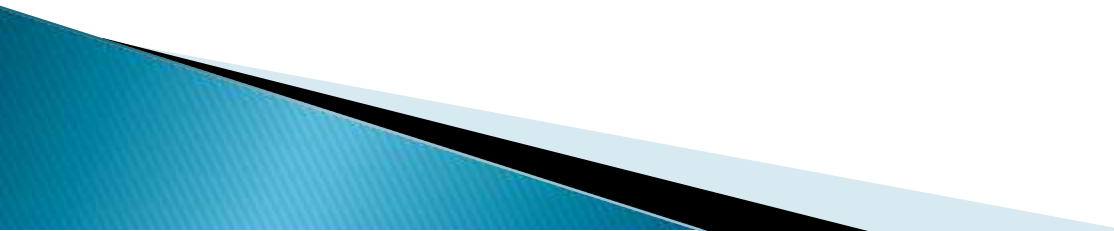
- ▶ Protect against hacking, identity theft, and data breaches.
  - ▶ Ensure privacy and security of personal and financial data.
  - ▶ Regulate digital content and prevent cyber terrorism.
  - ▶ Promote trust and reliability in online transactions.
- 

# Cybercrime on the Rise: Common Types

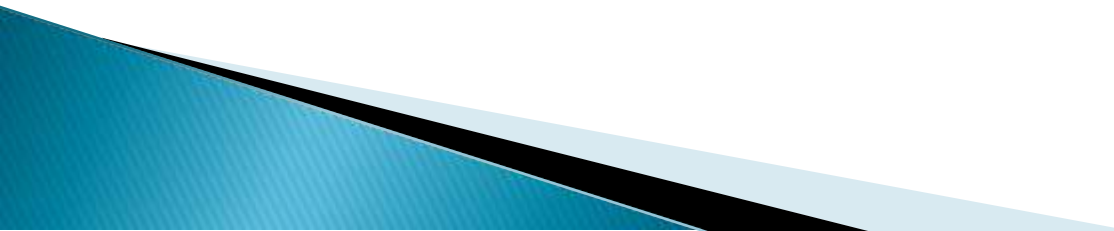
- ▶ Hacking: Unauthorized access to systems and networks.
  - ▶ Phishing: Deceptive emails or websites to steal data.
  - ▶ Malware: Viruses, worms, ransomware affecting systems.
  - ▶ Cyberstalking and cyberbullying via social platforms.
- 



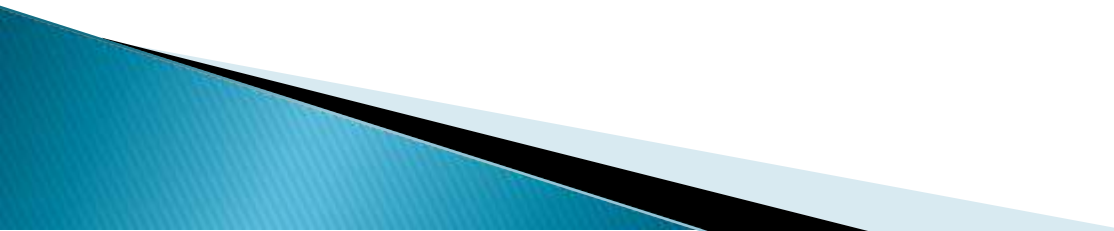
# Cybercrime on the Rise: Impacts

- ▶ Financial losses to individuals and businesses.
  - ▶ Loss of privacy and exposure of sensitive data.
  - ▶ Disruption of services (DDoS attacks, ransomware).
  - ▶ Threats to national security and infrastructure.
- 

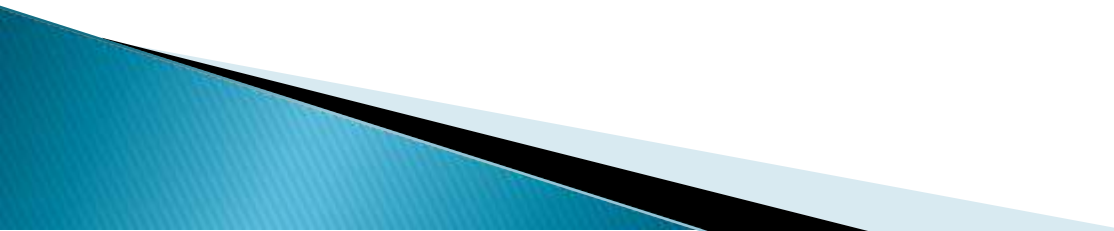
# Key Cyber Law Terms – Part 1

- ▶ Cybercrime: Illegal activity using computers or networks.
  - ▶ Hacking: Unauthorized intrusion into computer systems.
  - ▶ Phishing: Fraudulent attempts to obtain sensitive data.
  - ▶ Digital Signature: Cryptographic method to verify authenticity.
- 

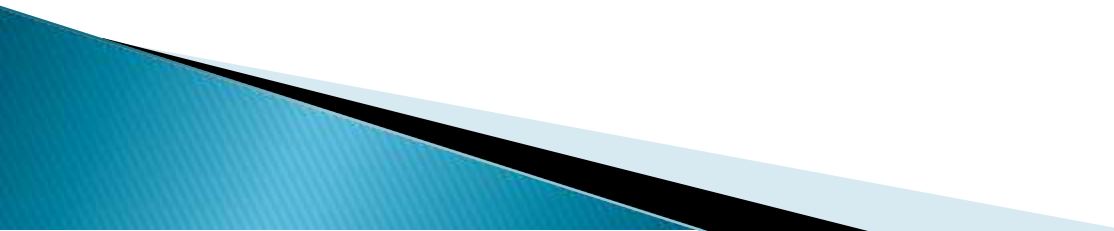
# Key Cyber Law Terms – Part 2

- ▶ Cyber Forensics: Investigation of digital crimes.
  - ▶ Firewall: Security system that controls incoming/outgoing traffic.
  - ▶ ISP (Internet Service Provider): Company offering internet access.
  - ▶ Data Protection: Legal control over the access and use of personal data.
- 

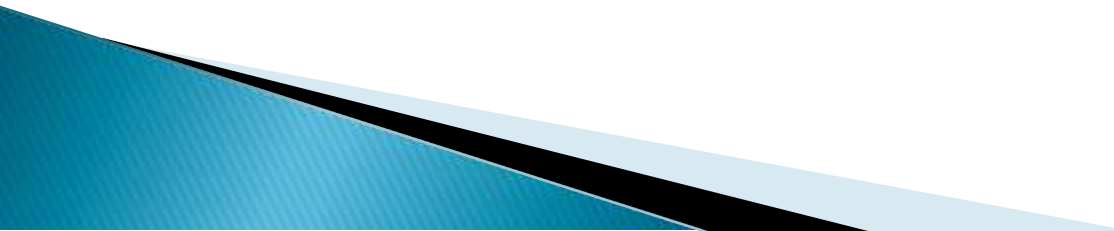
# Need for Cyber Law in India – Overview

- ▶ India's digital economy and user base is rapidly growing.
  - ▶ Cyber threats such as hacking, data breaches, and fraud are increasing.
  - ▶ Need for protecting personal data and online transactions.
  - ▶ Existing traditional laws were not equipped to handle cybercrimes.
- 

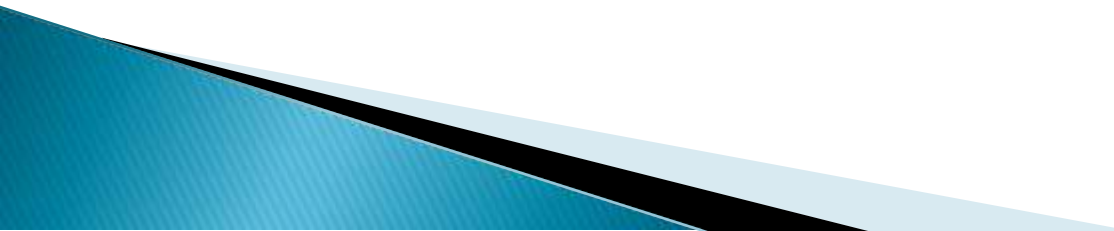
# Need for Cyber Law in India – Specific Reasons

- ▶ To provide legal recognition for electronic records and signatures.
  - ▶ To regulate e-commerce and online banking.
  - ▶ To curb cyber terrorism, child pornography, and digital harassment.
  - ▶ To ensure national security in cyberspace.
- 

# History of Cyber Law in India – Early Stage

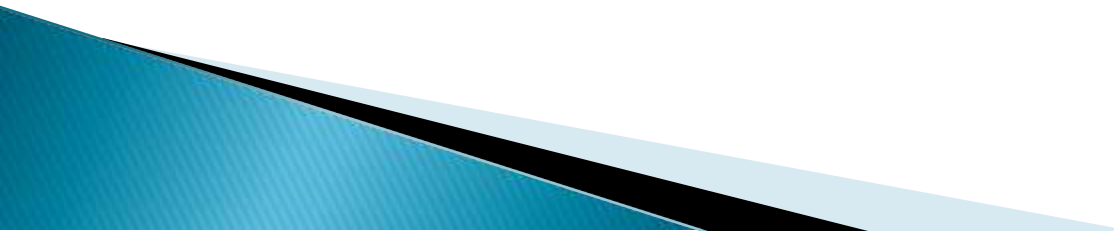
- ▶ Before 2000: No dedicated laws for cyber activities.
  - ▶ Crimes involving computers handled under Indian Penal Code (IPC).
  - ▶ Need for a comprehensive law felt with increasing online activity.
  - ▶ Influence from UNCITRAL Model Law on Electronic Commerce (1996).
- 

# History of Cyber Law in India – IT Act, 2000

- ▶ Enacted on 17th October 2000.
  - ▶ India's first law on electronic commerce and cybercrime.
  - ▶ Provided legal recognition for electronic documents.
  - ▶ Defined cybercrime and laid penalties for offenses.
- 

# Information Technology Act, 2000

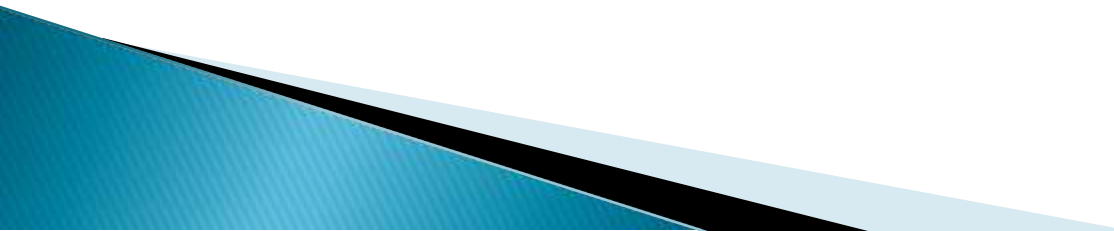
## – Key Objectives

- ▶ Grant legal recognition to e-documents and digital signatures.
  - ▶ Facilitate electronic filing of documents with government agencies.
  - ▶ Prevent and punish cybercrimes like hacking, phishing, and identity theft.
  - ▶ Enable e-Governance and online contracts.
- 

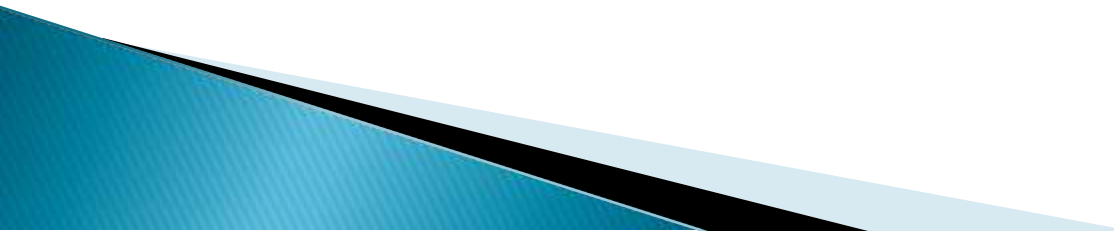


# Information Technology Act, 2000

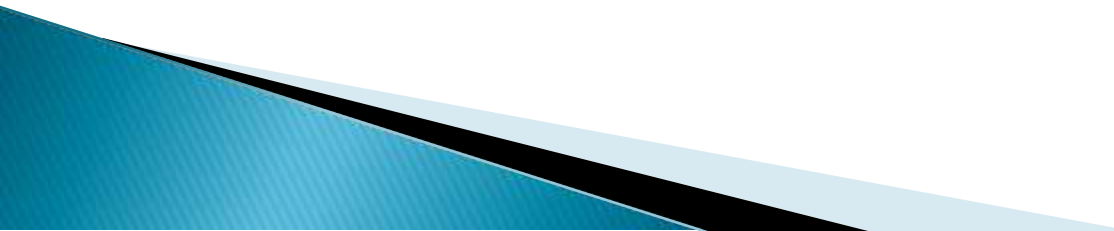
## – Key Features

- ▶ Covers cyber offenses and data protection.
  - ▶ Empowers law enforcement with investigation tools.
  - ▶ Recognizes electronic records and digital signatures.
  - ▶ Establishes Certifying Authorities and Cyber Appellate Tribunal.
- 

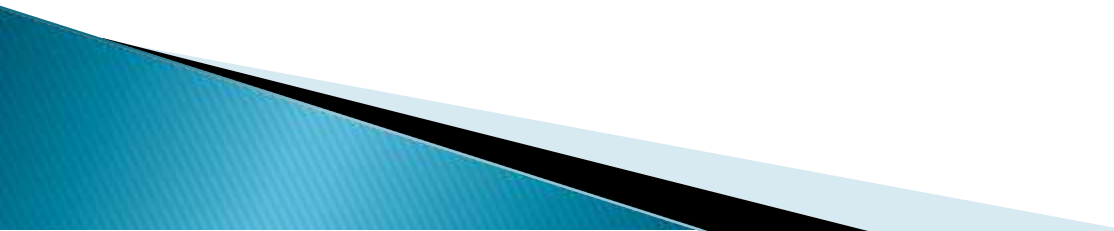
# Other Laws Amended by IT Act, 2000

- ▶ Indian Penal Code (IPC), 1860 – to include cyber offenses.
  - ▶ Indian Evidence Act, 1872 – admissibility of electronic evidence.
  - ▶ Bankers' Books Evidence Act, 1891 – inclusion of digital records.
  - ▶ Reserve Bank of India Act, 1934 – support for digital banking regulations.
- 

# National Policy on Information Technology 2012 – Vision

- ▶ Empower citizens and businesses through Information Technology.
  - ▶ Make India a global hub for IT and IT-enabled services.
  - ▶ Promote innovation and R&D in digital technologies.
  - ▶ Ensure secure and reliable IT infrastructure.
- 

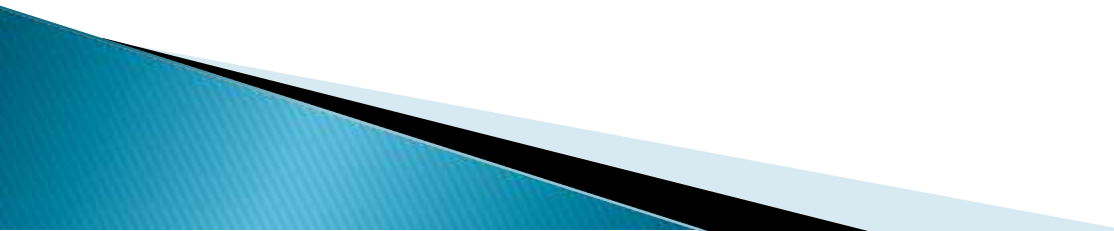
# National Policy on Information Technology 2012 – Key Goals

- ▶ Increase ICT contribution to GDP.
  - ▶ Promote digital literacy and IT skill development.
  - ▶ Enhance cyber security and data protection.
  - ▶ Foster e-Governance and inclusive growth through IT.
- 

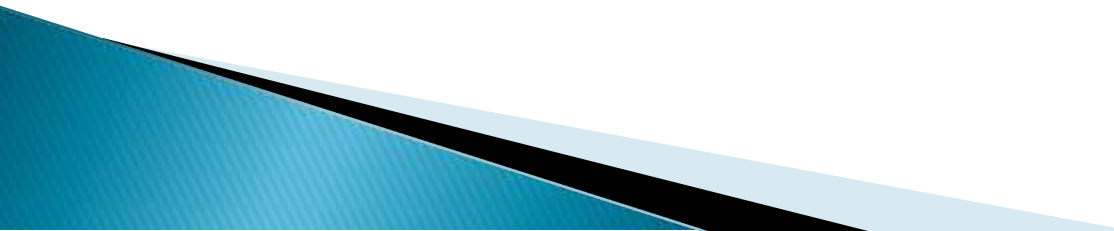
# UNIT-II



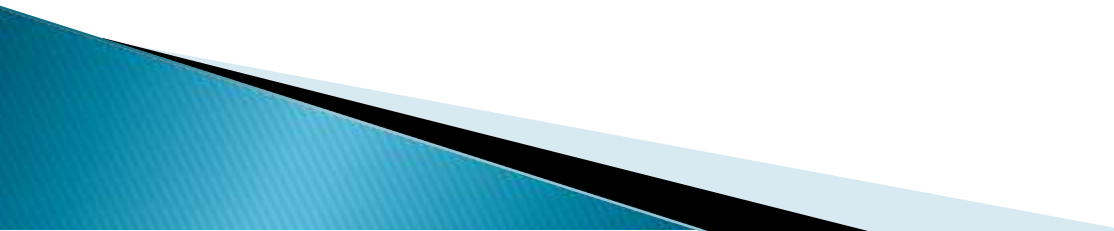
# Applicability of the IT Act, 2000

- ▶ • Applies to the whole of India.
  - ▶ • Also applies to any offence or contravention committed outside India by any person.
  - ▶ • Covers all electronic records and digital communications.
  - ▶ • Applicable to companies, individuals, and intermediaries involved in digital transactions.
- 

# Important Provisions of the Act

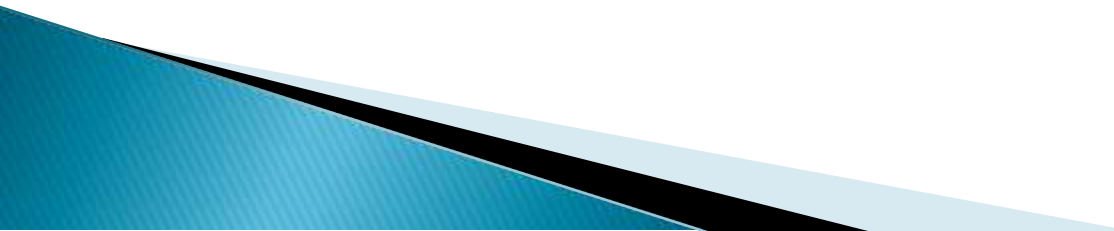
- ▶ • Legal recognition of electronic records.
  - ▶ • Legal recognition of digital signatures.
  - ▶ • Use of electronic records and digital signatures in government and its agencies.
  - ▶ • Regulation of certifying authorities.
  - ▶ • Penalties and adjudication for cyber offences.
- 

# Digital and Electronic Signatures

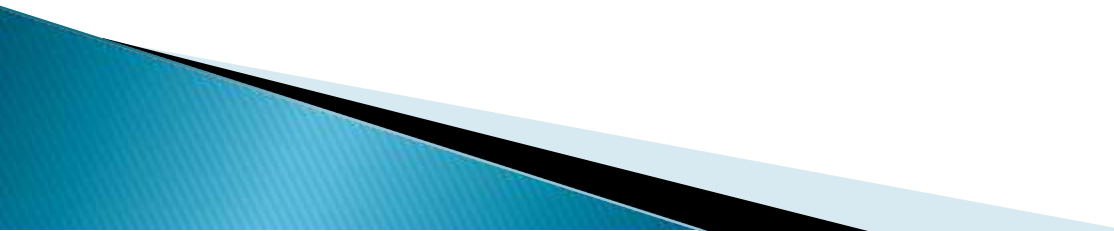
- ▶ • Digital Signature: Ensures authenticity and integrity of electronic documents.
  - ▶ • Electronic Signature: Broader term including various types of electronic authentication.
  - ▶ • Both provide legal validity to electronic records.
- 



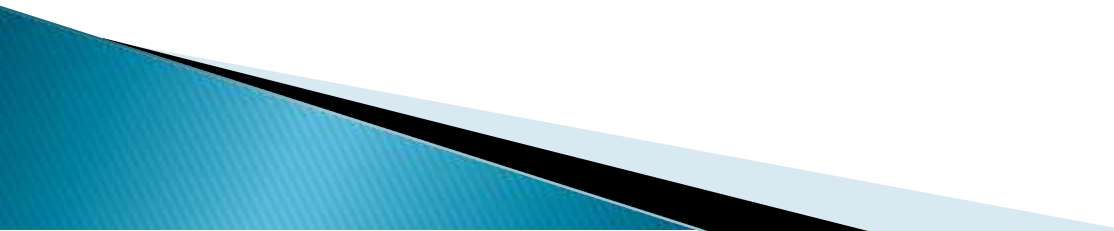
# Digital Signature under the IT Act, 2000

- ▶ • Used to authenticate an electronic record.
  - ▶ • Must be secure and issued by a licensed Certifying Authority.
  - ▶ • Ensures non-repudiation and security of digital communications.
- 

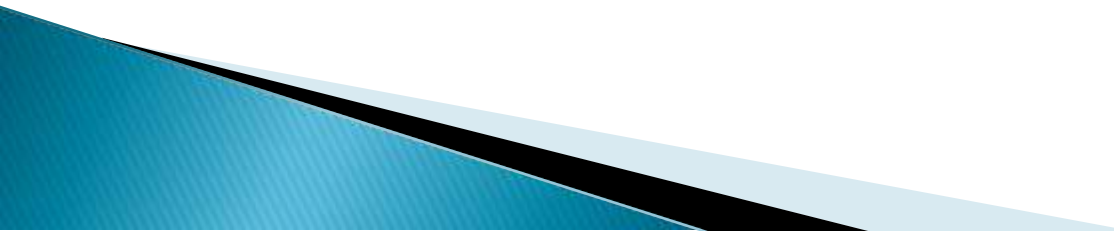
# E-Governance

- ▶ • Promotes electronic governance and digital record maintenance.
  - ▶ • Allows filing of applications, forms, and other documents online.
  - ▶ • Facilitates delivery of services through electronic means.
- 

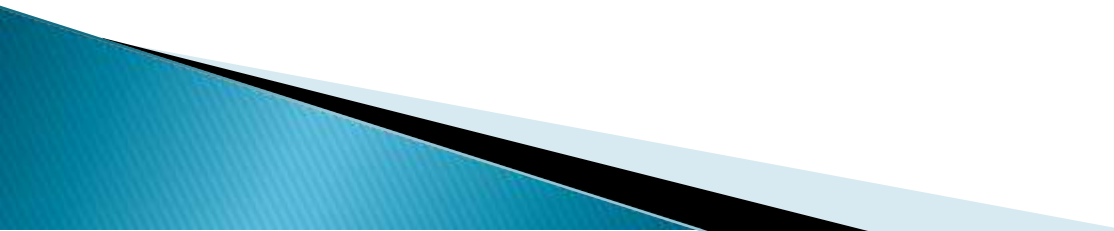
# Electronic Records: Attribution, Acknowledgement & Dispatch

- ▶ • Attribution: Establishes authorship of electronic records.
  - ▶ • Acknowledgement: Confirms receipt of electronic records.
  - ▶ • Dispatch: Time and place of sending/receiving electronic communications.
- 

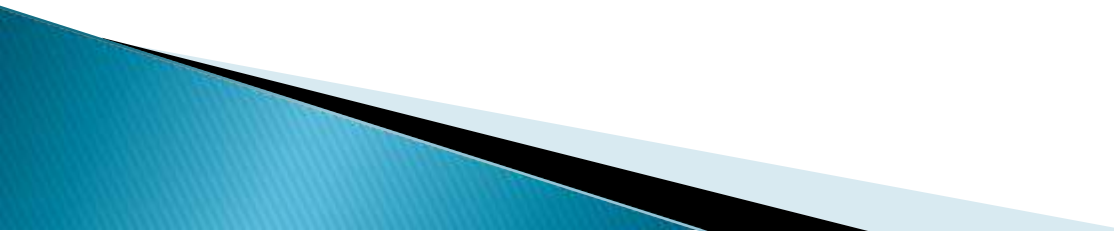
# Certifying Authorities

- ▶ • Licensed to issue Digital Signature Certificates (DSCs).
  - ▶ • Monitored by the Controller of Certifying Authorities (CCA).
  - ▶ • Ensure security and validity of electronic signatures.
- 

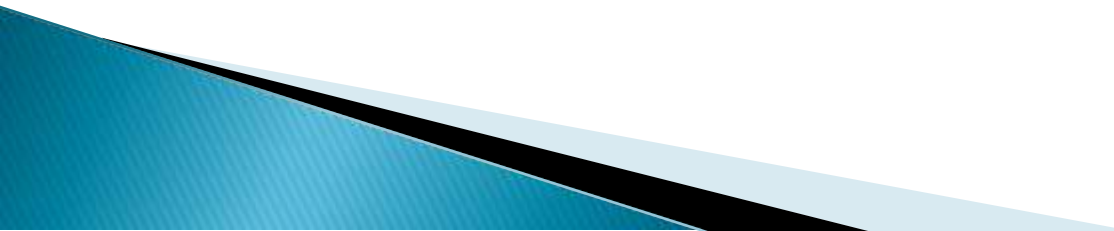
# Electronic Signature Certificates

- ▶ • Issued by Certifying Authorities.
  - ▶ • Contains subscriber's public key, identity, and digital signature.
  - ▶ • Legally binding and recognized under the Act.
- 

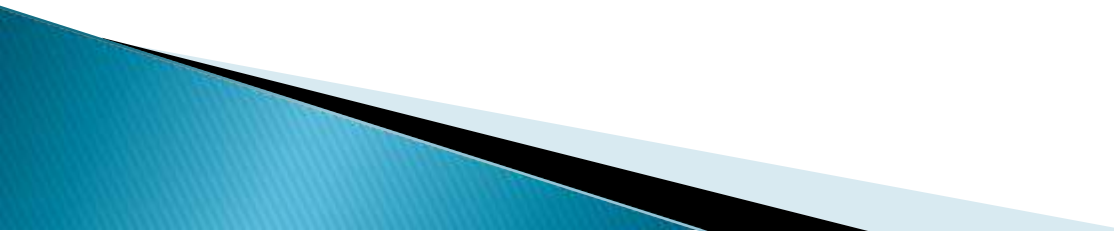
# Duties of Subscribers

- ▶ • Generate key pair securely.
  - ▶ • Accept responsibility for protection of private key.
  - ▶ • Inform Certifying Authority in case of key compromise.
  - ▶ • Ensure usage aligns with certificate conditions.
- 

# Penalties and Offences

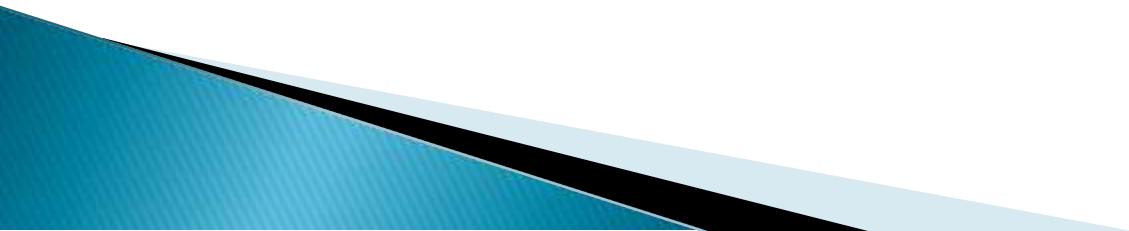
- ▶ • Cyber crimes like hacking, identity theft, phishing.
  - ▶ • Fines and imprisonment depending on severity.
  - ▶ • Adjudicating officers and Cyber Appellate Tribunal handle disputes.
- 

# Intermediaries

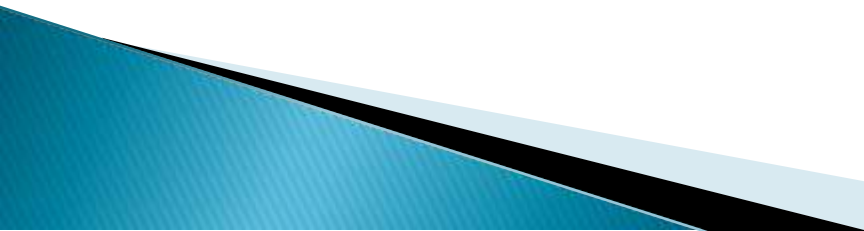
- ▶ • Entities like ISPs, web-hosting services, social media platforms.
  - ▶ • Required to observe due diligence and cooperate with authorities.
  - ▶ • Not liable for third-party content if acting as a neutral facilitator.
- 



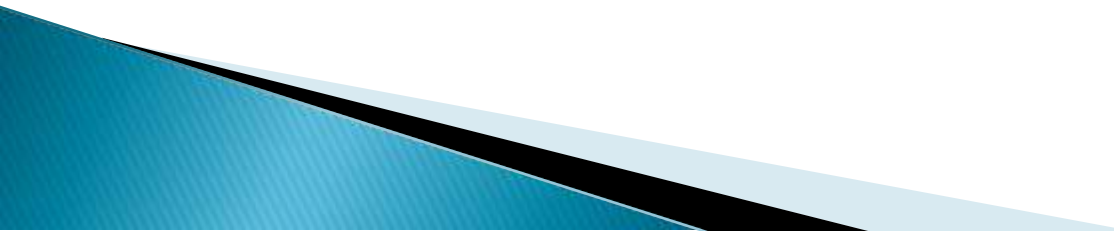
# UNIT-III



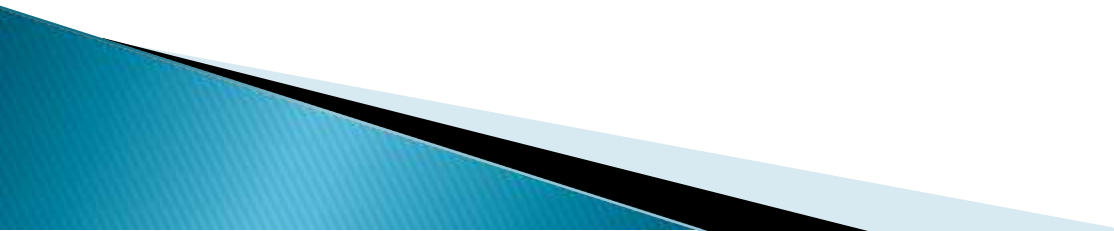
# Rules Issued Under IT Act, 2000

- ▶ • Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
  - ▶ • The Intermediary Guidelines and Digital Media Ethics Code Rules, 2021.
  - ▶ • Rules for Certifying Authorities.
  - ▶ • Cyber Appellate Tribunal (Procedure) Rules.
  - ▶ • Rules for electronic service delivery, electronic records retention, etc.
- 

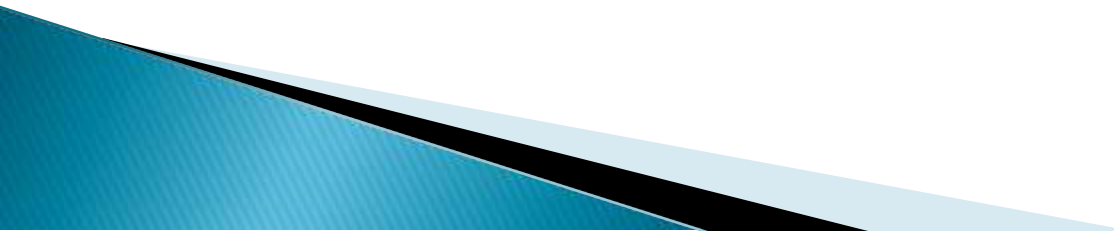
# Electronic Commerce

- ▶ • Conducting business transactions through electronic means.
  - ▶ • Includes buying, selling, online banking, e-marketing.
  - ▶ • IT Act provides legal recognition to electronic transactions.
  - ▶ • Enables e-filing of documents and e-payment systems.
  - ▶ • Secures online data exchanges and communications.
- 

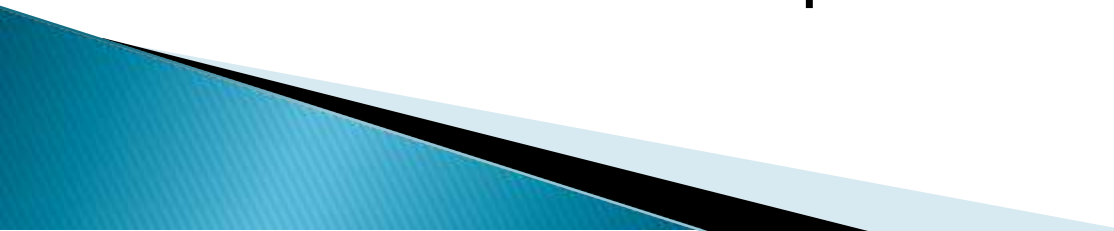
# Electronic Contracts

- ▶ • Legally valid under Section 10A of the IT Act.
  - ▶ • Formed through electronic communication like email, online forms.
  - ▶ • Offer, acceptance, and intention to contract are essential.
  - ▶ • Digital/electronic signatures authenticate contracts.
  - ▶ • Binding if compliant with legal formalities.
- 

# Cyber Crimes

- ▶ • Criminal activities involving computers or networks.
  - ▶ • Examples: Hacking, phishing, identity theft, data breaches.
  - ▶ • Punishable under IT Act and IPC provisions.
  - ▶ • Handled by Cyber Crime Cells across India.
  - ▶ • Increased regulation to ensure digital safety and trust.
- 

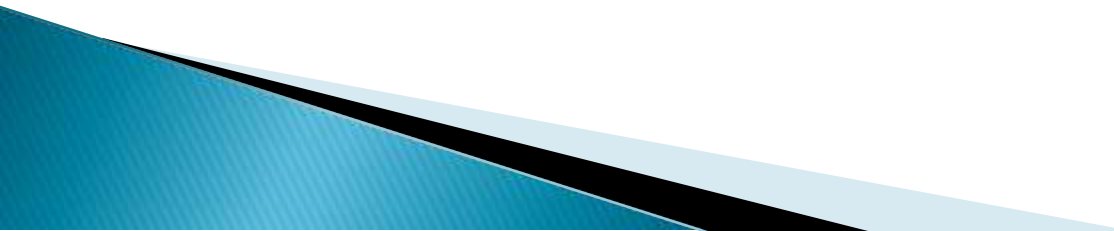
# Cyber Frauds

- ▶ • Fraudulent activities executed via digital means.
  - ▶ • Includes online scams, financial frauds, fake websites.
  - ▶ • Often target banking, e-commerce and personal data.
  - ▶ • Legal remedies available under IT Act & Indian Penal Code.
  - ▶ • Users advised to practice cybersecurity awareness and report incidents.
- 

# UNIT-IV

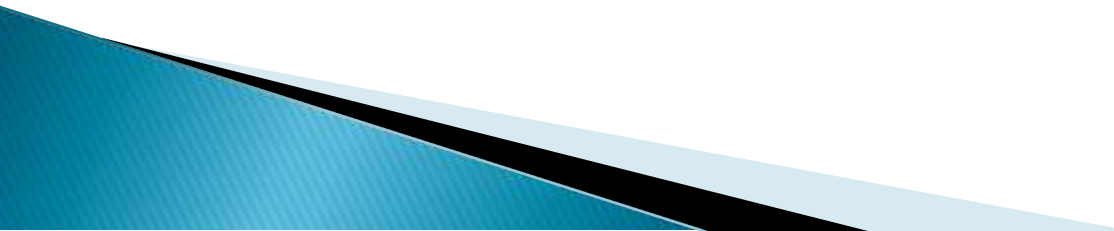


# Department of Electronics and Information Technology (DeitY)

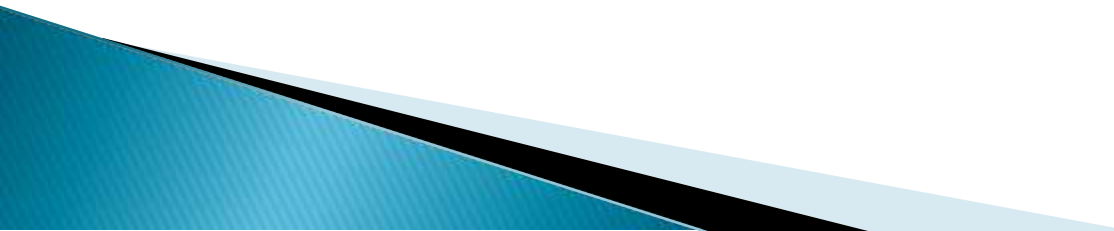
- ▶ • Now part of Ministry of Electronics and Information Technology (MeitY).
  - ▶ • Formulates policies on IT, electronics, and internet governance.
  - ▶ • Responsible for promotion of e-Governance and digital services.
  - ▶ • Implements IT Act provisions and cybersecurity policies.
- 



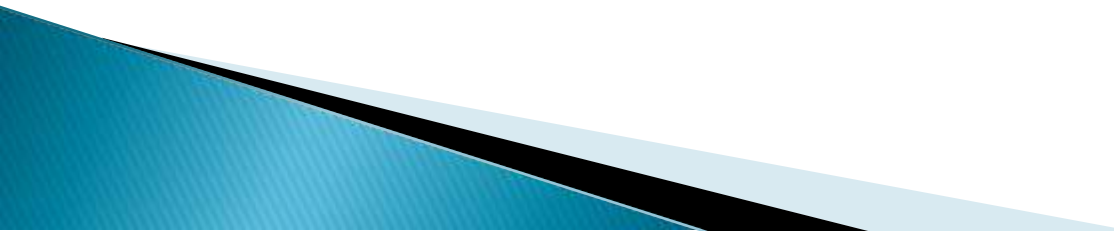
# Controller of Certifying Authorities (CCA)

- ▶ • Established under the IT Act, 2000.
  - ▶ • Regulates functioning of Certifying Authorities (CAs).
  - ▶ • Issues licenses and ensures compliance with standards.
  - ▶ • Maintains trust in digital signature ecosystem.
- 


# Cyber Appellate Tribunal

- ▶ • Established to handle appeals against orders of adjudicating officers.
  - ▶ • Deals with disputes related to cyber crimes and contraventions under IT Act.
  - ▶ • Replaced by Telecom Disputes Settlement and Appellate Tribunal (TDSAT) in 2017.
  - ▶ • Ensures justice in digital and cyber law cases.
- 


# Indian Computer Emergency Response Team (ICERT)

- ▶ • National agency for responding to cyber security incidents.
  - ▶ • Operates under MeitY.
  - ▶ • Issues alerts and advisories on latest cyber threats.
  - ▶ • Coordinates incident response, vulnerability handling and risk mitigation.
- 

# Cloud Computing

- ▶ • On-demand delivery of IT services over the internet.
  - ▶ • Includes storage, servers, databases, networking, software.
  - ▶ • Raises data security and jurisdiction concerns.
  - ▶ • Not directly covered under IT Act, but subject to data protection norms.
  - ▶ • Regulated indirectly through IT rules and MeitY guidelines.
- 

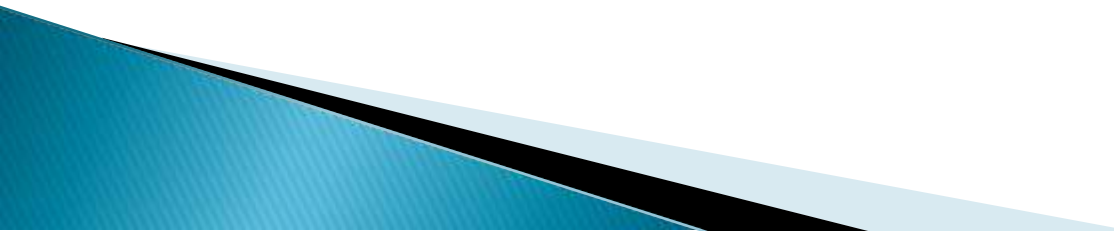
# Important Case Laws under IT Act

- ▶ • Avnish Bajaj v. State (Bazee.com case): Liability of intermediaries.
  - ▶ • Shreya Singhal v. Union of India: Struck down Section 66A for violating freedom of speech.
  - ▶ • Sony Sambandh case: First conviction under IT Act.
  - ▶ • Nasscom v. Ajay Sood: Email spoofing declared illegal.
  - ▶ • Illustrates evolving interpretation of IT law by judiciary.
- 


# UNIT-V



# Introduction to Cybercrime

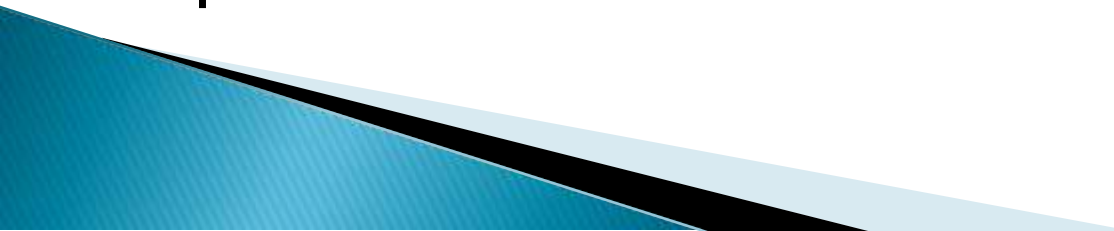
- ▶ • Cybercrime refers to illegal activities involving computers or digital devices.
  - ▶ • Includes hacking, identity theft, cyberstalking, phishing, online fraud, etc.
  - ▶ • Targets individuals, businesses, or governments.
  - ▶ • Rapid increase due to digital transformation and internet usage.
- 

# Procedure to Report Cybercrime

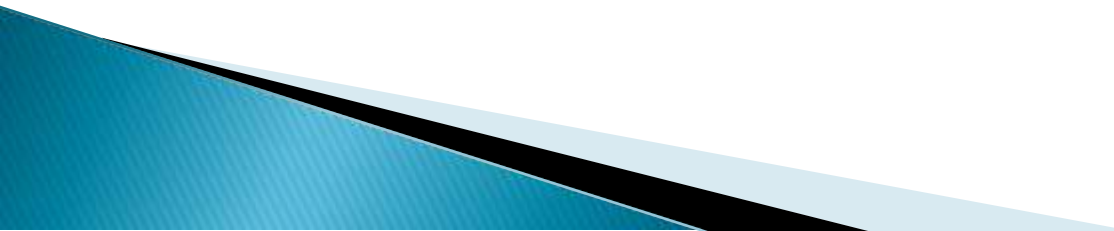
- ▶ • Visit the National Cybercrime Reporting Portal ([www.cybercrime.gov.in](http://www.cybercrime.gov.in)).
  - ▶ • Choose 'Report Women/Child Related Crime' or 'Report Other Cybercrime'.
  - ▶ • Register complaint with local Cyber Cell or police station.
  - ▶ • Provide necessary details and evidence such as screenshots, emails, etc.
  - ▶ • FIR can be lodged under IT Act and Indian Penal Code (IPC).
- 



# Basic Rules for Safe Operations

- ▶ • Use strong, unique passwords and change them regularly.
  - ▶ • Install antivirus and update software frequently.
  - ▶ • Avoid clicking on suspicious links or downloading unknown attachments.
  - ▶ • Use secure websites (HTTPS) for financial transactions.
  - ▶ • Enable two-factor authentication where possible.
- 

# Criminal Law (Amendment) Act, 2013

- ▶ • Enacted in response to rising crimes against women, including online harassment.
  - ▶ • Expanded the definition of sexual offences under IPC.
  - ▶ • Introduced new sections to cover stalking and voyeurism.
  - ▶ • Recognized online harassment as a punishable offence.
- 

# Remedies for Online Harassment & Cyberstalking

- ▶ • Section 354D IPC: Punishes stalking including online stalking (up to 3 years imprisonment).
  - ▶ • Section 509 IPC: Addresses obscene gestures, comments or emails.
  - ▶ • IT Act Section 66E: Punishes violation of privacy through electronic means.
  - ▶ • Victims can report anonymously and seek legal protection and restraining orders.
  - ▶ • Cyber Cells and women's helplines are available for assistance.
- 