CYBER LAWS

Code of Conduct for the Digital Age.

super notes.
by CIVILIANZ

super notes.
by CIVILIANZ
TRUST THE PROCESS

INDEX

"The future belongs to those who believe in the beauty of their dreams."
— Eleanor Roosevelt

Reach us: 8281223366
JOIN NOW

IT ACT 2000

- The first cyber law introduced in India – IT Act 2000
- IT Act was passed in India on June 9, 2000
- IT Act 2000 came into force on October 17, 2000
- IT Act 2000 had 13 Chapters, 94 Sections, and 4 Schedules.
- Schedule 1 - Amendment to IPC
- Schedule 2 – Amendment to Indian Evidence Act
- Schedule 3 - Amendment to Bankers Book Evidence Act
- Schedule 4 – Amendment to RBI Act
- The subject of cyber laws is included in the Indian Constitution under – Residual Powers.

IT ACT (Amendment) 2008

- Year in which IT Act was amended – 2008
- IT Amendment Act was passed by Parliament on – December 23, 24, 2008
- IT Amendment Act 2008 was signed by the President on – February 5, 2009
- The amended IT Act came into force on – October 27, 2009

There are 14 chapters and 124 sections, 4 parts, 2 schedules in IT Act (Amendment) 2008

- Part 1- Preliminary
- Part 2 - Amendment to the IT ACT 2000
- Part 3 – Amendment to the Indian Penal Code
- Part 4 – Amendment to the Indian Evidence Act

Reach us: 8281223366 JOIN NOW

- Schedule 1 - Documents or transactions to which the act shall not apply
- Schedule 2 – Electronic signature or electronic authentication technique and procedure

CHAPTERS IN IT ACT

- Chapter 1 – Preliminary (Section 1-2)

Explains the basic provisions of IT law. It clarifies the scope, objectives, and applicable areas of the law.

- Chapter 2 – Electronic Signature (Section 3)

Explains about Digital Signatures. Electronic signatures are used to ensure the authenticity of electronic records. This helps secure documents and ensure their trustworthiness.

- Chapter 3 – Electronic Governance (Section 4-10)

This chapter explains the procedures for Electronic Governance. It specifies the rules regarding sending and receiving electronic records, their time, place, and authentication. It provides a framework for delivering Government services electronically.

- Chapter 4 – Attribution, Acknowledgment, and Dispatch of Electronic Records (Section 11-13)

Origin, acceptance, and dispatch of electronic records.
This chapter explains the rules regarding who sent an electronic record, who received it, when, and where. It defines the responsibilities of the sender and receiver, and the method for confirming receipt.

- Chapter 5 – Secure Electronic Records and Secure Electronic Signatures (Section 14-16)

Explains the technical standards for ensuring the security of Electronic Records and Electronic Signatures.

Reach us: 8281223366
JOIN NOW

- **Chapter 6 – Regulation of Certifying Authorities (Section 17-34)**

This chapter explains the rules for regulating Certifying Authorities (CAs) that issue digital certificates.

- **Chapter 7 – Digital Signature Certificates (Section 35-39)**

This chapter deals with the issuance, revocation, and use of Digital Signatures and Certificates (DSCs). It explains the procedures for issuing certificates and their validity.

- **Chapter 8 – Duties of Subscribers (Section 40-42)**

Users of digital certificates must fulfill their responsibilities. This section explains the security, confidentiality, and prevention of misuse of certificates.

- **Chapter 9 – Penalties and Adjudication (Section 43-47)**

This chapter explains the penalties and compensation for violations of IT law.

- **Chapter 10 – The Cyber Regulations Appellate Tribunal (Section 48-64)**

This chapter is about the Cyber Appellate Tribunal for resolving disputes related to IT law. It explains the formation, powers, and procedures of the Tribunal.

- **Chapter 11 – Offences (Section 65-78)**

This chapter deals with cyber crimes. It explains the punishments for hacking, data theft, virus dissemination, online fraud, publication of obscene material, and other related offenses.

- **Chapter 12 – Network Service Providers Not to Be Liable in Certain Cases (Section 79)**
- **Chapter 12A – Examiner of Electronic Evidence (Section 79A)**
- **Chapter 13 – Miscellaneous (Section 80-84)**

Reach us: 8281223366
JOIN NOW

super notes.
by CIVILIANZ
TRUST THE PROCESS

SECTIONS OF IT ACT

- Section 3 - Legal recognition of electronic records (Authenticity of electronic records)
- Section 3A - Electronic Signature
- Section 4-10 - Electronic Governance
- Section 5 - Legal recognition of digital signatures
- Section 6 - Use of electronic records and digital signatures in Government and its agencies
- Usage of electronic records and digital signatures in government and its agencies.
- Section 7 - Retention of electronic records Regarding the retention of electronic records.
- Section 8 - Publication of rule, regulation etc in electronic gazette
- Section 10 - Power to Make Rules by Central Government in respect of Electronic Signature
- Section 11 - Attribution of electronic records
- This is the rule for identifying who sent the electronic record (originator).
- Section 12 - Acknowledgement of receipt
- This section deals with the procedures for the recipient of an electronic record to confirm its receipt.
- Section 13 - Time and place of dispatch and receipt of electronic records
- Explains when and where electronic records are considered to have been dispatched and received.
- Section 17 – Appointment of controller and other officers
- Regarding the appointment of the controller and other officers.

Reach us: 8281223366
JOIN NOW

- Section 18 - Functions of controller (Duties of the controller)
- Section 19 - Recognition of foreign certifying authorities
- Guidelines for recognizing foreign certifying authorities.
- Section 21 – The license to issue digital signature certificate
- Regarding the license to issue digital signature certificates.
- Section 44- Penalty for failure to furnish information, return etc
- This is about penalties applicable if an individual, institution, or company fails to provide requested information, returns, or other documents under IT law, or provides them late, or provides incorrect information.
- Section 48 - Establishment of Cyber Appellate Tribunal
- Section 62 - Appeal to High Court
- Section 65 - Tampering with Computer Source Document
- Cyber tampering (removing correct documents or inserting incorrect documents in an electronic medium).
- Section 66 - Hacking (Under the 2008 amendment, hacking was made a computer-related offense)
- Section 66A- Punishment for sending offensive messages through electronic means
- (This section was scrapped by the Supreme Court in 2015)
- Section 66B – Receiving stolen computer or communication device (Theft/receiving stolen electronic devices).
- Section 66C - Identity theft
- Identity theft is the act of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person. This includes stealing a person's password, digital signature, biometric data, bank account details, credit card information, etc., through electronic means.

- Section 66D - Cheating by personation by using computer resources
- Impersonation.
- Section 66E - Violation of privacy
- Section 66F - Cyber terrorism
- Section 67A - Pornography - Publishing images containing sexually explicit act Displaying, disseminating obscene pictures, videos.
- Section 67B - Child Pornography (Displaying, disseminating child obscene pictures, videos)
- Section 69A - Power of Central Government to issue directions for interception or monitoring or decryption of any information through any computer resource. In 2020, the Central Government banned several Chinese apps under IT Act Section 69A.
- Section 70- Unauthorized access to protected system
- Section 70B – Indian Computer Emergency Response Team (CERT-in)
- Section 73 – Penalty for publishing false digital signature certificate (Manufacturing and disseminating false digital signatures).
- Section 74 – Fraudulent Publication
- The term 'Electronic Signature' was introduced by Information Technology (Amendment) Act 2008.

Reach us: 8281223366 JOIN NOW

super notes.
by CIVILIANZ
TRUST THE PROCESS

CYBER PUNISHMENTS

Section	Contents	Imprisonment Up to	Fine Up to
65	Tampering with computer source code documents	3 years or/and	200,000
66	Hacking with computer system dishonestly or fraudulently	3 years or/and	500,000
66B	receiving Stolen computer resource	3 years or/and	100,000
66C	Identity Theft - fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person	3 years and	100,000
66D	cheating by Personation by using computer resource	3 years and	100,000
66E	Violation of Privacy	3 years or/and	200,000
66F	Acts of cyber terrorrism	Imprisonment for Life	
67	Publish or transmit Obscene material - 1st time Subsequent Obscene in elec. Form	3 years and 5 years and	500,000 10,00,000
67A	Publishing or transmitting material containing Sexually Explicit Act - 1st time Subsequent	5 years and 7 years and	10,00,000 10,00,000
67B	Publishing or transmitting material containing Children in Sexually Explicit Act - 1st time Subsequent	5 years and 7 years and	10,00,000 10,00,000
67C	Contravention of Retention or preservation of information by intermediaries	3 years and	Not Defined
68	Controller's directions to certifying Authorities or any employees failure to comply knowingly or intentionally	2 years or/and	100,000

Reach us: 8281223366
JOIN NOW

69	Failure to comply with directions for Intercepting, monitoring or decryption of any info transmitted through any computer system/network	7 Years and	Not Defined
69A	Failure to comply with directions for Blocking for Public Access of any information through any computer resource	7 Years and	Not Defined
69B	Failure to comply with directions to Monitor and Collect Traffic Data	3 Years and	Not Defined
70	Protected system. Any unauthorised access to such system	10 years and	Not Defined
70B (7)	Failure to provide information called for by the *I.C.E.R.T or comply with directions	I year or	1,00,000
71	Penalty for Misrepresentation or suppressing any material fact	2 years or/and	100,000
72	Penalty for breach of confidentiality and privacy of el. records, books, info.,etc without consent of person to whom they belong.	2 years or/and	100,000
73	Penalty for publishing False Digital Signature Certificate	2 years or/and	100,000
74	Fraudulent Publication	2 years or/and	100,000

- The criminal activity done by using computer, Internet, or advanced technology
- Cyber crimes are offenses committed using information communication technology devices like computers, the internet, and mobile phones.

super notes.
by CIVILIANZ
TRUST THE PROCESS

Hacking

- Unauthorized access in a computer or network is called hacking.
- The process of gaining unauthorized access to a computer or network and finding information.

Types of hackers

1. White hat hackers – Ethical hackers
2. Grey hat hackers – They hack sometimes for good reason and sometimes for malicious reasons.
3. Black hat hackers – Hacking for malicious reasons. They are also referred to as crackers.

IT ACT Section 66 – Hacking

Cyber cracking

- Destroying confidential files through hacking.

Data Theft

- The act of trespassing into a computer or network with malicious intent and stealing information from it.
- The act of transferring information from one computer to another using CD, DVD, pen drive, etc., without permission.

Reach us: 8281223366
JOIN NOW

Snooping

- Unauthorized access to another person's or company's data.
- The process of gaining unauthorized access to another individual's or company's data.

PHISHING

- A scam that attempts to obtain sensitive information such as USERNAME, PASSWORD, credit card details, etc.
- Vishing (Voice Phishing): Phishing via voice calls (phone scams).
- Smishing (SMS Phishing): Phishing via SMS (SMS scams).

Pharming

- With the help of a malicious code misdirecting users to fraudulent websites without their knowledge or consent is known as Pharming.
- The process of redirecting users to fake websites with the help of malicious code without their knowledge or consent.

E-mail Spoofing

- Sending e-mail to another person in such a way that it appears like the e-mail was from someone else.
- The act of sending an email in such a way that it appears to be from another person using a fake email address.

Reach us: 8281223366 JOIN NOW

E-mail spamming

- It is also known as Junk mail (SPAM).
- Sending unwanted bulk emails (mainly advertisements).
- This is also known as Junk mail (SPAM).

Email bombing

- The act of sending thousands of emails to a person's email account to crash it.
- It is a type of DOS attack.
- In cyber terminology DOS stands for Denial of Service.

Cyber Squatting

- The act of creating fake websites and addresses, misleading people into believing they are official or authentic websites.

Cyber stalking

- Harassing an individual or group using a computer or the internet. This is also known as cyberbullying.

Reach us: 8281223366
JOIN NOW

Cyber Slacking

- Using the employer's internet or email for personal purposes during working hours. Employees who use company resources in this manner are known as cyber slackers.

Cyber defamation

- An act intended to harm the reputation of an individual or an organization.

Cyber Forgery

- Creating fake documents using a computer (e.g., certificates, currency, stamps, IDs, etc.).
- Eg; Certificates, currency, stamps, ids etc.

Salami attack

- A financial cybercrime where bank employees use a program to debit small amounts from account holders' accounts. These small attacks collectively become a large attack, making it difficult to detect.

Cyber vandalism

- The act of destroying or damaging data or information stored on a computer.

Reach us: 8281223366 JOIN NOW

Cyber vandals: Those who destroy information and infrastructure for entertainment or pleasure.

Intellectual Property Right

- Intellectual property infringement is the violation of an intellectual property right.

Intellectual property right violation includes

1. Trademark violation
2. Software piracy
3. Patent violation etc.

- World Intellectual Property Day - April 26
- World Computer Security Day – November 30
- World Computer Literacy Day – December 2
- World Telecommunication Day – May 17
- Internet Security Day – February 6
- Internet Security Day – February 6 (Repeated, likely an error in original)

Password Sniffer

- Programs that record a user's username and password during login.

Data diddling

- A crime of deliberately altering data before it is input into a computer or before the output.

Reach us: 8281223366 JOIN NOW

Web jacking/ web hijacking

- The act by hackers of taking control of someone else's website.

Website defacement

- Website defacement is an attack on a website that changes the visual appearance of the website or a web page.

SPAM

- Unwanted or non-requested e-mails received in a folder is known as Spam.

SPIM

- Unwanted Instant Messages (Spam over Instant Messages).

CYBER TERRORISM

- Activities conducted through cyber means against the unity, sovereignty, and security of the country.

Reach us: 8281223366 JOIN NOW

super notes.
by CIVILIANZ
TRUST THE PROCESS

Intrusion problem (Access Attack)

- The method by which an authorized user accesses highly confidential data.

SOFTWARE PIRACY

- The act of illegally copying software.

Data Diddling

- The crime of deliberately altering data when it is input into a computer, or before it is input.

Operation P. Hunt - A project launched by Kerala Police to prevent the circulation of child pornography on the internet.

INDIA'S FIRST

1. First cyber court in India – Delhi
2. First cyber post office in India – Chennai
3. India's first cyber forensic laboratory was situated in – Tripura
4. First cyber crime Police station in India - Bengaluru
5. First cyber Police station in Kerala – Pattom
6. First e – state in India - Punjab
7. First Digital state in India – Kerala
8. First digital district in India – Nagpur (MH)
9. First cyber village in India – Melli Dara Paiyong (South Sikkim)
10. First minority cyber village in India – Chandoli (Rajasthan)

Reach us: 8281223366
JOIN NOW

IMPORTANT SOURCES USED

- **Social Science (Class VIII – Civics)**
- **Class VIII - IT Textbook**
- **Class X - IT / ICT Textbook**
- **Class XII – Computer Application / Computer Science**

PRACTICE QUESTIONS

1. Which are the correct statements about phishing?
Attempt to obtain sensitive information like passwords.
Vishing (Voice Phishing) - Phishing via voice calls.
Smishing (Smishing) - Phishing via SMS.
(A) 1 only
(B) 2, 3 only
(C) 1, 2, 3
(D) 1, 2 only
Answer: (C) 1, 2, 3

2. Identify the correct statements from the following:
Pharming redirects users to fake websites.
Email spoofing - Sending an email that appears to be from someone else.
Email bombing - The act of sending only one or two emails.
(A) 1, 2 only
(B) 1 only
(C) 2, 3 only
(D) 1, 2, 3
Answer: (A) 1, 2 only

Reach us: 8281223366
JOIN NOW

3. Which of the following statements about hacking is correct?
Hacking is unauthorized access to a computer or network.
White hat hackers = Ethical hackers.
Grey hat hackers always act with malicious intent.
(A) 1, 2 only
(B) 1 only
(C) 2, 3 only
(D) 1, 2, 3
Answer: (A) 1, 2 only
4. Sending an email in such a way that it appears to be from someone else is known as _____.
(A) Email spoofing
(B) Email bombing
(C) Email spamming
(D) Pharming
Answer: (A) Email spoofing
5. A financial crime that causes a big loss by moving small amounts from bank accounts is known as _____.
(A) Cyber defamation
(B) Salami attack
(C) Cyber squatting
(D) Cyber vandalism
Answer: (B) Salami attack
6. The act of illegally copying software is known as _____.
(A) Data diddling
(B) Spoofing
(C) Software piracy
(D) Software hacking
Answer: (C) Software piracy

Reach us: 8281223366
JOIN NOW

7. Consider the statements related to the IT Amendment Act 2008 and find the correct ones:
i) It was passed by Parliament on December 23, 24, 2008.
ii) It received the President's assent on February 5, 2009.
iii) It came into force on October 27, 2009.
iv) It contained 14 chapters, 124 sections, and 2 schedules.
(A) i, ii, iii only
(B) i, iii, iv only
(C) ii, iii, iv only
(D) All are correct
Answer: D

8. Identify the correct statements regarding Electronic Records in the IT Act:
i) Section 3 – Legal recognition of electronic records.
ii) Section 5 – Legal recognition of digital signatures.
iii) Section 7 – Retention of electronic records.
iv) Section 10 – Rules regarding electronic signatures.
(A) i, ii only
(B) i, ii, iii only
(C) ii, iii, iv only
(D) All are correct
Answer: D

9. Consider the statements related to cyber crimes and punishments and choose the correct ones:
i) Hacking is punishable with imprisonment up to 3 years or a fine of ₹5 lakhs.
ii) Identity theft is punishable with imprisonment up to 3 years and a fine of ₹1 lakh.

Reach us: 8281223366
JOIN NOW

iii) Cyber terrorism is punishable with life imprisonment.
iv) Publishing Obscene material under Section 67 is punishable with imprisonment up to 3 years and a fine of ₹5 lakhs for the first offense.
(A) i, ii, iii only
(B) ii, iii, iv only
(C) i, iii, iv only
(D) All are correct
Answer: D

10. How many chapters were initially included in the IT Act 2000?
(A) 12
(B) 13
(C) 14
(D) 15
Answer: B