

## Unit 5: Cyber Law:-

Meaning, Types of Crimes, Punishment.

The Parliament of India has passed the "The Information Technology Act, 2000. And cyber laws are the part of the Information Technology Act-2000.

The Act provides the legal infrastructure for e-commerce in India by accordinig Legal sanctity to all electronic records and other activities carried out by electronic means.

Meaning of Cyber Law:

Cyber law refers to those laws which are concerned with communication & automatic control systems.

Meaning and Definition of Cyber Crime.

Cyber crime involves the use of computer and network in attacking computers & networks as well.

① Cyber crimes may be defined as "any crime committed with the help of computer or any Telecommunication Technology, with a view to influencing functioning of computers or the computer systems".

The Cyber Crimes are punished by the provisions of Information Technology Act-2000.

② A Cyber crime is an "unlawful act wherein the computer is either a tool or a target or both". Thus Cyber Crimes are defined as "acts that are punishable by the Information Technology Act".

(15 marks question)

## Kinds Of Types of Cyber Crimes & Punishments

These are many kinds of cyber crimes that are likely to be committed by the cyber criminals who can be classified as 'hackers', 'information merchants' and mercenaries, 'terrorists', extremists and deviants. The following are the some kinds of cyber crimes.

### 1) Hacking

Hacking involves the partial or complete acquisition of certain functions within a system, network or website. It also aims to access to important data and information, breaching privacy or destroy or deletes or alter any information residing in a computer system.

Whoever commits hacking is punished with imprisonment upto three years or with a fine upto two lakh Rupees, or with both.

### 2) Cracking

The term 'Cracking' means 'illegal access' means gaining entry into instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network. However, 'access' includes entering of another computer or computer system where it is connected with public communication network on a same network (LAN).

### 3) Fraud on the Internet

Fraud on the internet is a form of white collar crime. Fraud is a general term used to describe a cybercrime that intends to deceive

a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing or suppressing any information to secure lawful or unfair gain.

#### 4) Identity theft:

Identity theft is a specific form of fraud in which cybercriminals steal personal data, including password, date about the bank A/c, credit cards, social security and other sensitive information.

#### 5) E-mail Scams:

E-mail containing useless and bogus information, known as junk mail is easy to create and therefore, fraudulent people very often find it easy to spread bogus investments schemes or spread false information about the securities of a company.

#### 6) Tampering with Computer Source Documents:

Section 65 of the Act providing that if any person knowingly or intentionally conceals, destroy or alters the information, he shall be punishable with imprisonment up to 3 yrs or with fine which may extend up to 2 lakh or with both.

#### 7) Publishing of information, which is obscene in electronic form.

Section 67 of the Act, provides for publishing punishment for publishing or transmit in electronic form any material which is obscene, with 5 year imprisonment or with fine up to 1 lakh or with both.

### 8) Publishing false Digital Signature :

Section 73 of the Act, if a person knows that a digital signature certificate is erroneous in certain particulars & still goes ahead & publishes, he shall be punishable with imprisonment for 2 yrs or with a fine up to 1 lakh or with both.

### 9) Computer viruses :

Most criminals take advantage of virus to gain unauthorised access to system & steal important data. Mostly, high skilled programmes sends viruses, malware and Trojan among others to infect and destroy computers, network & system.

### 10) Spamming :

Spamming uses electronic messaging systems, most commonly email in sending messages that host malware, fake links of websites, and other malicious programs.

### 11) Phising :

Phishers act like a legitimate company or organisation. They use "email spoofing" to extract confidential information such as credit card numbers, security number, password etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

### 12) Cyber stalking :

Cyber stalking involves following a person online anonymously. The stalker will virtually follow the victim, including his/her activities. Most of the victims of cyber stalking are women & children being followed by men & pedophiles.

### 13) Software Piracy:

The internet is filled with torrents & others programs that illegally duplicate original contents, including songs, books, movies, albums & software. This crime is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

### 14) Child Pornography:

Porn content is very accessible now because of the internet. Most countries have laws that penalise child pornography. Basically this cyber crime involves the exploitation of children in the porn industry.

### 15) Internet Protocol Spoofing:

An Internet Protocol (IP) attack takes place when an attacker outside the network pretends to be trusted computer either by using an IP address which is within its range or by using an external IP address to which you wish to provide access to specified resources on your network.

Penalty for all these cyber crimes are defined by the Information Technology Act 2000. Imprisonment up to 2 to 5 yrs or with fine of Rs 1 to 5 Lakh or with both.