CYBER CRIME

The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. Defining cybercrimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cybercrimes, such as email spoofing and cyber defamation, sending threatening emails etc.

A simple yet sturdy definition of cybercrime would be "unlawful acts wherein the computer is either a tool or a target or both". Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers.

- **Cyber crimes** are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.
-
- **Classifications Of Cyber Crimes:** Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber crime and what is the conventional crime so to come out of this confusion, cyber crimes can be classified under different categories which are as follows:

1. **Cyber Crimes against Persons:**

- Harassment via E-Mails: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.
- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here an offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.

- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

. Crimes Against Persons Property:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence.
- The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.

- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another.
- Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person.
- These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer.
- Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network.
- They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person.
- The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.
- You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

. Cybercrimes Against Government:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc.
- Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage(spying). It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

- **Cyberterrorism** is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation.
- It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Cybercrimes Against Society at large:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.

- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Cyber laws

- Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days.
- To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T.
- The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes.
- The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

- Cybercrimes under the IT Act Tampering with Computer source documents - Sec.65●
- Hacking with Computer systems, Data alteration - Sec.66
- ● Publishing obscene information - Sec.67
- ● Un-authorized access to protected system Sec.70 Breach of Confidentiality
- ● and Privacy - Sec.72 Publishing false digital signature certificates - Sec.73
- ● 2. Cyber Crimes under IPC and Special Laws Sending threatening messages by email - Sec 503 IPC

- • Sending defamatory messages by email - Sec 499 IPC
- • Forgery of electronic records - Sec 463 IPC
- • Bogus websites, cyber frauds - Sec 420 IPC•
- Email spoofing - Sec 463 IPC
- • Web-Jacking - Sec. 383 IPC
- • E-Mail Abuse - Sec.500 IPC
- • 3. Cyber Crimes under the Special Acts Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- • Online sale of Arms Act•
-

Preventive Measures For Cyber Crimes:

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.

- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.

- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programmes by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.

- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cyber crime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

- **Conclusion:**
- Since users of computer system and internet are increasing worldwide, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world.
- Certain precautionary measures should be taken by netizens while using the internet which will assist in challenging this major threat Cyber Crime.
-