Cybercrime

The world is more interconnected today than ever before. The use of computers, Internet, mobile phones etc has revolutionised such interconnection of people. Further the dependence of people on the computers and Internet for e-governance, communication, fund transfer, e-commerce etc is growing. This inter connection of population and dependence on the technology, has many advantages, but such increased connectivity and dependence brings increased risk of cyber offences i.e., online fraud, cyber stalking, phishing etc. The scenario is the same in India and thus Indian netizens have become vulnerable to cyber crimes. However the law enforcement agencies (LEAs) in India have been increasing their capabilities and equipped to safeguard people against cyber crime, and thereby striving for a secure cyberspace in India.

What is Cybercrime?

The general meaning of cyber crime is unlawful activities wherein computer is used as a tool, target or both. For instance in a scenario where in 'A' has sent an obscene e-mail to 'B', then 'A' has used his computer to commit an offence. In this scenario computer is used as tool to commit cyber offence. Other scenario wherein 'A' has hacked the computer of 'B', then the target of cyber offence is the computer of 'B'. In the second scenario the computer is a tool on one side and on the other it is target of an offence. The other meaning of cybercrime is criminal activity done with the use of computers and / or Internet.

Classification of Cybercrimes:-

A detailed discussion on cyber crime is covered while discussing on different provisions of Information Technology Act. However, for a broad understanding cyber crimes can be classified as follows

1. **Cyber Crimes committed against persons** due to personal rivalry, vendetta etc:

- Under this category, offences like cyber stalking, circulation of e-mails, creating fake or obscene profiles over social networking media can be categorised.

    - ✓ Cyber staking is repeated use of the Internet or other electronic communication methods to harass or frighten someone.
      Acts like sending abusive, obscene or threat e-mails, posting the identities; his or her name, photo, phone numbers etc of the victims on obscene or x-rated websites.

      Further, acts like creating fake profiles over social networking websites with the identities of the victim like name, photo, phone numbers etc and adding them objectionable content.

2. **Cybercrimes against property** are committed to gain financial benefit.

   Under this category two major streams can be observed basing on the usage of technology. In cases of phishing, debit / credit cards, online cheating cases the usage of technology is minimum but mostly the victim are deceived to divulge information and pay amounts, Whereas, in some other offences like ransomware usage of technology in perpetrating the offence is high. This latter category also considered as cyber crimes against technology

- Phishing
    - ✓ Phishing is to acquire critical information such as Internet banking usernames, passwords often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication i.e., emails

- Debit, Credit Cards Frauds.
    - ✓ Theft and fraud committed using a payment cards, such as credit cards or debit cards. This involves identity theft that is stealing critical information i.e., card numbers, CVV, PIN numbers, card expiry date, name as appears on the card etc

pertaining to the Credit / Debit Cards by means of skimming, vishing (Tele phishing) etc

Skimming is the theft of payment card information through skimmer machines clandestinely placed at ATM centres, shops and establishments etc where the cards are swiped for legitimate transactions.

In Tele phishing (vishing) the victims are called over phone by scammers pretending legitimate representative of banks and luring the victims into thinking that they are speaking with a trusted organisation and thus sensitive information such as credit card details are collected and misused.

- Nigerian Fraud / Lottery Scam / Advance Fee Scam.
  - ✓ Online lottery / prize scam is promising the victim a significant share of a large sum of money in the form of prize / lottery, and to get the same the fraudster requires a small up-front payment. If a victim makes the payment, the fraudster goes on requiring further amounts on different pretexts like advance fee, fee to get NOC etc from the victim; the promised prize will never be paid because it does not exist at all.

- Romance & Dating Scam
  - ✓ A romance scam is a confidence trick involving feigned romantic intentions towards a victims, gaining their affection, and then using that goodwill to commit fraud

Cyber Crimes against technology:

It is to be noted that of late these offences are mostly committed for financial gain, hither to youngsters used to commit these offences to get recognition, to expose vulnerabilities etc but this is no more the situation. Particularly, the incidence of ransome ware, defacement of websites a variant of hacking is growing.

- Hacking
  - ✓ Hacking is exploiting the weaknesses or vulnerabilities in a computer system or computer network and gaining access to

such systems may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment etc.

- Denial of Service Attack
  - ✓ Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users.

- Virus and worm attacks etc
  - ✓ Virus and worm attacks are infecting the computer systems with malware may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment etc.

- Ransom ware
  - ✓ A type of malicious software designed to block access to a computer system until a sum of money is paid.

3. Cybercrimes against Intellectual Property Rights (IPRs).

In this offence Intellectual Property Rights are violated and IPR violation is the main offence. In these offences IT Act provisions are invoked along with the provisions of Copy Rights etc.

While classifying as above the intent is not to look-at cyber offences in such a compartmentalised manner, but the classification is only for simple understanding. In Police parlance various offences are grouped under different heads i.e., murder, murder for gain, robbery, theft etc. If the cyber crime is to be looked in that way, the grouping broadly can be one head for each section of law Section 65, 66 r/w 43, 66-B to 66-F, 67 and 67 B Information Technology Act, 2000. The same can be done in other manner also: 1. Source Code Tampering, 2. General Computer Related Offence like hacking, virus & worm attacks etc. 3. Identity Theft Cases, 4. Online Frauds, 5. Cases of Obscene Content and 6. Other Cyber Crime Cases.

***