COMPUTER AND COMMUNICATION TECHNOLOGY

ETHICS, PRIVACY AND SECURITY

COMPUTER CRIME

Introduction:

- Computer crimes involve illegal exploitation of the computer and communication technology for criminal activities.
- Computer crimes are criminal activities, which involve the use of information technology to gain an illegal or an unauthorized access to a computer system with intent of damaging, deleting or altering computer data.
- Computer crimes also include the activities such as electronic frauds, misuse of devices, identity theft and data as well as system interference.
- Computer crimes may not necessarily involve damage to physical property.
- They rather include the manipulation of confidential data and critical information.
- Computer crimes involve activities of software theft, wherein the privacy of the users is hampered.
- These criminal activities involve the breach of human and information privacy, as also the theft and illegal alteration of system critical information.
- The different types of computer crimes have necessitated the introduction and use of newer and more effective security measures.

Hacking:

- The activity of breaking into a computer system to gain an unauthorized access is known as hacking.
- The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called hacking.
- The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes.
- Another highly dangerous computer crime is the hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal

activities.

Phishing:

- Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source.
- Phishing is carried out through emails or by luring the users to enter personal information through fake websites.
- Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

Computer Viruses:

- Computer viruses are computer programs that can replicate themselves and harm the computer systems on a network without the knowledge of the system users.
- Viruses spread to other computers through network file system, through the network, Internet or by the means of removable devices like USB drives and CDs.
- Computer viruses are after all, forms of malicious codes written with an aim to harm a computer system and destroy information.
- Writing computer viruses is a criminal activity as virus infections can crash computer systems, thereby destroying great amounts of critical data.

Cyberstalking:

- The use of communication technology, mainly the Internet, to torture other individuals is known as cyberstalking.
- False accusations, transmission of threats and damage to data and equipment fall under the class of cyberstalking activities.
- Cyberstalkers often target the users by means of chat rooms, online forums and social networking websites to gather user information and harass the users on the basis of the information gathered.
- Obscene emails, abusive phone calls and other such serious effects of cyberstalking have made it a type of computer crime.

Identity Theft:

- This is one of the most serious frauds as it involves stealing money and obtaining other benefits through the use of a false identity.
- It is the act of pretending to be someone else by using someone else's identity as one's own.
- Financial identity theft involves the use of a false identity to obtain goods and services and a commercial identity theft is the using of someone else's business name or credit card details for commercial purposes.
- Identity cloning is the use of another user's information to pose as a false user.
- Illegal migration, terrorism and blackmail are often made possible by means of identity theft.