First Chapter Lesson-10: Ethical Use of ICT & Impact of ICT on Social Life.

At the end of this lesson-

- 1. You will be able to explain ethical uses of ICT.
- 2. You will be able to explain impact of ICT on social life.

Ethical Use of ICT:

Ethics is a set of moral principles that govern the behavior of a group or individual. Therefore, computer ethics is set of moral principles that regulate the use of computers. Some common issues of computer ethics include intellectual property rights (such as copyrighted electronic content), privacy concerns, and how computers affect society.

For example, while it is easy to duplicate copyrighted electronic content, computer ethics would suggest that it is wrong to do so without the author's approval. And while it may be possible to access someone's personal information on a computer system, computer ethics would advise that such an action is unethical.

Cybercrime:

Cybercrime encompasses any criminal act dealing with computers and networks. Additionally, cybercrime also includes traditional crimes conducted through the Internet.

Type of Cybercrime:

Computer Fraud: Intentional deception for personal gain via the use of computer systems.

Privacy violation: Exposing personal information such as email addresses, phone number, and account details, etc. on social media, websites, etc.

Identity Theft: Stealing personal information from somebody and impersonating that person.

Sharing copyrighted files/information: This involves distributing copyright protected files such as eBooks and computer programs etc.

Electronic funds transfer: This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.

Electronic money laundering: This involves the use of the computer to launder money.

ATM Fraud: This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.

Denial of Service Attacks: This involves the use of computers in multiple locations to attack servers with a view of shutting them down.

Spam: Sending unauthorized emails. These emails usually contain advertisements.

Cyber-attack:

A cyber-attack is an assault launched by cyber criminals using one or more computers against a single or multiple computers or networks. A cyber-attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cyber criminals use a variety of methods, including malware, phishing, ransom ware, denial of service, among other methods.

Hacking:

Hacking generally refers to unauthorized access into a computer or a network. Hacking can also refer to non-malicious activities, usually involving unusual or improvised alterations to equipment or processes. Or Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.

- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

The person engaged in hacking activities is known as a hacker. Hackers are usually skilled computer programmers with knowledge of computer security. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.
Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.

Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

Script kiddies: A non-skilled person who gains access to computer systems using already made tools.

Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

Spamming:

Spamming is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. The term spamming is also applied to other media like in internet forums, instant messaging, and mobile text messaging, social networking spam, junk fax transmissions, television advertising and sharing network spam.

Spamming (especially e-mail spam) is very common because of the economics. Spam advertisers have little to no operating costs and so need only a minute response rate to make a profit. Most spam are commercial advertising, but some contain viruses, adware, or scams.

Spoofing:

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

Phishing:

Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page (see “website spoofing”).

Plagiarism:

Plagiarism is the “wrongful appropriation” and “stealing and publication” of another author’s “language, thoughts, ideas, or expressions” and the representation of them as one’s own original work. Plagiarism is considered academic dishonesty and a breach of journalistic ethics.

Impact of ICT on Social Life:

There are many positive and Negative impacts:

<u>Positive Impact of ICT on Social Life:</u>

- ICT has brought the world together through social networking sites.
- ICT has made researching information easier, as information can be found by looking over the internet.
- Through social networking people can speak to family and friends from across the globe.
- ICT has created many jobs for the people who are able to communicate and work away from an office which has made working from home a more popular choice.

<u>Negative Impact of ICT on Social Life:</u>

- Children and Teenagers spend most of their free time using computers, which affects their social development as they will lack the social skills to speak confidently in school or work.
- ICT can also affect people’s personal health, as they aren’t getting enough exercise as they are spending most of their free time indoors on computers instead of going outside.
- Small local businesses are being affected by the effects of ICT as people would rather shop online which is causing smaller businesses that aren’t online to close down as they are losing revenue and can’t afford to stay open.
- Many older people are feeling pressured and overwhelmed with learning how to use new technology and with many services such as Banking, Bill

paying and shopping rapidly becoming internet based, some older people are struggling accessing these services.

- ICT has caused many legal impacts. Many media forms such as Movies and Music have become easily available across the internet, which has led to copyright material to become easy to steal.
- There are also ethical impacts to ICT. With personal information being stored on computers, personal privacy has become an issue.

Lesson Evaluation-

Knowledge Based Questions:

- a. What is software piracy?
- a. What is cybercrime?
- a. What is cyber-attack?
- a. What is hacking?
- a. What is spamming?
- a. What is spoofing?
- a. What is fishing?
- a. What is plagiarism?

Comprehension Based Questions:

- b. Explain the relation of hacking with ethics.
- b. “Hacking is unethical activities”-explain.
- b. “Cyber Crime is one kind of threat to the technology”-explain.
- b. “Implementation of ICT has made social life easy and modern” -explain.

Creative Questions:

Multiple Choice Questions: