TOPIC 8: SYSTEM SECURITY, ICT ETHICAL ISSUES&EMERGING TECHNOLOGIES

What is meant by system security?

This refers to safe guarding computer resources, ensuring data integrity, limiting access to unauthorized users, and maintaining data confidentiality.

Distinguish between data security and data corruption?

***Data Security** refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites*. While.

***Data corruption** refers to error or damages in data that may occur during reading, writing, processing, storage or transmission of said data which may introduce unintended/unwanted changes to the original data*.

Define the term a computer security risk.

This refers to any event or action that could cause a loss of damage to computer hardware, software, data, information, or processing capability.

Mention examples of security risks commonly experienced today.

- *Hardware theft*
- *Software theft*
- *Information theft*
- *Unauthorized access and use*
- *System failure*
- *Internet and network attacks.*

Define the term a computer virus.

A computer virus is a program designed specifically to damage, infect and affect other programs, data or cause irregular behavior to the computer.

Suggest the possible symptoms of a virus infected computer.

- *System slows down.*
- *System crushes and hangs up.*
- *Hard disk will not boot.*

- *Corrupted hard disk data.*
- *Program sizes keep changing.*
- *Computer programs take long to boot than normal.*
- *Files will not open.*

Why do people create computer viruses? Give four reasons

- *To take control of a computer and use it for specific tasks.*
- *To generate money.*
- *To steal sensitive information.*
- *To prove a point, to prove it can be done.*
- *To cripple a computer or a network.*

Explain any five examples of computer viruses that you know.

1. A boot sector virus

This executes when a computer starts up because it resides in the boot sector of a floppy disk or the master boot record of a hard disk.

2. A file virus

This attaches itself to program files, and is loaded into memory when the infected program is run.

3. A macro virus

This uses the macro language of an application (e.g., word processor or spread sheet) to hide the virus code.

4. A logic bomb

This is a virus that activates when it detects a certain condition.

5. A time bomb

This is a kind of logic bomb that activates on a particular date.

6. A worm

This copies itself repeatedly in memory or on a disk drive until no memory or disk space remains, which makes the computer stops working.

7. A Trojan horse

This is a program that hides within or looks like a legitimate program, but executes when a certain condition or action is triggered.

8. A polymorphic virus

This modifies its program code each time it attaches itself to another program or file, so that even an antivirus utility has difficulty in detecting it.

Explain the ways how computer viruses are activated

- *Opening an infected file*
- *Running an infected program*
- *Starting up the computer with an infected floppy disk, flash disk*

Suggest the ways how computer viruses are spread

- *Through E-mail attachments.*
- *Rogue websites. E.g. some adult sites, gambling sites, e.t.c.*
- *Sharing infected disks.*
- *Through networks.*
- *Through infected software.*
- *Hackers.*
- *Through downloads from the internet.*
- *Through software updates*

Explain the possible ways of protecting data from viruses in a computer system.

- *Save your work*
- *Make a back-up of all important files.*
- *Always update your software.*
- *Perform regular maintenance.*
- *Scan all disks from other computers.*
- *Protect your password and change it after some time.*

Discuss the precautions that can be applied in order to prevent virus infection.

- *Ensure that the e-mail is from a trusted source before opening or executing any e-mail attachment.*
- *Install an antivirus utility and update its virus definitions frequently for detecting and removing viruses.*
- *Never start up a computer with a floppy disk in the floppy drive.*

- *Scan all floppy disks and files for possible virus infection before opening them*
- *Set the security level for macros in an application so that the user can choose whether or not to run potentially unsafe macros.*
- *Write-protect the recovery disk before using it.*
- *Back up important files regularly.*
- *Ensure that there is a policy of how computers are used and protected.*

Define the term a computer crime?

This is the crime illegal or unauthorized use of computer technology to manipulate critical user data.

OR

It refers to any crime that involves a computer and a network.

Explain the meaning of the following computer crimes.

1. ***Hacking***

Breaking into a computer system without unauthorized access.

2. ***Phishing***

The act sending emails to people with the aim of attempting to acquire sensitive information such as username, password by disguising as a trustworthy source.

3. ***Malware such as viruses***

These replicate themselves and harm a computer system or network without user's knowledge.

4. **Cyber stalking**

This is using technology e.g internet to send threatening e-mails, spread false information.

5. Identity theft

Act of pretending to be someone else by using another person's identity.

6. Computer industrial espionage

Involves stealing of trade secrets or spying through tech means for bribery, blackmail, etc

7. Software piracy

The illegal act of duplicating copyrighted software.

8. Phreaking

The act of illegally breaking into a communication system to make calls without paying

10 Unauthorized use

This is the use of a computer or its data for illegal/unapproved activities.

11 Spoofing

Is a malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

12. Unauthorized access.

This refers to the use of a computer system without permission from the owner.

13. Pharming

This is the fraudulent practice of directing internet users to fake/bogus/wrong websites that mimics/resembles the appearance of a legitimate one in order to obtain personal information.

*14**. Spamming***

Sending of unwanted e-mails.

15. ***Knowingly selling***

Is the act of distributing and selling child pornography

Explain the measures that are intended to control computer crimes.

- *Never open suspicious documents.*
- *Do not give out personal information to people you don't know.*
- *Sensitization. (learn about computer crimes)*
- *Use strong passwords on your accounts that are difficult to guess.*
- *Keep watch over what children do and how they use the internet.*
- *Shop only from secure websites.*
- *Use firewalls to protect your computer from hackers.*
- *Don't go on opening unknown websites*

Distinguish between a computer ethics and computer code of conducts.

Computer Ethics *refer to a set of moral principles that regulate the use of computers. OR The human values and moral conduct relating to right and wrong decision made when using computers. While*

A code of conduct *is a written guideline that helps determine whether a specific action is ethical or unethical*

Give the common unethical computer codes of conduct

- *Modifying certain information on the internet*
- *Selling information to others without the owners permission.*
- *Using information without authorization*
- *Invasion of privacy*
- *Involving in the stealing of software*

State the computer ethics that can be put in place

- *Respect the privacy of others.*

- *Always identify the user accurately*
- *Respect copyrights and licenses*
- *Respect the intellectual property.*
- *Respect the integrity of the computer system.*
- *Exhibit responsible and sensible use of hardware and software.*

Describe what is meant by access control.

This is a security measure that defines who can access a computer, when the users can access the computer, and what actions the users can take while accessing the computer.

Explain the two-phase process of access control of a computer.

- **Identification-** *verifies whether the user is a valid one.*
- ***Authentication*** *-verifies that the user is really the one he or she claims to be.*

What are the four methods of identification and authentication exist

- *User names and passwords*
- *Possessed objects*
- *Biometric devices*
- *Call back system*

Define the term a password

A password is a string of characters that allows access to a computer, interface, system or network.

Explain the following terms

A possessed object *is any item that a user must carry to gain access to a computer or computer facility.e.g. badges, cards, keys. Possessed objects are often used in combination with personal identification numbers.*

A personal identification number (PIN) *is a numeric password, either assigned by a company or selected by a user.*

A biometric device *authenticates a person's identity by verifying personal characteristics (e.g., fingerprints, iris, thumb).*

State the commonly used examples of biometric devices

- **A fingerprint scanner**, *which captures curves and indentations of a fingerprint.*
- **A hand geometry system,** *which can measure the shape and size of a person's hand.*
- **A face recognition system**, *which captures a live face image and compares it with a stored image.*
- A **voice recognition system**, *which compares a person's live speech with their stored voice pattern.*

- **A signature verification system**, *which recognizes the shape of handwritten signature of a person.*
- **An iris recognition system**, *which reads patterns in the tiny blood vessels in the back of the eye, which are as unique as a fingerprint.*

Distinguish between a call back system and system failure.

A call back system *connects a user to a computer only after the computer calls the user back at a previously established telephone number. While*

A system failure *is a prolonged malfunction of a computer that can also cause failure of hardware, software, data, or information loss.*

Give the causes of system failure that you know.

- *Aging hardware*
- *Natural disaster (e.g., fires, floods, storms, or earthquakes)*
- *Electrical power variation*

Explain the cause and prevention of the following computer health risks.

(a) Repetitive stress injury caused by

- *Prolonged typing*
- *Prolonged mouse usage*
- *Continual shifting between the mouse and the keyboard*

Prevention

- *Take frequent breaks during the computer session to exercise the hands and arms.*
- *Place a wrist rest between the keyboard and the edge of the desk.*
- *Place the mouse at least six inches from the edge of the desk.*
- *Minimize the number of times to switch between the mouse and the keyboard***.**

2. Eyestrain

3. Lower back pain

4. Muscle fatigue

5. Emotional fatigue

Prevention

- *Pay attention to sitting posture.*
- *Take a break to stand up, walk around, or stretch every 30 to 60 minutes.*
- *Place the display device about an arm's length away from the eyes with the top of the screen at eye level or below.*
- *Adjust the lighting in the room.*

- *Ensure that the workplace is designed ergonomically.*
- *Ergonomics means incorporating comfort, efficiency, and safety into the design of items in the workplace.*
- *Some keyboards have built-in wrist rests.*

Explain what is meant by the term Software Piracy.
This is the illegal duplication and distribution of copyrighted software.
Give two dangers of software piracy to the user.

- *Leads to loss of income.*
- *Can lead to imprisonment of the offender.*
- *Leads to spread of computer viruses.*
- *Does not allow getting support from the software developer or service centre.*

What are the ways software piracy can be controlled in our society?

- *Copy protection system.*
- *Separate demo and full version.*
- *Online game features or online registration.*
- *Give discounts or lower the product price.*
- *Legal action.*
- *Enforce copy rights*

What is a virus signature/definition?
This refers to a string of characters or numbers that makes up the signature that anti-virus programs are designed to detect. Or
It is a set of unique data, or bits of code that allow the virus to be identified by anti-virus programs.

Define the term antivirus program
This refers to a software program that is designed to detect, and remove malware and viruses from the computer.
Mention three examples of antivirus programs

- *Avira*
- *AVG*
- *Bitdefender*
- *Avast*
- *Lavasoft Ad-ware Free*
- *eScan Anti-virus*
- *Trend Micro HouseCall*
- *Malwarebytes Anti-Malware*

- *Panda Free Anti-Virus*
- *ZoneAlarm*
- *Kaspersky*
- *Smadav.*

Differentiate between unauthorized access and unauthorized use of computer systems

Unauthorized access *is the use of a computer or a network without permission****.*** *While.*

Unauthorised use *is the use of a computer or its data for un approved or possibly illegal activities.*

Differentiate between brownout and blackout

A brownout –This refers to intentional or unintentional reduction, drop, decrease in voltage in an electrical power supply. While

A blackout refers is a complete interruption/loss of power in a given service area.

Describe what is meant by emerging technologies?

These refer to new and advanced technologies that are currently developing or will be developed over the next five to ten years and which will substantially alter business and social environment. These may include Information Technology, wireless data communication, on demand printing, bio-technologies, and advanced robotics.

Explain the following terms as used in emerging technologies.

(a) Artificial intelligence

This refers to the creation and development of computers systems able to perform tasks that normally require human intelligence such as visual perception, speech recognition, decision making and translation between languages.

It can also mean an area of computer science that emphasizes the creation of intelligent machines that work and react like humans.

It can also be defined as the simulation of human intelligence by machines.

(b) Digital forensics

This refers to the process of investigating and recovery of evidence/material using digital devices left on crime scenes.

Suggest the benefits of emerging technology.

- *It allows you express your ideas so that others can learn from you.(Blogs)*
- *New technology connects you with people who are very far away from you.(Whatsapp, Facebook, Skype*
- *Allows people to learn and get entertainment in modern and advanced ways*
- *Responds to problems in the society.*
- *Leads to creativity and innovation in business*
- *Allows competition in the society.*

Suggest five limitations of emerging technology.

- *They contribute to environmental degradation*
- *They associated with health risks.*
- *They are expensive to maintain by the people e.g 4G internet.*
- *Requires a lot technical knowledge.*
- *Contributes to information theft and identity theft*