MODERN TRENDS IN COMPUTING

SYSTEM SECURITY

- The rise of technology is responsible for the violence, terrorism, crime and violation of privacy in the world today.
- There is need to protect computers, data and confidential information. The three major security principles are; **confidentiality, integrity** and **availability.**
- **Confidentiality** means sensitive data should not be disclosed to unauthorized people.
- **Integrity** mean data should not be altered without the owner permission.
- **Availability.** Means data is available on demand but only right users.

COMPUTER SECURITY THREATS

These are events or actions that may damage computer resources i.e. threats originate from;

1. System failure.
2. Malware
3. Privacy and confidentiality
4. Physical Hardware and software theft
5. Fraud
6. Sabotage

SYSTEM FAILURE

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

- Hardware failure due to improper use.
- Unstable power supply
- Network breakdown
- Aging hardware
- Natural disaster (e.g., fires, floods, storms, or earthquakes)

HOW TO PREVENT SYSTEM FAILURE

- Protect computer systems against dangers of unstable power by installation of surge protector or UPS.
- Backup all important data on alternative storage.
- Install lightening arrestors
- Replace aged hardware from time to time.
- Have a recovery policy

EXERCISE

- What is information security?
- Differentiate between private and confidential data
- Define the following; threat, risk, vulnerability, security control measure
- Explain any four threats to information systems
- What is system security and what measures can be put in place to guard against it?
- Explain five causes of system failure

MALICIOUS CODE (MALWARE)

- **Malware:** ***This refers to dangerous software that attacks and poses threat to unprotected computers*****. These malicious codes include;**
  - **viruses,**
  - **worms,**
  - **Trojan horses,**
  - **Bots, etc.**

  A computer virus is a computer code or program specially designed to damage or cause irregular behavior in other programs in a computer

CLASSIFICATION OF VIRUSES

- Viruses are classified according to their way of hiding. Some viruses are **stealth** because of the way they hide while others are **polymorphic** because they camouflage themselves to avoid virus removers (antivirus) from detecting them.

CLASSIFICATION OF VIRUSES

1	TYPE OF VIRUS	DESCRIPTION
2	**Boot sector viruses**	execute when a computer starts up.
3	**Portion sector viruses**	attack the partition sector (first sector on a hard disk which contains information about the disk specifications) of the hard disk and causes the computer not to boot fully.
4	**File viruses**	viruses that attach themselves to program files and are loaded into memory whenever the infected program is run
5	**Overwring viruses**	viruses infect files by overwriting the entire or part of a file thereby causing the file not to execute or work as it is supposed to do.
6	**Macro viruses**	virus uses the macro language of an application (e.g. Word processing, Spreadsheet) to hide the virus code
7	**Companion viruses**	virus that works by creating a different file name with an extension**.com**.
8	**Multi partite viruses**	use a combination of techniques to infect the different executable files, boot sectors and or partition sectors

CHARACTERISTICS OF COMPUTER VIRUSES:

1. Cannot exist in a viable form, apart from another (usually legitimate) program.
3. Propagates when the host program is executed.
4. Has an incubation period, during which no damage is done.
5. After incubation period, begins to manifest its behavior.

HOW VIRUSES ARE TRANSMITTED?

1. Through gradual downloading of infected e-mail attachments.
2. By sharing network resources like files, folders, etc..
3. Using infected boot disks.
4. Installing infected application programs like computer games.
5. Gradual sharing of storage media like compact discs, hard disk, flash disc, e.t.c.
6. Phishing schemes like spamming, e.t.c.

SYMPTOMS OF INFECTED COMPUTERS

- The computer files are deleted without notice.
- Some computer files get corrupted.
- The computer becomes slow.
- The computers freeze most of the times.
- The file sizes increase abnormally.
- Some computer files do not open or even respond at all.
- Some software work abnormally or don't respond at all.
- Some computers fail to start.
- Some hardware especially screens flicker.

FUNCTIONS OF ANTIVIRUS PROGRAMS

What anti viruses do?

1. **They clean infected computer files.**
2. **They delete un healable computer files.**
3. **They quarantine / vault computers files infected with dangers programs.**
4. **They scan computer files stored in a computer.**
5. **They provide notification to users concerning status of computer files.**

EXAMPLES OF ANT VIRUSES

1. Avira anti virus program.
2. Panda anti virus program.
3. Norton anti virus program.
4. Bull Guard anti virus program.
5. Komodo anti virus program.
6. kaspersky anti virus program.
7. Penicillin anti virus program.
8. Doctor Solomon tool kit program.

DANGERS OF COMPUTER VIRUSES:

- They delete computer files.
- They corrupt computer files.
- They make a computer become slow.
- They make the computer freeze most of the time.
- They increase file size.
- They make computer files not to open and respond.

CONTROLLING COMPUTER VIRUSES

a) Ensure that the e-mail is from a **trusted source** before opening or executing any e-mail attachment.
b) Install an antivirus utility and update its **virus definitions** frequently for detecting and removing viruses.
c) Never start up a computer with a floppy disk in the floppy drive.
d) Scan all floppy disks and files for possible virus infection before opening them.
e) Set the security level for macros in an application so that the user can choose whether or not to run potentially unsafe macros.

CONTROLLING COMPUTER VIRUSES

f) Write-protect the recovery disk before using it.

g) Back up important files regularly.

EXERCISE

- Distinguish between computer security risks and computer security threats
- Give the categories of systems security risks you know
- What do you understand by the term network and internet attacks?
- Give the difference between malware and viruses
- Distinguish between polymorphic and stealth viruses
- Mention five types of computer viruses
- How are computer viruses spread and what caution would you give to computer users?
- What is the role of antivirus in data protection?

PRIVACY AND CONFIDENTILAITY

- Private and confidential data shouldn't be disclosed to unauthorized users
- **Privacy** means data belonging to an individual shouldn't be disclosed to others while **confidentiality** means sensitive data belonging to an individual should not be disclosed to unauthorized users.
- ***Unauthorized access*** is the use of a computer or network without permission, e.g. an employee using a company computer to send a personal e – mail
- ***Un authorized use*** is the use Of a computer or its data for unapproved activities.

The following are some of the common threats to privacy and confidentiality;

- **Eavesdropping** . This refers to tapping(listening) into communication channels to get information
- **Hacking and cracking**. A hacker is a user that gains unauthorized access to a computer system for fun while a cracker is a user that gains unauthorized access to a computer system for malicious reasons.
- **Social engineering**. This is the act of soliciting for sensitive information from unsuspecting people.
- **Industrial espionage**. This is spying on a competitor with an intention to cripple them.
- **Alteration**. This is illegal modification of private or confidential information with an aim of misrepresenting facts.

PREVENTION OF UNAUTORISED ACCESS

- Unauthorised access is prevented through use of **access controls**
- An access control is a security measure that defines;

a) Who can access a computer?
b) When the users can access the computer?
c) What actions the users can take while accessing the computer?

- Access control is normally implemented using a two-phase process:

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

PREVENTION OF UNAUTORISED ACCESS

- **Possessed objects:** A possessed object is any item that a user must carry to gain access to a computer resources. E.g. (PIN) (numeric password), keys, budges either assigned by a company or selected by a user.
- **Biometric devices:** authenticates a person's identity by verifying personal characteristics (e.g., fingerprints) using personal characteristic
- **Installation of security monitors like CCTVs**
- **Backing up** by a duplicating of a files
- **Encryption data sent across networks**
- **Installation of firewalls to filter communications**

PASSWORDS

A password is a combination of characters associated with a user name that allow a user to access a computer or a network. Password should be easy to remember, but not too obvious (e.g., birthday) so that others can guess it easily. Longer passwords provide greater security than shorter ones.

Qualities of a good password

- ***At least eight characters, if supported by the system.***
- ***A combination of mixed case letters and digits.***
- ***A password that can be typed easily without looking at the keyboard.***

Tips for safeguarding your password:

- ***Do not share your password with others.***
- ***Do not write down your password.***
- ***Change your password frequently***

HARDWARE THEFT & VANDALISM

Hardware theft is the act of stealing computer equipment. The act of defacing or destroying computer equipment is known as hardware vandalism.

Precautions to prevent hardware theft include

- Use physical access controls, such as locked doors, and windows.
- Employ security guards
- Use cables to lock the equipment to desk, cabinet, or floor.
- Install alarm systems for additional security.
- Never leave a notebook computer or handheld computer unattended in a public place.
- Use passwords, possessed objects, and biometrics as a method of security.
- Back up all the files stored on the computer regularly.
- Install surveillance cameras (CCTV).

EXERCISE

- Write a short note on the following

a) Spoofing b) sniffing c) phishing d) eavesdropping e) DoS

- Distinguish between the following
  - hacking and cracking
  - Private and confidential data
  - Unauthorized access and unauthorized use
  - Hacking and eavesdropping
  - Social engineering and eaves dropping
  - Encryption and decryption keys
  - Validation and authentication
- State some measures for preventing unauthorized access to systems
- Distinguish between a PIN and password
- What causes system failure
- Explain forms of power disturbances that may lead to system failure

ETHICAL AND LEGAL ISSUES

Definition:

- ✓ Ethical issues are general moral guidelines of conduct or behavior for computer systems acquisition, usage and disposal.
- ✓ Legal and ethical questions affect many areas of computing including privacy, sharing, hacking and the environment.

ETHICAL AND LEGAL ISSUES …

1. **Information Privacy**: Refers to the right of individuals or organizations to deny or restrict the collection and use of information about them.

2. **Sharing**: Deals with laws protecting the distribution of films and other media. It is illegal to rip a copyrighted DVD or CD and distribute it online.

ETHICAL AND LEGAL ISSUES …

3. **Hacking:** It refers to any activity which makes unusual use of, or attempts to break, a computer system. Hacking can be used for negative purposes such as looking for weaknesses in systems to access and steal private data, but it can also be used for positive purposes such as:

a) creatively exploring new ways of using a program or computer.
b) working around bugs in code.

ETHICAL AND LEGAL ISSUES …

c) exposing security risks in **software** and websites, and warning the general public
d) testing the security of a system
e) a 'hack day' - where people get together to explore new technologies.

Note: Hackers who attempt to do good through hacking are called 'white hats' but those that carry out criminal activity are called 'black hats'.

ETHICAL AND LEGAL ISSUES …

3) **Data protection:** It refers to how to keep data that it is only used in the right / safe way. The **Data Protection Act (DPA)** sets out principles that govern:

- ✓who can access data
- ✓the accuracy and validity of data
- ✓selling data
- ✓removal of data

ETHICAL AND LEGAL ISSUES …

4. **Sharing data online:** When we use personalized websites requiring logins, such as social media sites, we often add data about ourselves. Whenever we sign up to these sites we are agreeing to share a certain amount of personal data with the provider.

5. **Computer misuse:** As the use and importance of computer systems in society has increased, the opportunities to misuse them have also increased. These include:

ETHICAL AND LEGAL ISSUES …

- ✓ **Cyber bullying:** involves abuse of another person using threats, insults and hurtful remarks and messages over the internet. There have been numerous reports of people who have been driven to suicide by persistent cyber bullying.
- **Internet trolls:** post messages and comments that try to evoke an emotional response from other people. BBC presenter Richard Bacon and other celebrities have spoken about being victims of trolls.

ETHICAL AND LEGAL ISSUES …

- The Computer Misuse Act makes it an offence to:

✓ access computer material without permission, e.g. looking at someone else's files

✓ access computer material without permission and with intent to commit criminal offences, e.g. **hacking** into your bank's computer and increasing the money in your own account

✓ alter computer data without permission, e.g. writing a **virus** to destroy someone else's data

ETHICAL AND LEGAL ISSUES …

6. **The digital divide:** The gap between those who have access to the latest technology and those who do not is called the **'digital divide'**.

Some of the main causes of the digital divide:

- ✓ **Money** - people need money to access the internet and buy the latest devices, such as computers, **smartphones** and **tablets**.

ETHICAL AND LEGAL ISSUES …

- ✓ **Location** - Most large towns and cities have good network coverage and access, but rural areas can have limited or no coverage.
- ✓ **IT literacy** - knowing how to use technology empowers people to make the most of it. People who don't know how to use computers and the internet do not have the opportunities that IT-literate people do.
- ✓ **Internet access** - the internet provides many opportunities for people who want to access online shopping, banking and job adverts. Students with internet access at home can research or revise with online help.

ETHICAL AND LEGAL ISSUES …

7. **Computers and the environment:** The use of computers affects the environment in different ways, such as energy consumption, technological waste, and the impact of remote working.

Advantages:

- ✓ using email and working electronically means that less printing is required, and so less paper is used
- ✓ using systems like **FaceTime**, **Skype** and **video conferences** can reduce the need for people to travel to meet each other, and so less fuel is used

ETHICAL AND LEGAL ISSUES …

- ✓ people can work from home - which reduces commuting (less fuel is used) and means that less office space is needed.

Disadvantages:

- ✓ **Technology consumes energy**. Computers require electricity, and most **smartphones** and**tablets** require recharging after just a few hours of use.
- ✓ **Technological waste** - also known as e-waste - sometimes contains poisonous chemicals and can be an environmental hazard.

ETHICAL AND LEGAL ISSUES …

8. **Intellectual property rights:** Refers to work created by inventors, authors, and artists. **Intellectual property rights** are the rights to which creators are entitled for their work.

- **Copyright:** Copyright gives the creators of media the rights to control how media is used and distributed.
- ✓ Copyright law usually gives the public **fair use** to copyrighted material (e.g., for educational purposes)..

ETHICAL AND LEGAL ISSUES …

- **Patents**: gives authors and artists exclusive rights to duplicate, publish, and sell their materials.

- **A trademark** protects a company's logos and brand names. The controversy with trademarks often relates to domain names, when some people or smaller companies purposely acquire a domain name that uses the exact trademarked name of their competition.

ETHICAL AND LEGAL ISSUES …

9. **Piracy:** The un authorised use of another person's work is known as piracy.

✓ **Software piracy:** is any attempt to break the licence terms of a piece of software.

When you buy software, music or films legally, copyright law forbids you from:

- giving a copy to a friend.
- making a copy and then selling it.

ETHICAL AND LEGAL ISSUES …

- giving a copy to a friend.
- making a copy and then selling

Those who use pirate software:

✓ Increase the chances that the software will not function correctly or will fail completely;

✓ Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;

✓ Have no warranty to protect themselves;

ETHICAL AND LEGAL ISSUES …

- ✓ Increase their risk of exposure to a virus that can destroy valuable data;
- ✓ May find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;
- ✓ Are subject to significant fines for copyright infringement; and
- ✓ Risk potential negative publicity and public and private embarrassment.

ETHICAL AND LEGAL ISSUES …

10). **Information accuracy:** refers to the right of individuals or organizations to deny or restrict the collection and use of information about them.

ETHICAL ISSUES INCLUDE …

Ethical issues include:

1. Respect of computer ownership without recourse to laws.
2. Guarding against computer misuse.
3. Systems safety (Hardware, software, Data and users safety).
4. Systems privacy.
5. Environmental protection.
6. Respect for human dignity.
7. Usage with permission.
8. Shutting down the computer properly after use.

ETHICAL ISSUES INCLUDE …

- Virus alerts.
- Polite tone.

LEGAL ISSUES:

- Legal issues relate to a system of rules/laws and principles backed by sanctions governing computer system acquisition, usage and disposal.

CODE OF CONDUCT

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

Sample IT Codes of Conduct:

1. **Computers may not be used to harm other people.**
2. **Users may not interfere with other's computer work.**

CODE OF CONDUCT …

3. Users may not meddle in other's computer files.
4. Computers may not be used to steal.
5. Computers may not be used to bear false witness.
6. Users may not copy or use software illegally.
7. Users may not use other's computer resources without authorization.

CODE OF CONDUCT …

8. Users may not use other's output.
9. Users shall consider the social impact of programs and systems they design.
10. Users should always use computers in a way that demonstrates consideration and respect for other people.

EXERCISE

- Explain five ways in which computers are misused.
- Distinguish between legal issues and computer ethical issues
- Explain any five ethical and unethical issues considered while you use computers in the schools computer laboratory
- What are cyber crimes?. Explain any five common cyber crimes you know
- Distinguish between

a) copyright and patent rights
b) Copyright and intellectual property rights
c) Computer law and ethical issues.

- What is software piracy?
- State five ways of pirating software.
- Give five dangers of using pirated software.
- What is meant by the term green computing?

COMPUTERS AND SOCIETY

- Computers are nowadays used in almost all areas of life i.e.

1. Banking
2. Health
3. Business
4. Education
5. Security
6. Governance etc.

However, in all these areas they have had an impact

POSTIVE IMPACTS/EFFECTS

- Created and widened employment opportunities
- Improved education and research by simplifying teaching
- Improved entertainment and leisure
- Improved communication and collaboration
- Improved security management
- Improved service delivery
- Improved data and document productions
- Reduced production time and manufacturing processes

NEGATIVE IMPACTS/EFFECTS

- Increased crimes related to computers
- Increased moral degeneration
- Increased cost of production since hardware and software costs are high
- Increased health and environmental hazards
- Increased loss of employment
- Erosion of human integrity and creativity
- Increased cyber terrorism
- Increased death and accidents due to malfunction

EMERGING TECHNOLOGIES

- **ETs refers to technological innovations that are currently developing or becoming common with a potential to transform an industry or field.**
- **ETs usually have an impact on existing systems and their resources i.e. emerging technologies have an impact hardware , software in general and applications in particular as well as networks**

IMPACT OF ETS

- **ETs usually have an impact on existing systems and their resources i.e. emerging technologies have an impact hardware , software in general and applications in particular as well as networks,**

IMPACT OF ETS ON HARDWARE

- ICT devices have become more sophisticated (ipads, smartphones, laptops)
- Increased storage
- Increased Wireless connectivity (li-fi, wi-fi,)
- Devices become cheaper
- Improved output devices
- Increased sharing of storage space

IMPACT OF ETS ON SOFTWARE

- Increase in improved OS like win 10, android,
- Increased use of apps
- Advanced encryption techniques
- Advanced DBMS for big data storage
- Advanced software for cloud computing
- Increased advanced software for web services
- Sophisticated software for cellular communications (4G, 5G…)
- Increased use of AI in software design

EXAMPLES OF ETS

- Artificial intelligence
- Robotics
- Digital forensics
- Cloud computing
- Virtual reality
- Internet of things
- Green computing
- Cyber storage
- 4G cellular comm
- Language translation
- Qn answering

EMERGING TECHNOLOGIES

- **Artificial Intelligence**: this a branch of computer science concerned with making computers behave like humans. It is the capability of the machine to imitate intelligent human behavior. This includes game playing, expert system, natural language, robotics etc.
- **4G cellular communication**: the fourth generation of cellular communication system known as 4G it is the emerging technology of the current wireless network

EMERGING TECHNOLOGIES

- **Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information.**
- **Virtual reality: Uses computer technology to create the simulation of a real-world environment**

EMERGING TECHNOLOGIES

- **Machine translation:** is a sub field of that investigates the use of software to translate text or speech from one natural language to another.
- **Question answering** (QA): is a field that is concerned with building systems that automatically answer questions posed by humans in a natural language.

EMERGING TECHNOLOGIES

- **Internet of things**: refers Internet connected objects (things) working together to solve a business problem.
- **Cloud computing**: refers to use of internet to carry out all computing tasks as well as obtain services
- **Digital forensics** is a branch of investigative science around material found in digital devices, often in relation to computer crime

EXERCISE

- What are emerging technologies
- Explain any five emerging trends in IT
- Give five trending technologies in the field of education
- How do the emerging technologies affect;

a) Computer hardware

b) Computer software

- What is cloud computing? State five advantages of cloud computing.
- Explain the term cyber storage. State three examples

GREEN COMPUTING:

DEFINATION:

- Green computing is the environmentally responsible and eco-friendly use of computers and their resources.

GOALS OF GREEN COMPUTING:

1. **Green use**: Minimizing the electricity consumption of computers and their peripheral devices and using them in an eco-friendly manner.

GREEN COMPTUING CONT …

2. **Green disposal**: Re-purposing an existing computer or appropriately disposing of, or recycling, unwanted electronic equipment.
3. **Green design**: Designing energy-efficient computers, servers, printers, projectors and other digital devices.
4. **Green manufacturing**: Minimizing waste during the manufacturing of computers and other subsystems to reduce the environmental impact of these activities.

GREEN COMPTUING CONT …

NOTE: Average computer users can employ the following general tactics to make their computing usage more green:

1. Use the hibernate or sleep mode when away from a computer for extended periods.
2. Use flat-screen or LCD monitors, instead of conventional cathode ray tube (CRT) monitors.
3. Buy energy efficient notebook computers, instead of desktop computers.
4. Activate the power management features for controlling energy consumption.

GREEN COMPTUING CONT …

6. Make proper arrangements for safe electronic waste disposal
7. Turn off computers at the end of each day
8. Refill printer cartridges, rather than buying new ones
9. Instead of purchasing a new computer, try refurbishing an existing device

CYBER STORAGE:

DEFINATION:

- **Online data storage / cyber storage is a virtual storage approach that allows users to use the Internet to store recorded data in a remote network.**

Examples of online storage:

- **Skydive.**
- **Drop box.**

ADVANTAGES OF CYBER STORAGE:

1. **World Wide accessibility:** You can access your data anywhere in the world. You don't have to carry your hard disk, pen drive or any other storage device.
2. **Data safety:** In order to make your data safe from such hazards you can keep it online.
3. **Security:** Most of the online storage sites provide better security.
4. **Easy sharing:** you can share data with your friends' faster, easy and secure manner, which makes you can your close ones happy.

ADVANTAGES CONT …

5. **Data recovery:** online data storage sites provide quick recovery of your files and folders. This makes them more safe and secure.
6. **Automatic backup:** you can even schedule automatic backup of your personal computer in order to avoid manual backup of files.

DISADVANTAGES OF CYBER STORAGE

1. Improper handing can cause trouble: You must need your user-id and password safe to protect your data as if someone knows or even guess your credentials, it may result in loss of data.
2. Some storage sites out there do not provide adequate security checks.
3. One must be online to store or retrieve a file from the remote locations.

COMPUTER AND HEALTH RISKS

Prolonged computer usage can lead to health risks such as:

a) Repetitive stress injury, which include tendonitis and carpal tunnel syndrome.
b) Eyestrain.
c) Lower back pain.
d) Muscle fatigue.
e) Emotional fatigue.

ERGONOMICS…

Ergonomics means incorporating comfort, efficiency, and safety into the design of items in the workplace.

- ✓ Some keyboards have built-in wrist rests.
- ✓ Most display devices have a tilt-and-swivel base and controls to adjust the brightness, contrast, positioning, height, and width of images.
- ✓ Most CRT monitors today also adhere to the **MPR II standard**, which defines acceptable levels of electromagnetic radiation.

COMPUTER AND HEALTH RISKS …

Precautions to help prevent such risks include:

- ✓ 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.

SYSTEMS ANALYSIS

computer or information system is a collection of interrelated components that work together to process and provide information**.**

An information/computer system constitutes users of the system, hardware, software, data, and a communication network.

COMPUTER SYSTEM

- **Users are required for the operation of any information system. These include:**
- **End users; these include those who feed the system with data and those who use the information produced. E.g. Accounts, secretaries, students customers, managers, etc.**
- **Hardware resources of a system include all physical devices such as video screen, computers, cameras, etc. and storage media.**

WHAT IS SYSTEMS ANALYSIS

Systems analysis is the process of studying a business' information system in order to improve its efficiency in operation.
System analysis is a stage in a system development cycle of an enquiry of the problem that an organization will try to solve with an information system, which involves defining the problem, identifying its cause, specifying the solution and identifying the information requirements that must be met by a system solution.

IMPORTANCES OF SYSTEMS ANALYSIS

- To overcome failure rates of existing systems
- **The current system may be slow**
- **To address the complaints from clients of the organization**
- **To address decline in profits or performance**
- **To reduce costs of operation and maintenance**
- **To meet the requirements of new technologies.**
- **To increase the flexibility of the current system**

PHASES OF SYSTEMS DEVELOPMENT

1. Preliminary study
2. Feasibility study
3. System analysis
4. System design
5. Coding
6. Testing
7. Implementation
8. Maintenance

SDLC

PHASE	DESCRIPTION
Preliminary study	Involves preparing system proposals, problem defn, terms of reference and background analysis
Feasibility study	Involves examining whether the system is feasible in terms of available resources
Systems analysis	Involves collecting factual data, understand the processes involved, identifying problems and recommending feasible suggestions for improving the system functioning
System design	Involves modeling of the new system using tools like flow charts, DFDs, data dictionaries etc.
Coding	Involves writing code using a certain language
Testing	Involves checking the system for bugs and its functionality
Implementation	Involves installation and training of user
Maintenance	Involve giving support, updates, upgrades

EXERCISE

- Define a systems analysis.
- Distinguish between a systems analyst and systems analysis
- Describe the term system development life cycle
- Discuss five importances of system analysis in a systems development.
- Discuss the phase of systems development

CAREERS IN COMPUTING

- Information and communication technology (ICT) creates many jobs/professions such as **computer operators, computer technicians, system analysts, computer programmers, software engineers, computer engineers, information system manager, data base administrators, computer trainer, website administrators, computer graphic designers and network administrators, etc**

COMPUTER TECHNICIAN

- Trouble shooting computer hardware and software related problems

NB Trouble shooting. Troubleshooting is a logical, systematic search for the source of a problem so that the product or process can be made operational again.

- Assembling and upgrading computers and their components
- Ensuring that all computer related accessories such as printers, scanners modems storage media and other devices are in good working condition
- Install new programs needed by the company / organization
- Repair and maintain computers in working conditions

ICT TRAINER/INSTRUCTOR

- Training people on how to use various application programs
- Developing training reference material
- Guide learners on how to acquire knowledge through carrying out research
- Advising the learners on the best career opportunities in the broad filed of ICT
- Preparing learners for ICT certification examinations

DATABASE ADMIN (DBA)

- Designing and developing database applications for the organization
- Setting up security measures needed to control access to data and information
- Keeping the database up to date by adding new records, modifying or deleting unnecessary records
- Data backup from time to time
- Data recovery
- Database/DBMS upgrade
- Defining database user privileges

COMPUTER ENGINEER

- Design and develop computer components such as storage devices, motherboards and other electronic components
- Determine electronic power requirements for each component
- Design and develop engineering and manufacturing computers controlled devices such as robots, ATMs etc.
- Re-engineer computer components to enhance its functionality and efficiency
- Define hardware requirements for systems

SOFTWARE ENGINEER

- Developing system and application software
- Developing user and technical documentation for the new software
- Maintaining and updating the software to meet day to day requirements
- Upgrade system and application software
- Define system requirements
- Find and correct software bugs

SYSTEMS ANALYST

- Reviewing the current manual information system and making recommendations on how to replace it with a more efficient one.
- Working with programmers to construct and test the system
- Co-coordinating training for users of the new system
- Defining recommendation for the new system

WEB MASTER

- Developing and testing websites
- Maintaining , updating and modifying information on the websites to meet new demands by the users
- Monitoring the access and use of internet connection by enforcing security measures
- Identifying hosting companies for the website.

NETWORK ADMINISTRATOR

- Network administrators are responsible for building, maintaining, managing, and repairing an organization's computer networks.
- Network administrators handle a company's Local Area Networks (LANs), Wide Area Networks (WANs) and network segments, as well as manage the company's Internet and intranet systems.
- They must install and maintain hardware and software that supports an organization's networks, making sure everything is working the way it is supposed to be.
- Network administrators keep a sharp eye on network performance, taking steps to ensure user's needs are being met and repairing any problems that crop up.
- Network security is also a vital component of a network administrator's work, as they must establish a means of protecting the organization's networks from

EXERCISE

- Distinguish between a computer career and a profession
- Distinguish between systems analyst and a programmer
- State example of computer careers that you know
- Explain the responsibilities of the following

a) Network administrator

b) Database administrator

c) Systems analyst

- What career can u take up after your final exams in order to earn a living?