A-LEVEL SUBSIDIARY ICT NOTE

NAJJEMBE HOMELAND SEC SCHOOL

P.O.BOX 176, LUGAZI

For inquiry

Email: lukwagoshaban820@gmail.com

COMPUTER SYSTEM SECURITY, ICT ETHICAL ISSUES & EMERGING TECHNOLOGIES

- Sub Topic 1: Computer System Security
- Sub Topic 2: Privacy and ICT Ethical Issues
- Sub Topic 3: Emerging Technologies
- Sub Topic 4: ICT Industry

Sub Topic 1: Computer System Security

- **Computer security**
  Refers to safe guarding computer resources, ensuring data integrity, limiting access to unauthorized users, and maintaining data confidentiality.
- **Computer Integrity** refers to methods and procedures of ensuring that data is real, accurate and safeguarded from unauthorized user modification in the computer.
- **Information security** means protecting information and systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Forms of computer security (data and physical security)

- ***1. Data Security** refers to protective measures that are applied to ensure integrity, availability and confidentiality of data or information.*
- **Data Integrity** means prevention of unauthorized modification of data and data Corruption. *Data corruption refers to errors in data that may occur during reading, writing, processing, storage or transmission .*
- **Data Availability** means prevention of unauthorized withholding of data access (Intended users can access whenever they need to access).
- **Data Confidentiality** means to avoid unauthorized disclosure of data third parties

2. Physical Security

- Physical Security refers to the measures put in place by protect computer systems from physical damage and mitigate physical security risks. Physical security includes:

- Locked doors.
- Burglar proofs.
- Parameter fences.
- Security guards.
- Server room environmental protection, optimisation.
- Concrete walls.
- Lightening conductors.
- Fire extinguishers.
- Strategic server and storage placement, etc.

Security threats for (hardware and software)

- **A computer security risk** is an Action that causes loss of or damage to computer system. Security threats to computer-based information systems, private or confidential data include:

1. System Failure
2. Information Theft
3. Hardware Theft
4. Software Theft
5. Internet And Network Attacks Such Us Hackers
6. Malicious Programs (Computer Viruses, Worms And Trojan Horses)
7. Unauthorized Access and Use
8. Unauthorized Alteration,
9. Malicious Destruction of hardware, software, data or network resources, as well as sabotage.

System failure

- Some of the causes of computerized information system failure include:
- Hardware failure due to improper use.
- Unstable power supply as result of brownout or blackout and vandalism.
- Network breakdown.
- Natural disaster
- Program failure

Control measures against hardware failure

- Protect computers against brownout or blackout which may cause physical damages or data loss by using surge protectors and Uninterruptible power supply (UPS).
- For critical systems, most organizations have put into place fault tolerant systems. A fault tolerant system has redundant or duplicate storage, peripherals devices and software that provide a fail-over capability to backup components in the event of system failure.
- Disaster recovery plans. Disaster recovery plan involves establishing offsite storage of an organization's databases so that in case of disaster or fire accidents, the company would have backup copies to reconstruct lost data

Hardware theft and hardware vandalism

Hardware theft is act of stealing computer equipment

- Protect computer equipment from theft by using locks.

Some notebook computers use passwords, possessed objects, and biometrics as security methods

- For PDAs, you can password-protect the device

Hardware vandalism is the act of defacing or destroying computer equipment

Software theft

Software theft is the act of stealing or illegally copying software or intentionally erasing programs.

Software piracy is illegal duplication of copyrighted software.

- To guard against software theft and piracy, product activation is used.

Product activation allows user to input product identification number online or by phone and receive unique installation identification number.

A license agreement gives the right to use software. Single-user license agreement allows user to install software on one computer, make backup copy, and sell software after removing from computer.

Unauthorized access and Use

- **Unauthorized access** is the use of a computer or network without permission.
- **Unauthorized use** is the use of a computer or its data for unapproved or possibly illegal activities.
- Unauthorized use includes a variety of activities:

✓ an employee using an organization's computer to send personal e-mail messages,

✓ someone gaining access to a bank computer and performing an unauthorized transfer.

Information theft

- **Information theft** occurs when someone steals personal or confidential information.
- An unethical company executive may steal or buy stolen information to learn about a competitor.
- A corrupt individual may steal credit card numbers to make fraudulent purchases.
- Safeguards against Information Theft: Most companies attempt to prevent information theft by implementing the user identification and authentication controls.
- To protect information on the Internet and networks, companies and individuals use a variety of encryption techniques.

Internet and network attacks

- Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises.
- In an organization, network administrators usually take measures to protect a network from security risks. On the Internet, where no central administrator is present, the security risk is greater.
- Internet and network attacks that jeopardize security include: computer viruses, worms, Trojan horses, and rootkits; botnets; denial of service attacks; hackers, back doors; and spoofing.

Computer virus.

A computer virus is a potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the user's knowledge.

- Once the virus infects the computer, it can spread throughout and may damage files and system software, including the operating system.
- Computer viruses, worms, Trojan horses, and rootkits are classified as malware. (short for malicious software)

What is the difference between viruses, worms, and rootkit and Trojan horses?

Virus is a potentially damaging computer program

Can spread and damage files

Worm copies itself repeatedly, using up resources and possibly shutting down computer or network

A **rootkit** is a program that hides in a computer and allows someone from a remote location to take full control of the computer.

Trojan horse hides within or looks like legitimate program until triggered

Does not replicate itself on other computers

Computer Crimes

- **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.
- This is the criminal offence illegal or unauthorized use of computer technology to manipulate critical user data. It refers to any crime that involves a computer and a network.

Types of computer crimes

1. 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.

- It may involve hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

Hacking

A Hacker refers to someone who accesses a computer or network illegally. Originally it was a complimentary word for a computer enthusiast.

A cracker also is someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious action.

- Both hackers and crackers have advanced computer and network skills. Some hackers claim the intent of their security breaches is to improve security, and may be hired by software companies to test the security of new software systems.

Types of computer crimes cont.…

2. 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**

Types of computer crimes cont.…

3. Cyber stalking is the use of communication technology, mainly the Internet, to torture other individuals which include activities such as false accusations, transmission of threats and damage to data and equipment.

4. The physical theft of computer hardware and software is the most widespread related crime especially in developing countries. The most common issues now, we here cases of people breaking into an office or firm and stealing computers, hard disks and other valuable computer accessories.

Control measures against theft

- Employ security agents to keep watch over information centers and restricted backup sites.
- Reinforce weak access points like windows, door and roofing with metallic grills and strong padlocks.
- Motivate workers so that they feel a sense of belonging in order to make them proud and trusted custodians of the company resources.
- Insure the hardware resources with a reputable insurance firm

Types of computer crimes cont....

5. Fraud is stealing by false pretense. Fraudsters can be either employees in a company, non-existent company that purports to offer internet services such as selling vehicles etc. other form of fraud may also involve computerized production and use of counterfeit documents.

6. Sabotage refers to illegal destruction of data and information with the aim of crippling services delivery, or causing great loss to an organization.

Sabotage is usually carried out by disgruntled employees or competitors with the intention of causing harm to an organization.

Types of computer crimes cont.…

7. Surveillance refers to monitoring use of computer system and networks using background programs such as spyware and cookies. The information gathered may be used for one reason or the other e.g. spreading sabotage.

8. Identity theft-Act of pretending to be someone else by using another person's identity

9. Computer industrial espionage-Involves stealing of trade secrets or spying through tech means for bribery, blackmail, etc

Types of computer crimes cont.…

10.Software piracy-The illegal act of duplicating copyrighted software.

11. Phreaking-The act of illegally breaking into a communication system to make calls without paying

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

Types of computer crimes cont....

13. Spoofing is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network.

- E-mail spoofing occurs when the sender's address or other components of the e- mail header are altered so that it appears the e-mail originated from a different sender. E-mail spoofing commonly is used for virus hoaxes, spam, and phishing scams.

Types of computer crimes cont.…

14. Spamming. Sending of unwanted e-mails.
Spam is an unsolicited e-mail message sent to multiple recipients at once. The content of spam ranges from selling a product or service, to promoting a business opportunity, to advertising offensive material.

15. Knowingly selling-Is the act of distributing and selling child pornography.

16. Eavesdropping is the act of secretly listening to a private conversation, typically between hosts on a network or telephone conversations. (sniffing) For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers

Types of computer crimes cont....

17. A denial of service attack, or DoS attack, is an assault whose purpose is to disrupt computer access to a network service.

- **The attackers may use an unsuspecting computer to send an influx of confusing data messages or useless traffic to a computer network. The victim computer network slows down considerably and eventually becomes unresponsive or unavailable, blocking legitimate visitors from accessing the network.**

Types of computer crimes cont.…

18. A cyberextortionist is someone who uses e-mail as a vehicle for extortion. They can send a company a threatening message indicating they will expose their credential information or launch an attack that will compromise the company's network if they are not paid a some of money.

20. A cyberterrorist is someone who uses the Internet or network to destroy or damage computers for political reasons. The cyberterrorist might target the nation's air traffic control system, electricity-generating companies, or a telecommunications infrastructure.

Types of computer crimes cont.....

21. A botnet is a group of compromised computers connected to a network such as the Internet that are used as part of a network that attacks other networks, usually for nefarious purposes.

- **A compromised computer, known as a zombie, is one whose owner is unaware the computer is being controlled remotely by an outsider. Cybercriminals use botnets to send spam via e-mail, spread viruses and other malware, or commit a denial of service attack.**

Types of computer crimes cont....

22. A back door is a program or set of instructions in a program that allow users to bypass security controls when accessing a program, computer, or network.

- Once perpetrators gain access to unsecure computers, they often install a back door or modify an existing program to include a back door, which allows them to continue to access the computer remotely without the user's knowledge.

Types of computer crimes cont.…

23.Accidental access - Threats to data and information come from peoples unknowingly giving out information to strangers is or unauthorized persons.

24. Alteration - is the illegal modification of private or confidential data and information with the aim of misinforming users.

- Alteration is usually done by people who wish to cancel the truth or sabotage certain operations. Alteration comprises the integrity of data and information making it unreliable

computer viruses

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

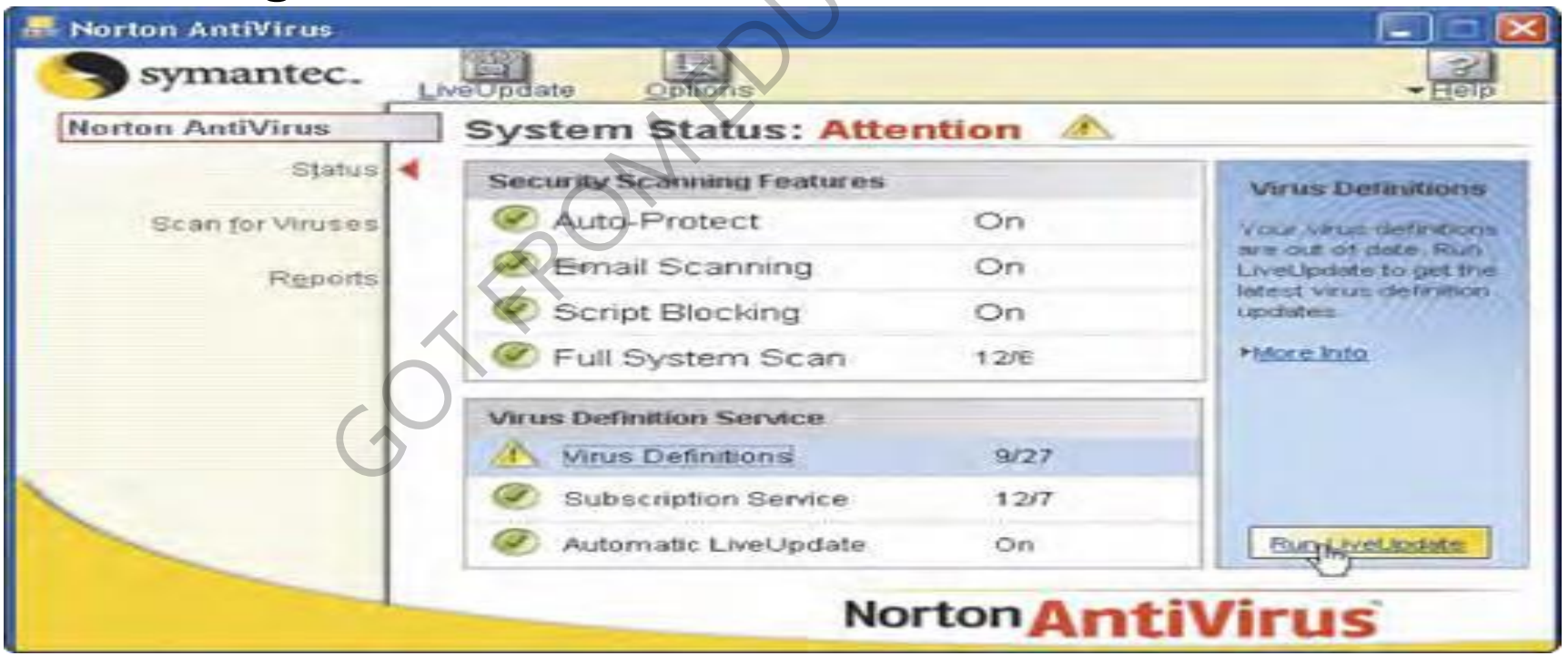
- A computer virus is a piece of software that can replicate itself and infect a computer, data and software without the knowledge of the user.

Symptoms of computer infected by viruses

- Operating system runs much slower than usual
- Available memory is less than expected
- Files become corrupted
- Screen displays unusual message or image
- Unknown programs or files mysteriously appear
- Music or unusual sound plays randomly
- Existing programs and files disappear
- Programs or files do not work properly
- System properties change
- Operating system does not start up
- Operating system shuts down unexpectedly

Virus signature

- **A Virus signature is specific pattern of virus code, also called a virus definition. Antivirus programs look for virus signatures.**



Virus spreads

How a Virus Can Spread through an E-Mail Message

Step 1
Unscrupulous programmers create a virus program that deletes all files. They hide the virus in a word processing document and attach the document to an e-mail message.

Step 2
They send the e-mail message to thousands of users around the world.

Step 3a
Some users open the attachment and their computers become infected with the virus.

Step 3b
Other users do not recognize the name of the sender of the e-mail message. These users do not open the e-mail message — instead they immediately delete the e-mail message and continue using their computers. These users' computers are not infected with the virus.

TYPES OF VIRUSES

- **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.
- **A file virus**-This attaches itself to program files, and is loaded into memory when the infected program is run.
- **A macro virus** -This uses the macro language of an application (e.g., word processor or spread sheet) to hide the virus code.
- **A logic bomb**-This is a virus that activates when it detects a certain condition.
- **A time bomb**-This is a kind of logic bomb that activates on a particular date.

TYPES OF VIRUSES cont....

- **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.
- **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.
- **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
- **Scare-ware** is a type of malware designed to trick victims into purchasing and downloading useless and potentially dangerous software.

TYPES OF VIRUSES cont....

- **Adware**- is a malicious program that usually presents unwanted advertisements to the user of a computer. The advertisements produced by adware are sometimes in the form of a pop-up.
- **Spyware** is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another individual without the consumer's consent, or that claims control over a computer without the consumer's knowledge.

Viruses are activated in three basic ways

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

How 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

Control measures against viruses

- Install the latest versions of anti-virus software on the computers. Make sure that you continuously update the anti-virus software with new virus definition to counter the new viruses.
- Always scan removable storage media for viruses before using them.
- Scan mail attachments for viruses before opening or downloading an attachment.
- Always keep a Recovery Disk: A Removable disk that contains uninfected copy of key operating system commands that enables computer to restart. Also called rescue disk.
- Protect your password and change it after some time

Anti-Virus Software

- Anti-Virus Software Antivirus software is a set of utility programs that looks for and eradicates a wide range of problems, such as viruses, Trojan horses, and worms.
- Examples of Anti-Virus Software
- AVG Anti-Virus
- Avira Anti-Virus
- Norton Anti-Virus Software
- Kaspersky Anti-Virus
- Avast Anti-virus
- Smadav USBAnti-Virus

antivirus program

- ***An antivirus program Identifies and removes computer viruses Most also protect against worms and Trojan horses.***
- **When an antivirus program identifies an infected file, it Attempts to remove any detected virus, Quarantines infected files that it cannot remove (Keeps file in a special area of on hard disk) so that it does not spread the virus to other files.**

Data protection in computer systems

Appropriate ways of protecting data in computer systems include:

1. Data Encryption.

Is the process of converting plaintext (readable data) into ciphertext (unreadable characters) in order to safeguards information against theft.

- To read the data, the recipient must decrypt, or decipher, the data

2. Surge protectors.

Protect computers and equipment from electrical power disturbances. Uninterruptible power supply (UPS) is surge protector that provides power during power loss

Data protection in computer systems cont..

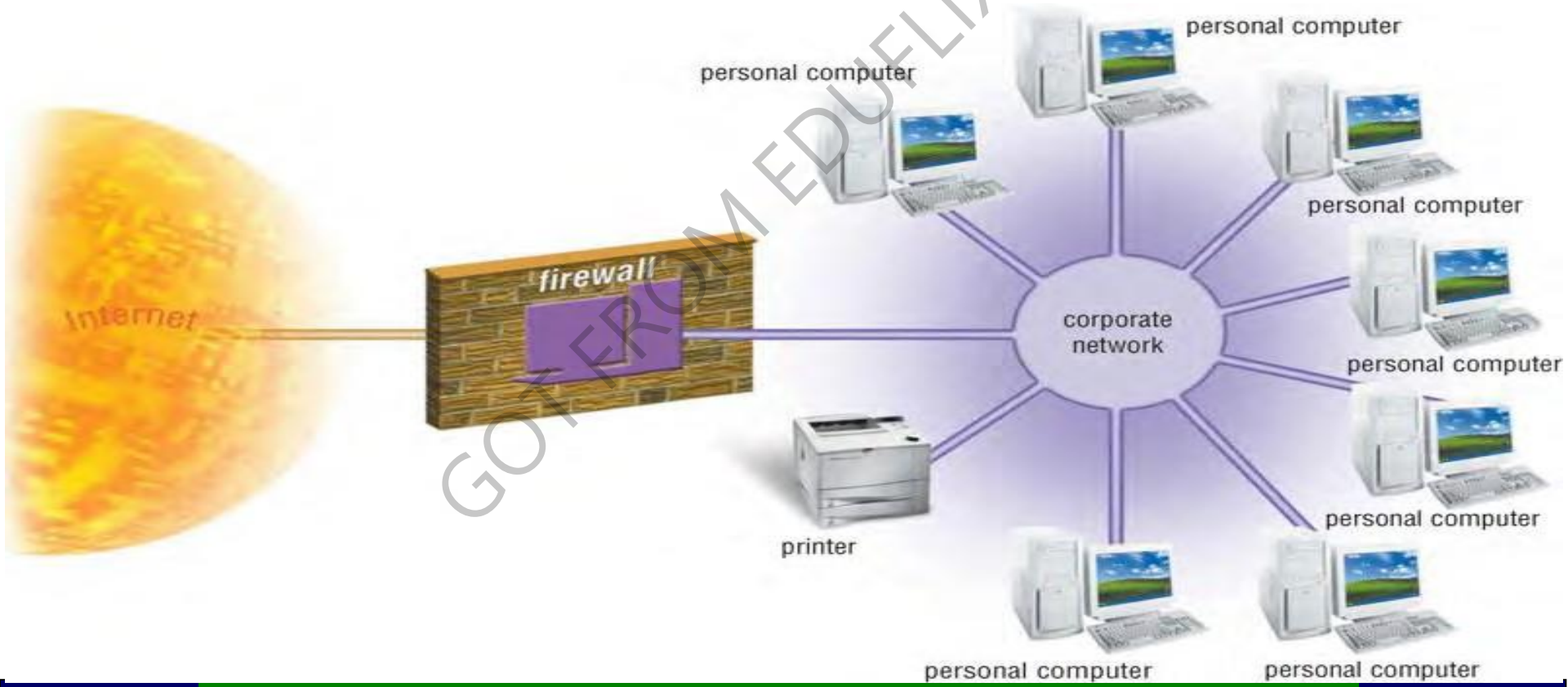
3. Data Backups: Users should frequently duplicate (copy) the information to different storage devices such as DVDs, external hard disk to be able to recover their information in case of a disaster.

4. Installing Firewall: Firewall is a security system consisting of hardware and/or software that prevents unauthorized network access.

- A firewall is a device or software system that filters the data and information exchanged between different networks by enforcing the host networks access control policy.
- The main aim of a firewall is to monitor and control access to or from protected networks

Firewall

People who do not have permission (remote requests) cannot access firewall restricted sites outside their network.



Data protection in computer systems cont..

5. Use of acceptable use policy (AUP)

- The AUP outlines the computer activities for which the computer and network may and may not be used.
- An organization's AUP should specify the acceptable use of computers by employees for personal reasons.

6. Intrusion Detection Software: To provide extra protection against hackers and other intruders, large organizations sometimes use intrusion detection software to identify possible security breaches.

- Intrusion detection software automatically analyzes all network traffic, assesses system vulnerabilities, identifies any unauthorized access (intrusions), and notifies network administrators of suspicious behavior patterns or system breaches

Data protection in computer systems cont..

7. Identifying and Authenticating Users

Many organizations use access controls to minimize the chance that a perpetrator intentionally may access or an employee accidentally may access confidential information on a computer.

- An access control is a security measure that defines who can access a computer, when they can access it, and what actions they can take while accessing the computer.

Data protection in computer systems cont..

8. User Names and Passwords. This is to restrict access to the computer systems, only allowing authorized users.

- **A username** is Unique combination of characters that identifies user
- **Password** is a secret code that combines characters and numbers that allow a user to access a computer or a network.

Rules for creating Secure Passwords

- Do not use your name or names of your close friends.
- Pick a mix of alphabetic and numeric characters. Never use an all-numeric password (especially your phone number or social security number).
- Pick long passwords. If your password is only a few letters long, an attacker will find it easy to try all combinations.
- Pick different passwords for the different machines or network nodes you access.

Data protection in computer systems cont..

9. Possessed objects

- Items that you must carry to gain access to computer or facility, E.g. badges, cards, smart cards, and keys.
- Often used with numeric password called personal identification number (PIN) e.g. ATM pin.

10. Security monitors are programs that monitor and keep a log file or record of computer systems and protect them from unauthorized access.

11. Biometric devices

- Authenticate people's identity using a human characteristic like Fingerprint, hand geometry, voice, signature, or iris.

Data protection in computer systems cont..

11. Callback systems

- User connects to computer only after the computer calls that user back at a previously established telephone number.
- Some networks utilize callback systems as an access control method to authenticate remote or mobile users. Callback systems work best for users who regularly work at the same remote location, such as at home or branch office.

12.Installing Antivirus Program:- Computer programs that attempt to identify, prevent and eliminate computer viruses and other malicious software (malware).

Data protection in computer systems cont..

13. Audit Logs:- Network managers should ensure that their system is able to create an audit log. An audit log will record every important event in an 'audit file such as who logged on to the system at what time and onto which computer, which files were opened, altered, saved or deleted or log events such as attempts to access proxy servers.

Privacy and ICT Ethical Issues

- ICT ethics and society
- ICT ethics are moral guidelines that govern use of computers and information systems.
- Ethics is knowing and understanding what is right and what is wrong, and then doing the right thing right. In simple terms, ethics are standards of moral conduct.
- A code of conduct is a written guideline that helps determine whether a specific action is ethical or unethical.

Computer Ethics for Computer Professionals

According to the Association for Computing Machinery (ACM) code, a computing professional:

- Contributes to society and human well- being.
- Always avoids harm to others.
- Should be honest and trustworthy.
- Should exercise fairness and takes action not to discriminate.
- Honors property rights, including copyrights and patents
- Gives proper credit when using the intellectual property of others.
- Respects other individuals' rights to privacy.
- Honors confidentiality.

IT Codesof Conduct.

IT CODE OF CONDUCT

1. Computers may not be used to harm other people.
2. Employees may not interfere with others' computer work.
3. Employees may not meddle in others' computer files.
4. Computers may not be used to steal.
5. Computers may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' computer resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use computers in a way that demonstrates consideration and respect for fellow humans.

Intellectual property

- **Intellectual property (IP) refers to creations of the mind that may include software, music, literature, discoveries and inventions.**
- **Intellectual property rights are the rights given to persons over the creations of their work /minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time. - Intellectual property rights include patents, copyright, industrial design rights, trademarks, trade dress, and trade secrets.**

Intellectual property rights

- **A patent** grants an inventor the right to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention
- **A copyright** is the exclusive legal right that prohibits copying of intellectual property without permission of the copyright holder. - A copyright gives the creator of original work exclusive rights to it, usually for a limited time
- **A trademark** is a recognizable sign, design or expression which distinguishes products or services of a particular trader from the similar products or services of other traders.
- A trademark protects a company's logos and brand names

Information privacy

- Information privacy refers to the right of individuals and companies to deny or restrict the collection and use of information about them.
- In the past, information privacy was easier to maintain because information was kept in separate locations. Each retail store had its own credit files. Each government agency maintained separate records. Doctors had their own patient files.

Concerns related to collection and use of private data are

- Data should not be disclosed to other people without the owner's permission.
- Data and information should be kept secured against loss or exposure
- Data and information should be kept longer than necessary
- Data and information should be accurate and up to date.
- Data and information should be collected, used and kept for specified lawful purposes

What are some ways to safeguard personal information?

- Limit the amount of information you provide to Web sites; fill in only required information
- Inform merchants that you do not want them to distribute your personal information
- Set up a free e-mail account; use this e-mail address for merchant forms
- Sign up for e-mail filtering through your Internet service provider or use an ant-spam program.

What are some ways to safeguard personal information? Cont..

- Do not reply to spam for any reason
- Install a personal firewall
- Turn off file and print sharing on your Internet connection
- Surf the Web anonymously with a program such as Freedom Web Secure or through an anonymous Web site such as Anonymizer.com
- Install a cookie manager to filter cookies
- Clear your history file when you are finished browsing.

Unethical computer codes of conduct

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

Computer ethics to 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

Emerging Technologies

- **Emerging technologies**: This involves innovations and advancements in the use of new technological tools that make technology more amazing
- ICT is always improving and changing and new technologies are being developed all of the time. Developments in technology will, by nature, impact on our everyday lives and these include:

Emerging Technologies

- Artificial Intelligence (AI)
- Digital forensics
- Biometrics
- Robotics
- Quantum Cryptography
- Computer Assisted Translation (CAT)
- 3D and Holographic Imaging (aka holograms)
- Virtual Reality

Artificial Intelligence (AI)

This is a computer science that is focused on creating computer systems that simulate human intelligence. AI is being developed in the following application areas:

Expert Systems - These are computers that have been programmed to make decisions based on information they are given. For example: Medical expert systems can diagnose patient's illnesses based on symptoms entered.

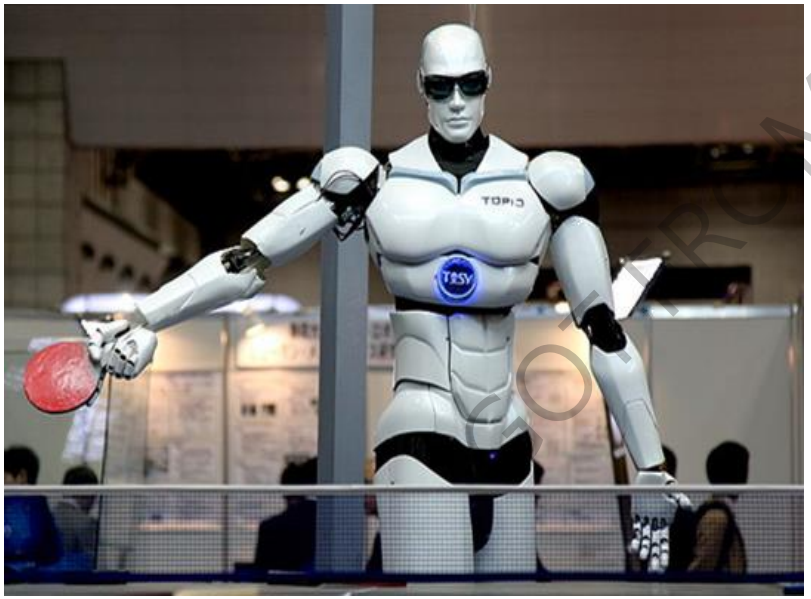
Languages - This type of AI involves computers that can understand different human languages as they are spoken to them.

Robotics - Robotic artificial intelligence is where machines are programmed to imitate a human.

Game Playing - Computers developed to play games against human players

Impact of AI on our daily life

- **Increased Personal safety** - Modern home alarm systems use artificial intelligence software that can tell the difference between the home owners and intruders. The software automatically alerts the police when intruders are detected.



Impact of AI on our daily life

- **Accurate prediction of weather** - AI software are used to sift through weather data more accurately than humans can and be used to predict approaching storms and automatically issue warnings.
- **Increased leisure time** .
- **Safer transport** – Self driving cars already exist will drastically reduce road accidents. Driverless trains too already exist in some countries!
- **Improved medical care** - Robotic surgery assistants are being used to quickly and accurately pass the correct surgical tools to doctors.

Digital forensics

- **Digital forensics**, also called **computer forensics**, **network forensics**, or **cyber forensics**,
- is the discovery, collection, and analysis of evidence found on computers and networks. or
- **Digital forensic** refers to the science encompassing the recovery and investigation of material found in digital devices often in relation to computer crime.
- Digital forensics involves the examination of computer media, programs, data and log files on computers, servers, and networks.

Digital forensics cont..

Many areas use digital forensics, including corporate structures and policies, a willingness to learn and update skills, and a knack for problem solving.

- law enforcement,
- criminal prosecutors,
- military intelligence,
- insurance agencies,
- Tax investigations and information security departments in the private sector.

Investigators carrying out data acquisition of computer and mobile device

Impact of Digital Forensics on everyday life:

- Forensics is changing in the digital age, and the legal system is still catching up when it comes to properly employing digital evidence.
- Broadly speaking, digital evidence is information found on a wide range of electronic devices that is useful in court because of its probative value.

Impact of Digital Forensics on everyday life:

- Technology changes evidence. This is not the first time that technology has impacted the way evidence is gathered and presented in courts. And it's not the first time that there have been problems in the way new evidence is used. E.g. DNA evidence.
- Cyber evidence: It is increasingly common for criminal trials to rely on digital evidence. And, regrettably, it is not uncommon for innocents to be convicted and guilty people acquitted because of digital evidence

Biometrics

- Biometrics is where parts of a person's body are used for identification purposes. Examples include:
  - **Fingerprints** - These are impressions embedded at the end of human fingers and thumbs. Fingerprints kept in a database can be matched to those left at crime-scenes to help identify the culprit.
  - **Eye recognition** - Eye scans analyses the iris which is the coloured ring that surrounds the pupil.

Biometrics cont..

- **Face recognition** - This is where the shapes of individual's faces are analysed.
- **Voice recognition** - Pitch, tone and frequency of voices are unique and can be analysed to identify people.

- All of these parts of the human body are unique from person to person and can be used to authenticate identity.
- Note: Even identical twins have slightly different fingerprints and voices etc.

Impacts of Biometrics on everyday life:

- **Better airport security**: Iris recognition is already in use in some airports. Travelers have their eyes and iris scanned into a system and this data is later matched up when the person is performing airport checks.
- **Increased building security**: Fingerprint access to buildings have been replacing the older methods of locks and keys. This methods ensures that only authorised people can enter restricted buildings or rooms.

Impacts of Biometrics on everyday life:

- **Reduced car theft**: Cars already exist that use fingerprints to only unlock their doors or start the engine for the fingerprint that is registered. This means that the doors will not unlock for a print that is not recognised and makes the car harder to steal.
- **More secure mobile phones**: Mobile phones contain our lives. We used our phones for everything from social media to shopping online. Apple recently released an iPhone model that uses a fingerprint reader to identify the true owner of the phone. It will not unlock for a fingerprint that it does not recognise

Robotics

- Robots are used to perform a wide range of physical tasks. They are either automated (controlled by a computer chip) or manually controlled by a human.

There are 4 different types of robots:

- Manufacturing robots (used to perform repetitive tasks such as welding)
- Carrier robots (used by the military to carry heavy loads over dangerous terrain)
- Domestic robots (used in homes to perform cleaning tasks such as vacuuming)
- Exploration robots (used to visit and send images from places such as Mars)

Some more typical tasks that robots can be used for are described below:

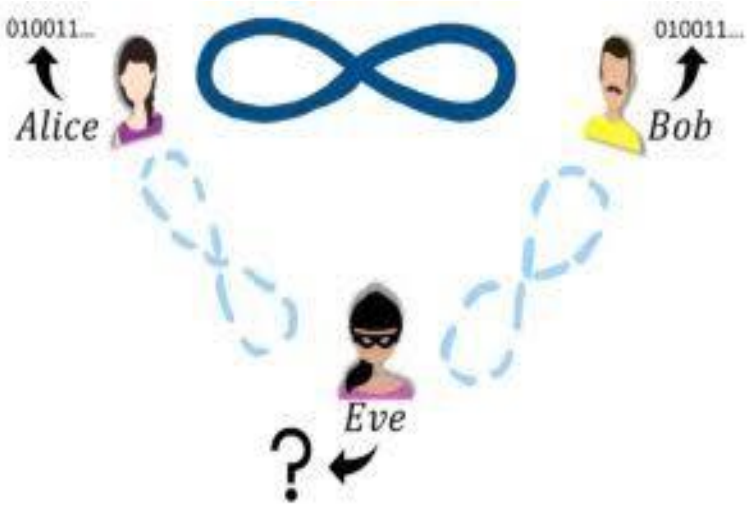
- **Dangerous jobs** -E.g. disposing of bombs, spray painting etc.
- **Exploring extreme environments-** E.g. inside volcanoes, planets or the depths of the ocean
- **Repetitive manufacturing jobs** -E.g. production lines, packing and welding etc.
- **Moving heavy objects** - E.g. installing large engines.
- Think about it! Robots can work 24/7 and never need to take Robots are increasingly being used in manufacturing due to their proven increase in productivity. breaks. They also do not require wages like humans do. This means that robots can produce more at a lower cost.

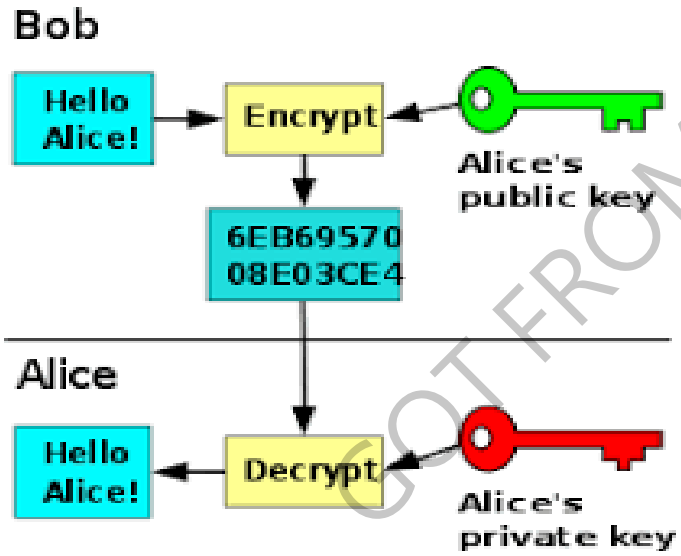
Impacts of Robotics on everyday life:

- **Increased personal time** - If robots can carry out domestic work, this frees up more time for us to spend as we wish.
- **More efficient manufacturing** - Robots can manufacturer products such as cars much faster and cheaper than humans can.
- **Safer working environments** - Robots can safely carry out tasks that are too dangerous for humans. For example: spraying cars with toxic paint, defusing bombs on battlefields and search and rescue operations in buildings destroyed by earthquakes.
- **Loss of jobs Due to higher and cheaper productivity** - Robots are taking over the manufacturing jobs that used to be carried out by humans. This means that humans are missing out on employment on assembly lines and factory work.

Quantum Cryptography

- **Quantum cryptography (encryption)** is an emerging technology that allows messages and data to be sent with complete privacy.
- Note: Encryption is where digital data and files are scrambled so that only authorized
- people are allowed to read it.
- Unauthorized people attempting to read the data would see illegible nonsense instead of the real information.





Impacts of Quantum Encryption on everyday life:

Completely secure voting. Citizens of countries have the right to vote-in new governments but history is littered with examples of where these votes have been tampered with in order to influence election outcomes. Securing votes with quantum encryption methods ensures that they cannot be tampered with or changed.

Completely secure communication - Messages sent by the military often include the locations of squadrons or special op's teams. If enemy forces intercepted these messages it could have severe consequences. Using quantum cryptography to secure the messages would eliminate the risk of them being read or heard by unauthorized ears.

Impacts of Quantum Encryption on everyday life:

- **Completely secure bank transfers** - Any electronic transfer of money, such as at ATM's or buying goods online, will be completely secure. Some banks are already using quantum cryptography for the purposes of securing money transfers.
- **Completely secure personal information** - Health records, bank details and other types of personal information will be absolutely secure from hackers and other people wishing to commit identity theft crimes.

Computer Assisted Translation (CAT)

- **CAT** is where a human translator uses computer software to help in the translation process. CAT software can reduce the amount of time that the translation Examples of different types of CAT tools include:
- **Spell checkers** - These are usually built-into word processing software and can automatically flag-up spelling errors and suggest translations of miss- spelt words.
- **Language search-engine software -** These are Internet based systems which allow translators to enter any text that they want translating and also to select which language they want the text translating into. The software will then search through a large collection of translation memory databases to try and find a match with the text entered into the search engine.

Impacts of Computer Aided Translation on everyday life:

- **More accurate documents Spell checkers** can quickly scan your word processed documents and automatically find spelling errors. Miss-spelt words can be quickly corrected to produce an error-free document.
- **Quicker and more efficient translations** Foreign visitors to countries can be communicated with much easier through these CAT tools. They are especially useful in places like embassies where a wide-range of foreign visitors may need to communicate with local officials about problems or ask for advice etc.

3D - Imaging

- This is a technique where images are made to appear three-dimensional and to actually have depth. The two- dimensional images need to have been shot at different angles.

Impacts of 3D imaging on everyday life:

Better movie experiences -Hollywood have been using 3D imaging within the production of movies for many years. These provide the viewer with a much more immersive experience.

Virtual Reality

Virtual reality is where computers are used to create an artificial environment that users can interact with as if it were real.

Virtual reality is not really meant for gaming purposes. It is used for more serious purposes such as:

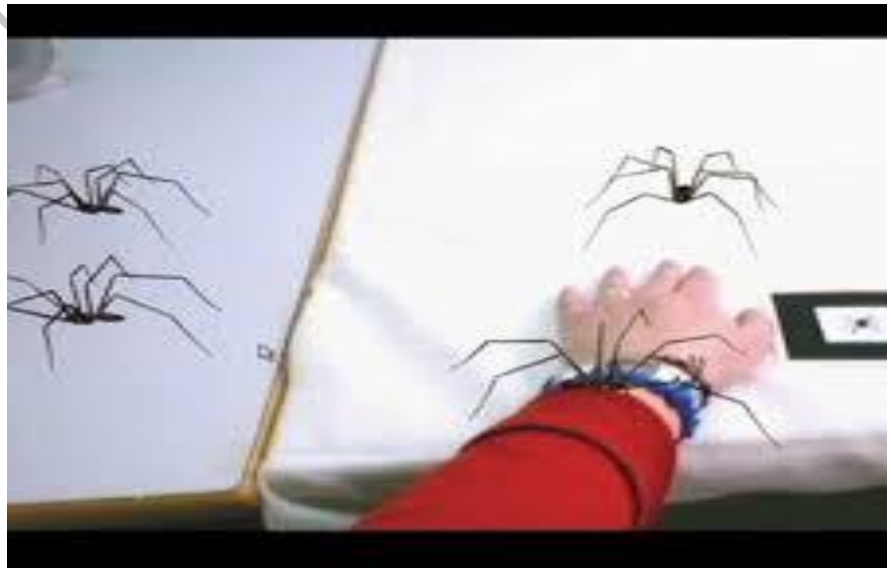
- Allowing architects to walk around a virtual version of their design (this gives a better idea of what the finished building will look like)
- Training soldiers in combat (flight simulation, battlefield simulation)
- Training surgeons (virtual patients can be operated on to provide experience to trainee surgeons).

Impacts of Virtual Reality on everyday life:

Improved medical surgeons - Surgeons can be trained using virtual patients. This allows them to practice over and over until they have perfected a particular surgery without risk to a real patient.

Larger and stronger buildings - Virtual buildings allow architects to walk around to experience what the building would look like when completed and check for potential errors before the actual building is constructed.

More effective treatment of phobias - VR is being used to help patients overcome phobias and anxieties. People can experience a controlled version of what they are afraid of. Slowly the person becomes used to the situation and can relax. For example: Someone might be terrified of spiders and so they could be gradually introduced to larger and larger virtual spiders.



Impacts of Virtual Reality on everyday life:

Training in dangerous situations - VR can be used for training in dangerous situations where it is impossible to practice the real thing. For example: A large fire in an office building could never be set up in reality, but it could in a virtual environment. This will allow workers to practice emergency evacuation in a safe environment.

More realistic education - VR can give students the opportunity to learn in a much more interactive way. For example: Astronomy students can learn about the solar system by engaging with the objects in the virtual environment. They could look around stars, move planets and track the orbits of comets. This approach is likely to allow students to retain knowledge much better than reading text out of a book.

Cloud computing

- Cloud computing operates on a similar principle as web-based email clients, allowing users to access all of the features and files of the system without having to keep the bulk of that system on their own computers. In fact, most people already use a variety of cloud computing services without even realizing it such as Gmail, Google Drive, Google Docs, etc.

ICT INDUSTRY

- Information and communication technology (ICT) has created new job titles such as computer operators, computer technicians, system analyst, computer programmers, software engineer, information systems manager, data base administrator, computer trainer, web administrator, computer graphics designers, system administrators and network administrator.

System analyst

This a person who is responsible for analyzing a company's needs or problems then designs and develops a computer based information system.

Some of the responsibilities of a system analyst include:

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

Computer operator

- Some of the responsibilities of a computer operator include;
- Entering data into the computer for processing.
- Keeping up-to-date records (log files) of all information processing activities.

Computer technician

- Given that computers require regular maintenance, upgrading as well as emergency repairs, demand for computer technicians. Some of the responsibilities of a computer technician are;
- Troubleshooting computer hardware and software related problems
- Assembling and upgrading computers and their components.
- Ensuring that all computer related accessories such as printers modems, storage media devices are in good working condition.

Computer engineer

Some of the responsibilities of a computer engineer include;

- Design and develop computer components such as storage devices, motherboards and other electronic components.
- Determine the electrical power requirement of each component.
- Re-engineer computer components to enhance its functionality and efficiency.
- Design and develop engineering and manufacturing computer controlled devices such as robots

Computer programmer

Some of the responsibilities of a computer programmer include;

- Develop in house application programs or system programs.
- Customize commercial application packages to suite the organization needs.
- Install, test, debug, and maintain programs developed or customized for the organization.

Web administrator /webmaster

A web administrator is responsible for:

- Developing and testing websites.
- Maintaining, updating and modifying information on the website to meet new demands by the users.

Network administrator

A network administrator is a specialist whose responsibilities are to:

- Set-up a computer network.
- Maintain and enforce security measures on the network.
- Monitor the use of network resources.
- Maintain and troubleshoot network related problems.

Software engineers and Computer Trainers

- **Software engineers**: Most Software engineers analyses user needs and create application software. Software engineers usually have experience in programming, but focus on the design and development of programs using the principles of mathematics and engineering.
- **Computer Trainers**: Computer trainers typically teach new users how to use the computer software and hardware

System Administrators

system administrator, or sysadmin, ***is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi- user computers, such as servers.*** ***Other responsibilities of an information system administrator include;***

- **Ensures that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget.**
- **A system administrator may acquire, install, or upgrade computer components and software; provide routine automation; maintain security policies; troubleshoot; train or supervise staff; or offer technical support for projects.**

Graphic designers

A graphic designer is a professional within the graphic design and graphic arts industry who assembles together images, typography, or motion graphics to create a piece of design