COMPUTER STUDIES
for
UGANDA

SIXTH EDITION 2018

BY

Rogers Mukalele

ICT Department, Kololo Senior Secondary School

0706-060740, www.mukalele.net

SALES AND MARKETING BY

Mpeirwe Nobles

0775-356622

ACKNOWLEDGEMENTS

The author would like to thank the following people in a special way for their valuable advice, assistance, support and encouragement in the development of this edition: Mr. Kanoonya Edward (Head teacher Kololo SSS), Mr. Wambedde James, Mr. Wamusi Ivan, Ms. Nandyose Eseza (Members - ICT Department Kololo SSS), Ms. Nakayinda Hanifah, Mr. Kiyimba Robert, Mr. Mutagana Moses, Mr. Ntubuura Steven (Members - ICT Department Jinja College), Mr. Sekizivu Hamdan (Co- Author First Edition),, Mr. Opio Joseph, Mr. Mukwaya John, Mr. Oryang David Wegesa, all members of the Uganda ICT Teachers and Sharebility Uganda platforms, my marketing team: Mr. Mpeirwe Nobles, Mr. Menya Julius, Members of Open Youth Care Foundation Uganda plus all my family members especially Ms. Najodo Peace, Ms. Talunga Primrose, Mr. Daada Raymond, Mr. Peter Mukenye Magoola, Ms. Christine Magoola, Ms. Nakamya Catherine Magoola and Ms. Joy Eliosi.

Likewise, we thank all our students over the years, for their contributions, insights and questions that have made this book comprehensive.

We also want to appreciate the National Curriculum Development Center (NCDC) for providing the Computer Studies Teaching Syllabus 840 and the Subsidiary Information and Communication Technology Teaching Syllabus S850.

Above all we thank the **Almighty God** for having granted us the knowledge, strength and persistence that has enabled us to publish the book.

PREAMBLE

There has been a demand for a correspondence course and resource that makes students participate, and understand the intention of learning computer studies.
All practitioners of ICT and our students need to ask one another, what will Information Technology and ICTs help them and our country Uganda in the future?
As we all know, it is becoming almost impossible to work in the administrative and business, to Education, Research, and Communication sectors without a great skill in Computer systems.

ICT is becoming more and more pivotal than before in whatever aspect of thing we do per second of our time. Offices are becoming paperless, you no longer need to line up at a bank queue, a teacher does not need to be present for a lesson delivery, and we have started to live in cashless societies where one needs better mobile equipment. This therefore means that Information Technology has started and will continue to steer every facet in our day to day lives in the third world countries as it is in first world.
In this book, we have arranged all content in an easy to read mode to enable students read ahead, there are a number of activity based exercises, Multiple Choice Questions, essay questions, and practical exercises to enable our students be possessed with enough activity to do.

Teachers will find this book very helpful, especially those with big classes in terms of dividing theory and practical lesson time appropriately. This book is designed for students doing Computer Studies at O' level, but it is also useful to students doing Subsidiary ICT at Advanced Level and Computer Literacy at Higher Institutions of Learning.

Books by the same author include:

- Computer Studies *for Uganda* (6th Edition 2018)
- Subsidiary ICT *for Uganda* (2nd Edition 2018)
- ICT REVISION Questions and Answers *for Uganda* (2nd Edition 2018)
- Lab Activities for Computer Practical Applications. (4th Edition 2017)

Find details on www.mukalele.net

For further enquiries, suggestions or useful criticism please refer to;

Mukalele Rogers
Email: mrogers4christ@gmail.com
Web: https://www.mukalele.net/
+256776 960 740
+256706 060 740

TABLE OF CONTENTS

LIST OF COMPUTER STUDIES ABBREVIATIONS (ACRONYMS)

ADC	Analog-to-Digital Converter
ADSL	Asymmetric Digital Subscriber Line
ALU	Arithmetic / Logic Unit
ARPANET	Advanced Research Projects Agency Network
ASCII	American Standard Code For Information Interchange
ATA	Advanced Technology Attachment
BASIC	Beginner's All-purpose Symbolic Instruction Code
BCC	Blind Carbon Copy
BIOS	Basic Input/Output System
BMP	Bitmap; Applied To Image Format As .bmp
CAA	Computer Assisted Assessment
CAL	Computer Assisted Learning
CAI	Computer Assisted Instructions
CAD	Computer-Aided Design
CC	Carbon Copy
CD	Compact Disc
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read-Only Memory
CD-RW	Compact Disc Re-Writable
COBOL	COmmon Business Oriented Language
CMOS	Complementary Metal Oxide Semiconductor
CMYK	Cyan Magenta Yellow Black
CPU	Central Processing Unit
CRT	Cathode Ray Tube
CSS	Cascading Style Sheet
DAC	Digital-to-Analog Converter
DBMS	Database Management System
DMA	Direct Memory Access
DNS	Domain Name System
DOS	Disk Operating System
DPI	Dots Per Inch
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
DVD-R	Digital Versatile Disc Recordable
DVD-RW	Digital Versatile Disk Rewritable
DVI	Digital Video Interface
EDI	Electronic Data Interchange
EBCDIC	Extended Binary Coded Decimal Interchange Code
EEPROM	Electrically Erasable Programmable Read Only Memory
FAQ	Frequently Asked Questions
FAT	File Allocation Table
FDD	Floppy Disk Drive
FTP	File Transfer Protocol
GIF	Graphics Interchange Format; Applied To Image Format As .gif

GIGO	Garbage In, Garbage Out
GUI	Graphical User Interface
HTML	Hyper-Text Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transport Protocol Secure
I/O	Input/Output
IC	Integrated Circuits
ICS	Internet Connection Sharing
IDE	Integrated Device Electronics (/Development Environment)
IGP	Integrated Graphics Processor
INTERNIC	Internet Network Information Center
IP	Internet Protocol
IPX	Internet Packet Exchange
IRC	Internet Relay Chat
IRQ	Interrupt Request
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
JPEG	Joint Photographic Experts Group; Applied To Image Format As .jpeg
KBPS	Kilobits Per Second
LAN	Local Area Network
LCD	Liquid Crystal Display
MAC (ADDRESS)	Media Access Control Address
MBPS	Megabits Per Second
MIDI	Musical Instrument Digital Interface
MIPS	Million Instructions Per Second
MPEG	Moving Picture Experts Group; Video Format
NIC	Network Interface Card
NTFS	New Technology File System
OCR	Optical Character Recognition
OMR	Optical Mark Recognition
OLE	Object Linking And Embedding
OOP	Object-Oriented Programming
P2P	Peer To Peer
PC	Personal Computer
PCI	Peripheral Component Interconnect
PDA	Personal Digital Assistant
PDF	Portable Document Format
PHP	Hypertext Preprocessor
PMU	Power Management Unit
PNG	Portable Network Graphic; Image Format
PNP	Plug And Play
PPI	Pixels Per Inch
PPM	Pages Per Minute
PROM	Programmable Read Only Memory

RAM	Random Access Memory
RGB	Red Green Blue
ROM	Read-Only Memory
RTF	Rich Text Format
SATA	Serial Advanced Technology Attachment
SDRAM	Synchronous Dynamic Random Access Memory
SDSL	Symmetric Digital Subscriber Line
SEO	Search Engine Optimization
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SPX	Sequential Packet Exchange
SQL	Structured Query Language
SRAM	Static Random Access Memory
SRGB	Standard Red Green Blue
TCP/IP	Transmission Control Protocol/Internet Protocol
TIFF	Tagged Image File Format; Applied To Image Format As .tif
UNC	Universal Naming Convention
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VGA	Video Graphics Array
VLSI	Very Large Scale Integration
VRAM	Video Random Access Memory
WAN	Wide Area Network
WI-FI	Wireless Fidelity
WWW	World Wide Web
XHTML	Extensible Hypertext Markup Language
ZIF	Zero Insertion Force

S4 - TOPIC 12: TRENDS IN COMPUTING

GENERAL OBJECTIVE: To enable the learner to understand and appreciate contemporary issues and developments in computing.

Teaching and Learning Strategies: Teacher should guide learners to discover on their own; Learning should be through observations by learners; Teacher should demonstrate to the learners to achieve learning; Learners should engage in self-study; ***a resource person can be used in this topic to supplement the teacher's input.***

COMPUTER INTEGRITY AND SECURITY

Definitions

Data Security *refers to protective measures that are applied to ensure integrity, availability and confidentiality of computer data or information.*

- **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 of said data which may introduce unintended/unwanted changes to the original data.*
- **Availability** means prevention of unauthorized withholding of data access (Intended users can access whenever they need to access).
- **Confidentiality** means to avoid unauthorized disclosure of data third parties.

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.

HARDWARE INTEGRITY

- A computer security risk is an Action that causes loss of or damage to computer system.
- Security threats to hardware include:
  1. System Failure
  2. Hardware Theft
  3. 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**
  - Cables sometimes used to lock equipment
  - 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

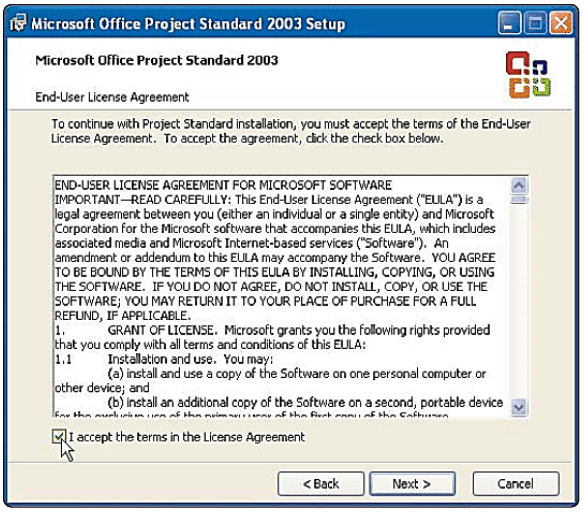
SOFTWARE INTEGRITY

- Security threats to computer software and data include:
  1. Information Theft
  2. Software Theft
  3. Internet And Network Attacks Such Us Hackers
  4. Malicious Programs (Computer Viruses, Worms And Trojan Horses)
  5. Unauthorised Access and Use
  6. Unauthorized Alteration.

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.



Information theft

- Information theft is yet another type of computer security risk. **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.

COMPUTER INTRUSION

This refers to compromising a **computer** system by breaking the security of such a system or causing it to enter into an insecure state. The act of intruding—or gaining unauthorized access to a system—typically leaves traces that can be discovered by **intrusion** detection systems

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, or someone gaining access to a bank computer and performing an unauthorized transfer.
- **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.

To utilize intrusion detection software requires the expertise of a network administrator because the programs are complex and difficult to use and interpret. These programs also are quite expensive

NETWORK INTRUSION AND 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.

Hacking

- The term 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.
- A **script kiddie** has the same intent as a cracker but does not have the technical skills and knowledge. Script kiddies often use prewritten hacking and cracking programs to break into computers.
- A **cyberextortionist** is someone who uses e-mail as a vehicle for extortion.
- 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.

Explaining how denial of service attacks, backdoors, spoofing are carried out.

- 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.
- Perpetrators have a variety of motives for carrying out a DoS attack. Those who disagree with the beliefs or actions of a particular organization claim political anger motivates their attacks. Some perpetrators use the attack as a vehicle for extortion. Others simply want the recognition.
- 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.
- 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.
- **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.
- IP spoofing occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source. Perpetrators of IP spoofing trick their victims into interacting with a deceptive Web site.

COMPUTER CRIMES

Identifying types of computer crimes

Physical theft - 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. In most cases such theft can be done by untrustworthy employees of firm or by outsiders. The reason behind an act may be commercial, destruction to sensitive information or sabotage.

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.

Piracy - illegal copying of software, information or data.

Fraud - 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. This is due to the dynamic growth of internet and mobile computing, sophisticated cybercrimes.

Sabotage - 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.

Eavesdropping - Eavesdropping refers to tapping into communication channels to get information. Hackers mainly use eavesdropping to access private or confidential information from internet users or from poorly secured information system.

Surveillance (monitoring) - 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.

Industrial espionage - Industrial espionage involves spying on a competitor to get information that can be used to cripple the competitor.

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

Alteration - 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 PROTECTION

Appropriate ways of protecting data in computer systems

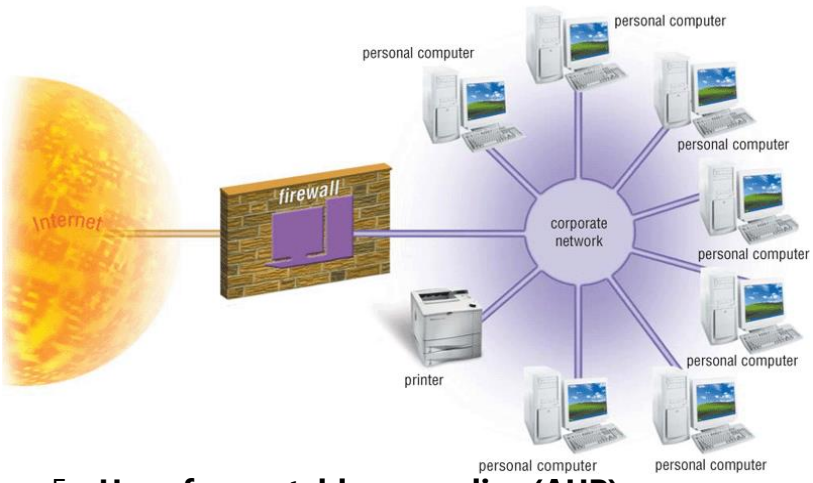
1. Data Encryption. Data on transit over the network faces many dangers of being tapped, listened to or copied to unauthorized destinations. Such data can be protected by mixing up into a form that only the sender and receiver is able to understand. This is by reconstructing the original message from the mix which is called data encryption.

   What is Data encryption?

   - Process of converting plaintext (readable data) into ciphertext (unreadable characters)
   - Safeguards against information theft
   - Encryption key (formula) often uses more than one method
   - 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.

3. Backups - the ultimate safeguard. Backups - the ultimate safeguard
   - Full backup - all files in computer
   - Selective backup select which files to back up
   - Three-generation backup preserves three copies of important files
   - In case of system failure or corrupted files, restore files by copying to original location.
4. 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. People who do not have permission (remote requests) cannot access firewall restricted sites outside their network.



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.
- Some organizations prohibit such use entirely. Others allow personal use on the employee's own time such as a lunch hour.

6. **Use of Intrusion Detection Software**

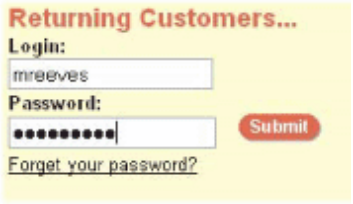
- To provide extra protection against hackers and other intruders, large organizations sometimes use intrusion detection software to identify possible security breaches.

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. In addition, the computer should maintain an **audit trail** that records in a file both successful and unsuccessful access attempts.

- An unsuccessful access attempt could result from a user mistyping his or her password, or it could result from a hacker trying thousands of passwords. Organizations should investigate unsuccessful access attempts immediately to ensure they are not intentional breaches of security

8. **User Names and Passwords**
   a. A username is Unique combination of characters that identifies user
   b. Password is private combination of characters associated with the user name that allows access to computer resources.



How can you make your password more secure?

How can you make your password more secure?

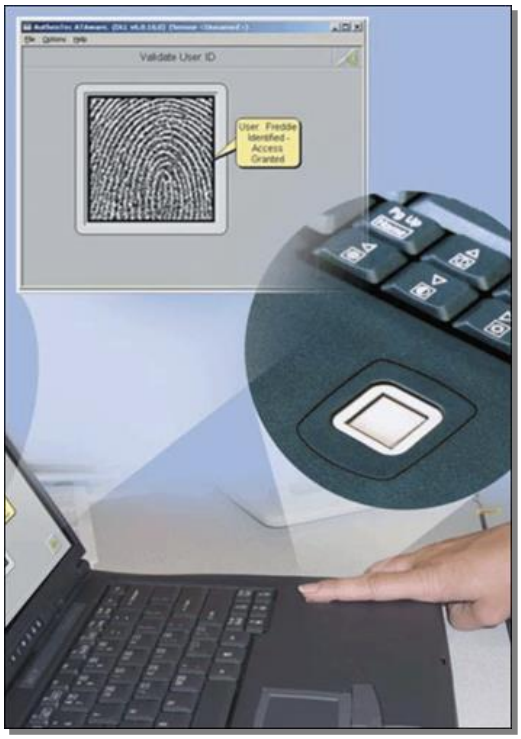
PASSWORD PROTECTION

		AVERAGE TIME TO DISCOVER	
Number of Characters	Possible Combinations	Human	Computer
1	36	3 minutes	.000018 second
2	1,300	2 hours	.00065 second
3	47,000	3 days	.02 second
4	1,700,000	3 months	1 second
5	60,000,000	10 years	30 seconds
10	3,700,000,000,000,000	580 million years	59 years

- *Possible characters include the letters A–Z and numbers 0–9*
- *Human discovery assumes 1 try every 10 seconds*
- *Computer discovery assumes 1 million tries per second*
- *Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations*

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**.
   — Access control can be enhanced by implementing multilevel authentication policies such as assigning users log on accounts, use of smart cards and a personal identification number (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.
    - Biometric security is a growing form of unauthorized control measure that takes the user's attributes such as voice, fingerprints and facial recognition. For example, you can log on swap a finger on a finger print swap windows.

12. 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.



13. **Secure web data transmission using HTTPS.** Users apply for SSL certificate from a certificate authority (CA). A CA is an Authorized person or company that issues and verifies SSL certificates.

The following are some examples of crimes perpetuated by use of computers.

COMPUTER ETHICS

- 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.
- Quite often, people in society do the wrong things either out of ignorance or deliberately to achieve selfish interests.
- In today's society, computers are involved to some extent in almost every aspect of life and sometimes they often perform life-critical tasks.
- This makes it very important to carefully consider the issues of ethics in use of computers and software.
- Ethical principles are important because they help us navigate through difficult situations and reflect the way to relate with our friends and community.

Three useful ethical principles:

- An act is ethical if society benefits from the act.
- An act is ethical if people are treated as an end and not as a means to an end.
- An act is ethical if it is fair to all parties involved.

Computer ethics involves use of computers & software in morally acceptable way.

ICT ethics are the moral guidelines that govern use of computers and information systems.

- Standards or guidelines are important in this industry, because technology changes are outstripping the legal system's ability to keep up.

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 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.

CODE OF CONDUCT

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

COMPUTER PIRACY

Piracy is a form of intellectual property theft which means illegal copying of software, information or data. Software, information and data are protected by copyright and patent laws.

Control measures against piracy - There are several ways of reducing piracy

- Enforce laws that protect the owners of data and information against piracy.
- Make software cheap enough to increase affordability.
- Use licenses and certificates to identify original software.
- Set installation passwords that deter illegal installation of software.

COPYRIGHT LAW IN UGANDA

Copyright law in Uganda is currently is governed by;

- the Copyright and Neighbouring Act, 2006 and the
- Copyright and Neighbouring Rights Regulations, 2010.

The Act provides that NO person of any kind shall produce, reproduce, distribute, broadcast, make available to the public, sale or offer for sale, lease or rent out or make public performances or import for distribution ...audio visual recordings in

Uganda except under a licence issued by the owner of the neighbouring rights or a **Collecting society**.

In Uganda, collecting society are catered for under Part VII of the Copyright and neighbouring Act, 2006. Also known as a copyright collecting agency or copyright collective management, the body is created by copyright law which engages in collective rights management. Collecting societies have the authority to license copyrighted works and collect royalties as part of compulsory licensing or individual licenses negotiated on behalf of its members. Collecting societies collect royalty payments from users of copyrighted works and distribute royalties to copyright owners.

In Uganda, the Uganda Federation of Movie Industry (UFMI) is one of the registered and certified Copyright Collecting Society that manages the rights of all the Audiovisual works.

What can be protected by Copyright law?

- Literary works (e.g. articles, novels, pamphlets, books)
- Dramatic works (e.g. scripts for films and dramas)
- Musical works (e.g. melodies)
- Artistic works (e.g. paintings, photographs, drawings, architecture, sculpture)
- Sound recordings
- Films
- Television and radio broadcasts
- Cable programmes
- Performances
- Computer programs
- What works are not protected by Copyright law?
- Ideas, concepts, procedures, methods, public benefit works or other things of a similar nature are not protected by Copyright law.

How is Copyright acquired?

Copyright is recognized and protected at creation.
A created work is automatically protected by copyright as soon as it exists. However the work must be original (it must have been developed independently by its creator) and it must be expressed in material form. Works are protected irrespective of their quality. The Copyright law of Uganda however, further provides that the owner of a copyright and neighboring right may register the right with the registrar for the purposes of keeping evidence of ownership of right, identification of works and authors and maintenance of record of the rights.

What is the procedure for registering a copyright?

- An application for registration must be made to the Registrar of copyright at Uganda Registration Services Bureau (URSB) and an application fee paid.
- The application for must be published in the Uganda Gazette for 60 days.
- If no objection is made to the registration of the said right, a certificate of registration will be issued to the applicant.
- How long does copyright protection last?
- Copyright protection generally lasts for the life of the creator and 50 years after the creator's death. This means that it is not only the creators that benefit from their works, but also their heirs.

COMPUTERS AND SOCIETY

Computers have had a lot of impact in various aspects of society as discussed below.

POSITIVE IMPLICATIONS OF USING COMPUTERS TO SOCIETY

- Created and widened employment opportunities e.g.; software engineers, computer teachers, technicians, etc.
- Improved education and research by simplifying teaching and learning. E.g. abstract content can be made real through cyber science technology – others are computer aided teaching and computer aided learning, presentations software, etc.
- Improved entertainment and leisure through computer games, music, etc for people to refresh and make-up.
- Improved communication and collaboration through computer networks.
- Improved health services where computers facilitate recording, monitoring, and diagnosis for patients.
- Improved security through computer managed gates and monitoring of commercial and domestic premises, detecting and controlling crime by police.
- Reduced production time and manufacturing processes through computer aided manufacturing and computer aided designing which have greatly improved the quantity and quality of life.
- Improved customer services delivery and care eg networked computers provide 24/7 on-line services like credit cards Improved business and investment opportunities.
- Improved data and document production, storage and manipulation.

NEGATIVE IMPLICATIONS OF USING COMPUTERS TO SOCIETY

- **Violation of Privacy:** In many instances, where personal and confidential records stored on computers were not protected properly, individuals have found their privacy violated and identities stolen.
- **Public Safety:** Adults, teens, and children around the world are using computers to share publicly their photos, videos, journals, music, and other personal information. Some of these unsuspecting, innocent computer users have fallen victim to crimes committed by dangerous strangers.

- **Impact on Labor Force**: Although computers have improved productivity and created an entire industry with hundreds of thousands of new jobs, the skills of millions of employees have been replaced by computers. Thus, it is crucial that workers keep their education up-to-date. A separate impact on the labor force is that some companies are outsourcing jobs to foreign countries instead of keeping their homeland labor force employed.
- **Health Risks:** Prolonged or improper computer use can lead to health injuries or disorders.
- **Impact on Environment:** Computer manufacturing processes and computer waste are depleting natural resources and polluting the environment.
- Computer related crime e.g. forgeries, cyberbullying, Piracy etc.
- Increased cost of production as computers are very expensive to buy and maintain. Computer experts can as well be expensive to hire.
- They are many health hazards e.g. can cause eye defects, Tendonitis, RSI, etc.
- Electronic fraud: Stealing money electronically through practices like Credit card cloning and illegal money transfers.
- Hacking: Unauthorized access into computers possibly to access information, compromising privacy. e.g. Wikileaks
- Virus threats which has made data storage and safety very unreliable.
- Loss of employment as they take over job assignments for semi and less skilled job functions.
- Deaths and accidents due to computer malfunctioning or explosion.
- Erosion of human integrity and creativity as even the smallest calculation is assigned to the computer. Other cases are Forgeries, GMFs, test tube children, etc.
- Loss of man-hours as some workers go for unproductive computer based leisure at the expense of their work. Cyber terrorism.
- Moral Decay: The internet has websites with content such as pornography, which have a bad impact on the users especially the young children.
- In politics, ICTs are being used for running new forms of political activism, for example mobilizing masses against to rebel against governments using social media channels like twitter.

HEALTH CONCERNS OF COMPUTER USE

Users are a key component in any information system. Thus, protecting users is just as important as protecting hardware, software, and data. The widespread use of computers has led to some important user health concerns.

A repetitive strain injury (RSI) is an injury or disorder of the muscles, nerves, tendons, ligaments, and joints. Computer-related RSIs include tendonitis and carpal tunnel syndrome.

Tendonitis is inflammation of a tendon due to some repeated motion or stress on that tendon.

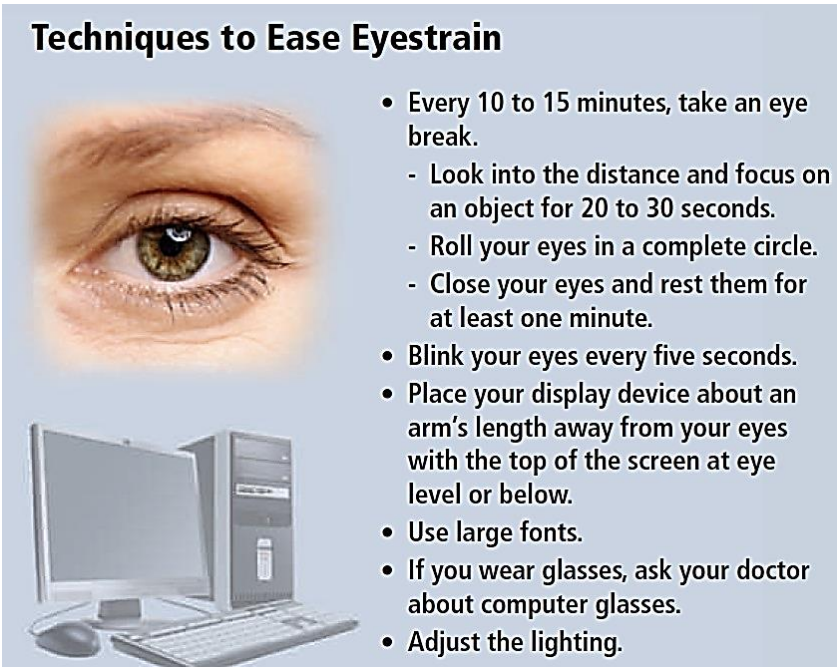
Carpal tunnel syndrome (CTS) is inflammation of the nerve that connects the forearm to the palm of the wrist.

Repeated or forceful bending of the wrist can cause CTS or tendonitis of the wrist. Symptoms of tendonitis of the wrist include extreme pain that extends from the

forearm to the hand, along with tingling in the fingers. Symptoms of CTS include burning pain when the nerve is compressed, along with numbness and tingling in the thumb and first two fingers.
Long-term computer work can lead to tendonitis or CTS. Factors that cause these disorders include prolonged typing, prolonged mouse usage, or continual shifting between the mouse and the keyboard. ***If untreated, these disorders can lead to permanent physical damage***.

You can take many precautions to prevent these types of injuries. Take frequent breaks during the computer session to exercise your hands and arms. To prevent injury due to typing, place a wrist rest between the keyboard and the edge of your desk. To prevent injury while using a mouse, place the mouse at least six inches from the edge of the desk. In this position, your wrist is flat on the desk. Finally, minimize the number of times you switch between the mouse and the keyboard, and avoid using the heel of your hand as a pivot point while typing or using the mouse.

Another type of health-related condition due to computer usage is computer vision syndrome (CVS). You may have CVS if you have sore, tired, burning, itching, or dry eyes; blurred or double vision; distance blurred vision after prolonged staring at a display device; headache or sore neck; difficulty shifting focus between a display device and documents; difficulty focusing on the screen image; color fringes or after-images when you look away from the display device; and increased sensitivity to light. Eyestrain associated with CVS is not thought to have serious or long-term consequences.



People who spend their workday using the computer sometimes complain of lower back pain, muscle fatigue, and emotional fatigue. Lower back pain sometimes is caused from poor posture.

Computer users can protect themselves from health risks through proper workplace design, good posture while at the computer, and appropriately spaced work breaks.

Ergonomics and Workplace Design

Ergonomics is an applied science devoted to incorporating comfort, efficiency, and safety into the design of items in the workplace. Ergonomic studies have shown that using the correct type and configuration of chair, keyboard, display device, and work surface helps users work comfortably and efficiently and helps protect their health. For the computer work space, experts recommend an area of at least two feet by four feet. Figure below illustrates additional guidelines for setting up the work area.

Computer Addiction

Computers can provide entertainment and enjoyment. Some computer users, however, become obsessed with the computer and the Internet. Computer addiction occurs when the computer consumes someone's entire social life. Computer addiction is a growing health problem but can be treated through therapy and support groups.

Symptoms of a user with computer addiction include the following:

- Craves computer time
- Irritable when not at the computer
- Overjoyed when at the computer
- Unable to stop computer activity
- Neglects family and friends
- Problems at work or school

GREEN COMPUTING

Green computing involves reducing the electricity and environmental waste while using a computer. People use, and often waste, resources such as electricity and paper while using a computer.

The United States government developed the ENERGY STAR program to help reduce the amount of electricity used by computers and related devices. This program encourages manufacturers to create energy-efficient devices that require little power when they are not in use. Computers and devices that meet the ENERGY STAR guidelines display an ENERGY STAR label.

Users should not store obsolete computers and devices in their basement, storage room, attic, warehouse, or any other location. Computers, monitors, and other equipment contain toxic materials and potentially dangerous elements including lead, mercury, and flame retardants. In a landfill, these materials release into the environment. Recycling and refurbishing old equipment are much safer alternatives for the environment.

Green Computing Suggestions

1. Use computers and devices that comply with the ENERGY STAR program.
2. Do not leave the computer running overnight.
3. Turn off the monitor, printer, and other devices when not in use.
4. Use LCD monitors instead of CRT monitors.
5. Use paperless methods to communicate.
6. Recycle paper.
7. Buy recycled paper.
8. Recycle toner cartridges.
9. Recycle old computers, printers, and other devices.
10. Telecommute (saves gas).
11. Use video conferencing and VoIP for meetings.

EMERGING TECHNOLOGIES

Definition: **Emerging technologies** are those that are currently being developed or will be developed in the next 5 to 10 years, and which will alter the business and social environment.

ICT is always improving and changing and new technologies are being developed all of the time.

These are many Developments in Hardware, Developments in Software and Developments in Application of computers. The Developments in technology will, by nature, impact on our everyday lives and these include:

a) **Artificial Intelligence (AI)**
b) **Digital forensics**
c) **Biometrics**
d) **Robotics**
e) **Quantum Cryptography**
f) **Computer Assisted Translation (CAT)**
g) **3D and Holographic Imaging (aka holograms)**
h) **Virtual Reality**

Artificial Intelligence (AI)

This is a computer science that is focused on creating computer systems that simulate human intelligence. The term was first used in 1956 by a computer scientist at the Massachusetts Institute of Technology (MIT) who was focused on trying to make computers behave like humans.

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. For example: In 1997 a computer named 'Deep-Blue' defeated a world champion in the game of chess.

Impacts of AI on everyday life:

Some of the impacts that artificial intelligence can have on everyday life are discussed in the table below:

- **Accurate prediction of weather** - AI software will soon be used to sift through weather data more accurately that humans can and will be used to predict approaching storms and automatically issue warnings.
- **Increased leisure time** - Robotic vacuum cleaners are becoming more and more popular. These can detect walls and other objects in order to vacuum around them. People can leave them running whilst they enjoy extra spare time.
- **Safer transport** – Self driving cars already exist will drastically reduce road accidents. Driverless trains too already exist in some countries!
- **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.
- **Improved medical care** - Robotic surgery assistants are being used to quickly and accurately pass the correct surgical tools to doctors. The few seconds saved in getting the correct tool to the doctor can save patient's lives.

Digital forensics

Digital forensics, also called computer forensics, network forensics, or cyberforensics, is the discovery, collection, and analysis of evidence found on computers and networks. Digital forensics involves the examination of computer media, programs, data and log files on computers, servers, and networks.

Many areas use digital forensics, including

- law enforcement,
- criminal prosecutors,
- military intelligence,

- insurance agencies,
- Tax investigations and
- information security departments in the private sector.

A digital forensics examiner must have knowledge of the law, technical experience with many types of hardware and software products, superior communication skills, familiarity with corporate structures and policies, a willingness to learn and update skills, and a knack for problem solving.

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.

- Forensics has led to increased legal use of digital evidence. Digital evidence is information found on a wide range of electronic devices that is useful in court because of its probative value.
- Technology changes evidence. There is still a vigorous debate in the legal world over the usage and reliability of DNA evidence, for example. This is now being mirrored in more recent court challenges over the use of digital evidence.
- Digital evidence tendered in court often fails to meet the same high standards expected of more established forensics practices, particularly in ensuring the evidence is what it purports to be. It is increasingly common for criminal trials to rely on digital evidence. And, regrettably, it is common 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 analyse the iris which is the coloured ring that surrounds the pupil.
- **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.

- Before biometric methods can be useful, people have to perform a process known as 'biometric enrolment'.

- This is where body-part data such as fingerprints or voice patterns are captured and stored within the system so that they can be used to identify the person later on.
- Biometrics are beginning to be used in place of passwords and physical locks as a means of security.
- Biometrics have advantages over these older methods as body parts cannot be lost, forgotten or stolen as can be the case with passwords and keys.

Impacts of Biometrics on everyday life:

Some impacts of biometrics are discussed below:

- **Better airport security** Iris recognition is already in use in some airports.
- Travellers 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 method ensures that only authorised people can enter restricted buildings or rooms.
- **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. They need to be as secure as possible in order to protect the valuable data that they contain. 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 in the table below:

- **Dangerous jobs -** E.g. disposing of bombs, spray painting or cleaning up nuclear waste. Note: these are all jobs that could harm or kill a human.

- **Exploring extreme environments-** E.g. inside volcanoes, planets or the depths of the ocean. Note: humans cannot visit these environments due to lack of oxygen and high pressure / heat levels.
- **Repetitive manufacturing jobs -** E.g. production lines, packing and welding etc.
- Note: these jobs can also be performed by humans but robots can do them much faster and more efficiently.
- **Moving heavy objects -** E.g. installing large engines, moving pallets of items etc.

Robots are increasingly being used in manufacturing due to their proven increase in productivity. Think about it! Robots can work 24/7 and never need to take 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:

Some impacts of robotics are discussed below:

- **Increased personal time** - If robots can carry out domestic chores, this frees up more time for us to spend as we wish.
- This could mean more time spent at work or for more enjoyable activities such as socialising.
- **More efficient manufacturing** Robots can manufacturer products such as cars much faster and cheaper than humans can. This means that companies can make more products at less cost and this means greater business profits.
- **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.
- **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.

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 authorised people are allowed to read it.

Unauthorised people attempting to read the data would see illegible nonsense instead of the real information. Older methods of encryption were based around mathematics but quantum cryptography uses physics instead.

This makes the encryption impossible to break.

In quantum cryptography, messages are encrypted using photons.

These are tiny packets of light.

Impacts of Quantum Encryption on everyday life:

Some impacts of quantum cryptography are discussed below:

- **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 unauthorised ears.
- **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 takes. Current CAT tools are not always 100% accurate. They need a human to check for errors.

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.
- NOTE: Most word-processors allow the user to select the language in which to spell-check.
- **Translation memory software** - Translation memory software are databases which store translated text as the human translator works through it in order to be reused in the future. Translated text is built-up in the database's memory and can be accessed by other translators in order to speed up their translation jobs.
- **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.

If a match is found, translated text will be shown on-screen.

Impacts of Computer Aided Translation on everyday life:

Some impacts of CAT are discussed below:

- **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.
- **A more multilingual society** Anyone with an Internet connection can access tools such as Google Translate and the vast collection of language databases that the tools can search through. This makes accessing other languages much easier than in the past and makes it easier for people to learn these new languages.
- NOTE: Google's new 'Voice Search' facility allows users to actually speak into a tablet or mobile phone and Google will automatically translate (and speak) the words or phrase in almost any language.
- **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 and Holographic Imaging (aka holograms)

This is a technique where images are made to appear three-dimensional and to actually have depth. Holograms work by taking two regular two-dimensional images of the same object and laying one on top of the other. The two-dimentional images need to have been shot at different angles. Two different types of laser beams are used to record the two-dimensional images onto a single photographic plate. This creates one single image that incorporates the angles of the original two-dimensional images. This produces a 3D effect. When viewing the image, human eyes see it from slightly different angles. The brain combines them into a three-dimensional image.

Impacts of 3D imaging on everyday life:

Some impacts of 3D imaging are discussed below:

- **Improved security** - Credit cards, ID cards, software and some bank notes include holograms as a way of trying to prevent forged duplicates being created. NOTE: Forgeries don't usually include a hologram as they are difficult and expensive to reproduce.
- **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. NOTE: 3D movies require the viewer to wear special glasses for the effect to take place. The glasses project two images shot at different angles (one in each eye) and your brain puts them together as one 3D image.
- **Greater data storage** - It is thought that the technology behind holograms will eventually be used to provide the means to store large amounts of data. Companies have already produced discs that use holographic layers that each have the potential to hold a massive 3.9 terabytes. NOTE: This is the equivalent of over 150 standard Blu-ray discs.

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).

As they walk around the virtual environment users will experience things in a similar way to the real world. For example:

- Objects get smaller as you walk away from them (and bigger as you move closer)
- The direction of sounds change as you move around
- Objects in the virtual world appear the same dimensions as they would in the real world (for example dogs are smaller than us but elephants are bigger).

Equipment needed to create the virtual reality experience includes the following:

- **Eye Goggles -** These produce the 3D images that make up the artificial world.
- The goggles project slightly different views into each eye and this fools your brain into thinking that the scene is 3D. Virtual chairs look solid and so on.
- **Special Gloves -** The gloves detect your hand and finger movements which are input into a computer and processed. As users touch or use items in the virtual world, the computer can carry out these commands and make them happen. This allows the user to interact with the virtual world and perform tasks such as moving objects or switching on lights etc.
- **Headphones** - These control what users hear in the virtual world. For example: Distant sounds will be quieter than sounds that are close by.
- **Powerful Computer -** A very powerful computer is needed to create the virtual environment and to process/output data sent into the system by the user's actions. For example: The computer produces graphics that appear as walls, outdoor scenes and objects such as trees.

Impacts of Virtual Reality on everyday life:

Some impacts of virtual reality are discussed below:

- **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. For example: Imagine a new surgeon performing surgery on you and accidentally cutting off your leg!!.
- **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. Virtual buildings will also be able to be tested against factors such as earthquakes to see what effects they would have on the current design. This allows architects to modify designs quickly and cheaply and will, potentially, allow for the development of much larger and safer buildings than we currently have.

- **More effective treatment of phobias** - VR is being used to help patients overcome phobias and anxieties. People can experience a tame, 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 (the virtual spiders would be controlled by the therapy team as well).
- **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.

Review Questions:

1. List 5 technologies that are currently being developed or are emerging.

2a. Describe 3 areas where artificial intelligence is being developed.

2b. Describe 3 impacts that artificial intelligence can have on everyday life.

3a. Explain what 'Biometrics' is

3b. Describe 3 areas where biometric technology is being used.

3c. Describe 3 impacts that biometrics can have on everyday life.

4a. State 3 different types of robot

4b. Describe 3 areas where robots are being used.

4c. Describe 3 impacts that robots can have on everyday life.

5a. Explain what 'Quantum Cryptography' is.

5b. Describe 3 impacts that quantum cryptography can have on everyday life.

6a. Explain what 'Computer Aided Translation' is.

6b. Describe 3 different examples of computer aided translation tools.

6c. Describe 3 impacts that computer aided translation can have on everyday life.

7a. Explain what '3D Imaging' is.

7b. Describe 3 impacts that 3D imaging can have on everyday life.

8a. Explain what 'Virtual Reality' is:

8b. Describe 3 purposes for which virtual reality is being used.

8c. Describe 3 impacts that virtual reality can have on everyday life.

9a. Discuss the reliability of digital forensic evidence in courts of law.

SYSTEMS ANALYSIS

INTRODUCTION

- **What is systems analysis?**

Systems analysis is the separation of a substance into parts for detailed study, examination and interpretation (oxford dictionary). (Substance = business system).

- System analysis is the study of an organization's problem or situation and the specification of business requirements for an improved system.

- **What is systems design?**

Systems design is the detailed specification of a computer based solution to the business requirements. The design includes the programming specifications.

What is systems analysis and design?

- Systems Analysis and Design covers the entire systems development process from: Planning to implementation, maintenance, and evolution. It includes all activities performed to produce an automated IS.

IMPORTANCE OF SYSTEMS ANALYSIS

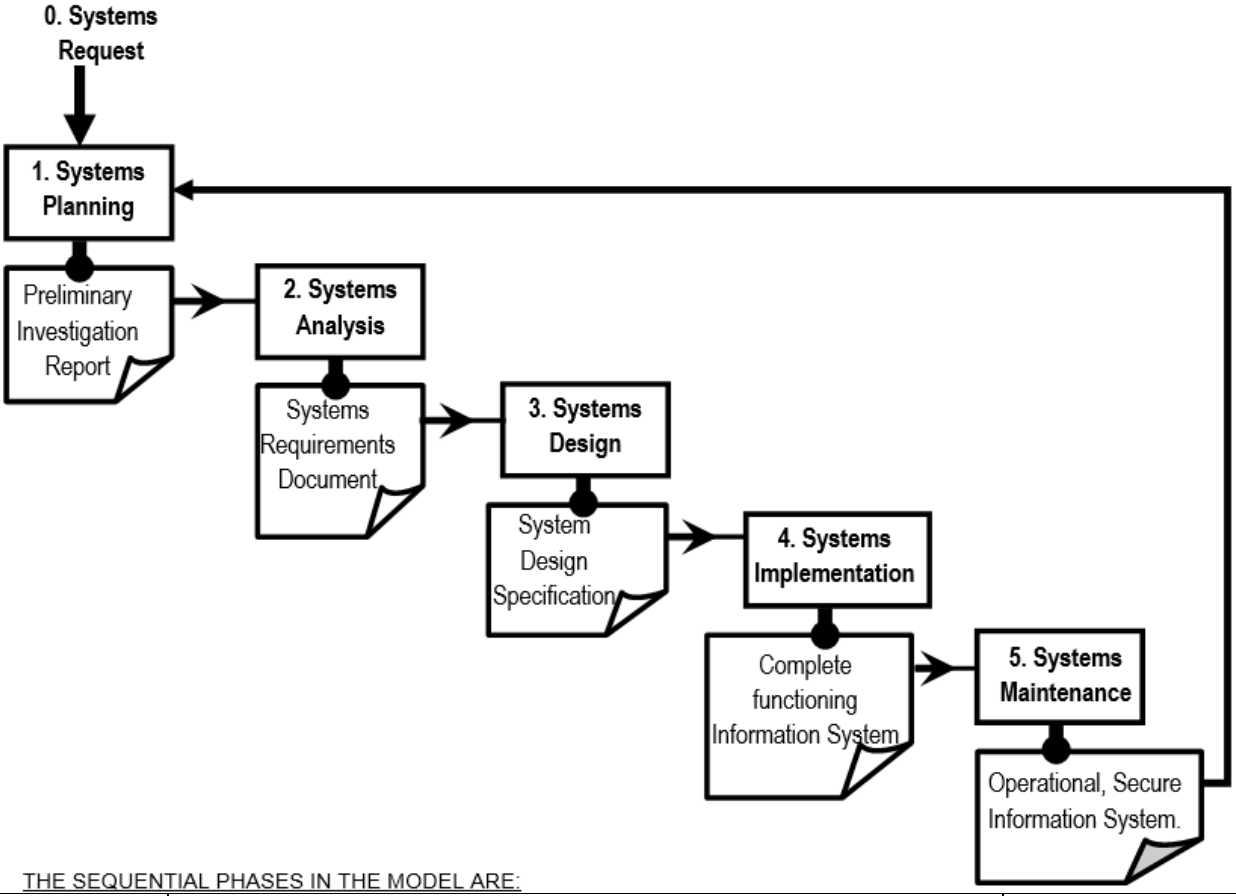
Why Systems analysis?

Projects do not succeed by chance. Successful IT projects follow a systematic "analysis and design" process in order to improve chances of success. Many people would think that software applications development is the actual programming of an application, and that the programming involves programmers writing codes and compiling them to make an application. Few people or users are quite aware that prior to these programmers doing the codes, a systems analysis and design is very critical. Here are the following reasons:

- A systems analysis process involves studying the actual business processes, understand where data is coming from, how it should be processed and what results are required.
- This is to find the bottlenecks in data or in processing that results in performance degradation of an application software.
- To sub-divide a more complex application system so that it can easily be managed.
- Participation of Users: The strategic purpose of the analysis of the system is to seek the acceptance of the people to a new development. System analysis process provides a sense of participation to the people. This helps in breaking the resistance to the new development and it also ensure the commitment to the new system.
- Understanding of Resource Needs: The analysis of the system helps in defining the resource requirements in terms of hardware and software. Hence, if any additional resources are required, this would mean an investment. The management likes to evaluate the investment form the point of view of return on such investment. If the return on the investment is not attractive, the management may drop the project.
- Assessment of Feasibility: The analysis of the system helps to establish its feasibility / viability from different angles. The system should satisfy the technical, economic and operational feasibility.
- System Boundaries: It is necessary to establish the system boundaries which would define the scope and the coverage of the system. This helps to sort out and understand the functional boundaries of the system, the department boundaries in the system, and the people involved in the system. It also helps to identify the inputs and the outputs of the various sub-systems covering the entire system.
- System Importance: It is necessary to understand the importance of the system in the organization. This would throw more light on its utility and would help the designer to decide the design features of the system. It would be possible then to position the system in relation to the other systems for deciding the design strategy and development.
- Nature of The System: The analysis of the system will help the system designer to conclude whether the system is the closed type or open. Such an understanding of the system is necessary, prior to design the process to ensure the necessary design architecture.

PHASES OF SYSTEMS ANALYSIS

The following are the core phases of system analysis basing on the traditional Systems Development Process



THE SEQUENTIAL PHASES IN THE MODEL ARE:

Phase	Explanation	Outputs
Systems Planning Phase	Begins with a formal request to the IT department, called a Systems request. The purpose of this phase is to perform a preliminary investigation to evaluate an IT-related business opportunity or problem. Feasibility study key at this phase and a course of action based on operational, technical, economic, and time factors is recommend after the study.	Preliminary Investigation Report Feasibility Study Recommendations
Systems Analysis Phase	The purpose of the systems analysis phase is to build a logical model of the new system. To understand the system, fact-finding techniques such as interviews, are used to collect facts necessary to build the model. Requirements modeling help to get the systems requirements of the system.	Systems Requirements Document
System Design Phase	The purpose of this phase is to create a physical model that will satisfy all documented requirements for the system. At this stage, you design the user interface and identify necessary outputs, inputs, and processes, plus the internal and external controls.	System Design Specification
Systems Implementation Phase	During the systems implementation phase, the new system is constructed - programs are written, tested, and documented, and the system is installed. This phase also includes an assessment, called a systems evaluation, to determine whether the system operates properly and if costs and benefits are within expectations.	Complete functioning information system

Systems Maintenance Phase	In this phase IT staff maintain, enhance, and protect the system. Maintenance changes correct errors and adapt to changes in the environment, such as new tax rates. Enhancements provide new features and benefits. Security controls safeguard the system from both external and internal threats. A scalable design can expand to meet new business requirements and volumes.	Operational, Secure information system

THE SYSTEM ANALYST

- She or he performs Systems Analysis
- Usually employed in the Information Systems department
- Has Wide ranging skills
- A *system analyst* studies the problems and needs of an Organisation. To determine how people, methods, and computer technology can best accomplish improvements for the business.

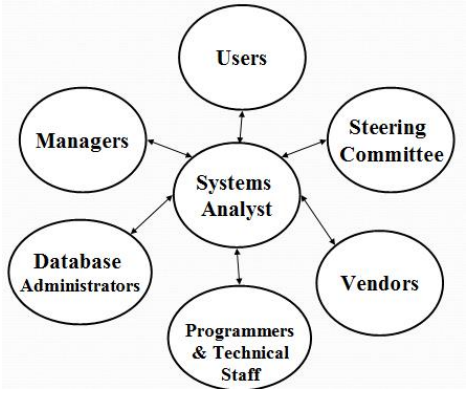
ROLE OF A SYSTEMS ANALYST

1. Investigate how information is used, handled and manipulated in an organization.
2. Identify inefficiencies and ineffectiveness in the current system used by the organization e.g. delays, high operating costs, huge clerical effort and health hazards.
3. Analyze the results of the investigation that will lead to designing the new system.
4. Design a specification of a new system which overcomes the inefficiencies and meets the organization objectives.
5. Oversees the process of testing during the testing of the system.
6. The analyst acts as a *facilitator*.

- He/She interfaces among many different types of people and facilitates the development of computer applications through these people.

NB. These teams in the diagram will be created and disbanded as projects are started and completed or cancelled.

- The analyst may well be the only individual who sees the big picture of the system.



TASKS OF A SYSTEMS ANALYST

Systems analyst tasks include

- Investigation
- Planning
- Understanding
- Communication
- Documentation

QUALITIES OF A SYSTEMS ANALYST

1. Working knowledge of IS Techniques and Technology.
2. Computer Programming Knowledge
3. Problem-solving skills (creativity)
4. Interpersonal Relations skills (confidence, persistent, patience)
5. Interpersonal communication skills
6. Ongoing interest in updating one's knowledge in IT.

STAKEHOLDERS OF AN INFORMATION SYSTEM

SYSTEMS ANALYST SKILLS - BEHAVIOURAL &TECHNICAL

Diplomacy	Being able to say "no" without being " blunt; displaying tact in dealing with others.
Interviewing	Asking the right questions in order to obtain the information needed.
Directing	Giving instructions and communicating user requirements to programming and support staff.
Patience	Continually refining user requirements by requesting - feedback; tolerating lack of computer literacy and specificity.
Assertiveness	Insisting on a course of action or what one believes in, even though it may be unpopular.

Leadership	Getting work done while keeping the team satisfied, effectively giving rewards and punishment.
Programming	Converting system specifications into effective and efficient computer code.
Speaking	Presenting your ideas in a manner easily understood by your audience, both in group meetings and person to person.
Writing	Preparing written documents that accurately communicate ideas in a manner that is easily understood by intended readers.
Listening	Paying attention to and concentrating on what is being said, and asking questions that refine points about which one is uncertain.
Empathy	Being able to understand how others feel; accurately determining what someone else thinks about an issue.
Sales	Promoting the system you advocate; persuading others to accept your viewpoint.
Politics	Understanding what motivates individuals; determining sources of power and influence in an organisation.
Management	Planning, organising and controlling projects so that they get done on schedule and within budget.
Training	Educating users and other non-technical groups on the capabilities of computers and systems.
Cooperation	Working with others productively; resolving conflict in an effective manner.

COMPUTER PROFESSIONS

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, as detailed below:

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.

A good system analyst is one who has at least the following attributes;

- Good problem solving skills and creativity, ie. Must have wide experience in solving problems.
- Good communication skills: The analyst must be able to communicate clearly and precisely both in writing and in speech. He/she must be able to talk to different groups of people e.g managers, operators, attendant and general public.
- Must have business knowledge: the analyst must clearly understand the environment for which the system is being developed.
- Technical knowledge: A system analyst must be well trained in relevant areas of computer science such as hardware, software programing knowledge.

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 continues to grow as more people computerize their workplaces and homes.
- 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

- Computer and electronic engineers are coming up with new and more efficient technologies in information and communication technology almost daily. Since computers are electronic devices, hardware designers must be good in electronic engineering in order to be able to:
- 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

- Large organizations such as insurance companies, banks, manufacturing firms and government agents hire programmers to work together with system analysts in order to:
- 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.
- **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.

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.

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.

System Administrators

- *A 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; The system administrator seeks to ensure 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.