

## COMPUTER SECURITY RISKS

A computer security risk is any event or action that could cause a loss or damage to computers, software, data or information. NB:

**Computer crime:** is any illegal act involving a computer.

**Cyber-crime:** is the online or internet – based illegal acts.

**Computer security risks include;**

1. Internet and network attacks
2. Unauthorized access and use of computer systems.
3. Hardware and software theft
4. Information theft and information piracy.
5. System failure.

### 1.Internet and network attacks

Information transmitted over networks has a higher degree of security risk than information kept on a company's premises.

On a vast network such as the Internet with no central administrator, the risk is even greater.

Below are the most common and most damaging forms of security threats to Internet users and site operators:

- ☞ Malicious code,
- ☞ Unwanted programs,
- ☞ Phishing and identity theft,
- ☞ Hacking and cybervandalism
- ☞ Credit card fraud/theft,
- ☞ Spoofing (pharming) and spam (junk) Web sites,
- ☞ Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks,
- ☞ Sniffing, insider attacks,
- ☞ Poorly designed server and client software.

### 1.MALICIOUS CODE:

Every unprotected computer is susceptible to the attack from malicious code.

**Malicious code** (also called **malware**) includes a variety of threats such

as;

- a. viruses,
- b. worms,
- c. Trojan horses,
- d. Bots, etc.

#### a) VIRUSES

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

**Or**

It is a program which attaches itself to the system and alters the normal functioning of a computer.

- Computer viruses are basically designed to carry out two tasks i.e.;
- ➡ To be able to replicate themselves from one computer to another.
- ➡ To be able to position themselves in a computer system and destroy software programs.
- Each virus code works independently of the “Mother” virus.

### **CLASSIFICATION OF VIRUSES**

Viruses are classified according to their way of hiding.

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

#### **(i) Boot Sector Viruses**

- These execute when a computer starts up.
- These viruses alter the information in the boot sector of a diskette and this causes a computer to display messages like “Non System Diskette, please switch off and start again”.

NB: A **boot sector** is the first sector on a floppy diskette which contains vital information about the diskette’s logical setup.

#### **(ii) Partition Sector Viruses**

These attack the partition sector (first sector on a hard disk which contains information about the disk specifications) of the hard disk and causes the computer not to boot fully.

#### **(iii) File viruses**

These are viruses that attach themselves to program files and are loaded into memory whenever the infected program is run.

#### **(iv) Overwriting Viruses**

These viruses infect files by overwriting the entire or part of a file thereby causing the file not to execute or work as it is supposed to do.

#### **(v) Macro viruses**

- A macro virus uses the macro language of an application (e.g. Word processing, Spreadsheet) to hide the virus code.
- They can cause some tool bar icons to work differently.

#### **(vi) Companion viruses**

Is a virus that works by creating a different file name with an extension **.com**.

#### **(vii) Multipartite viruses**

- These are viruses that use a combination of techniques to infect the different executable files, boot sectors and or partition sectors.
- They are normally difficult to trap.

#### **b) Worms**

- A worm is a computer program that sits in the computer’s memory, rewrites itself continuously into the memory until the system runs out of memory and crashes.
- It differs from a virus in that the “reproduced” segments keep communicating with the “mother” code to function.

c) **Trojan Horse**

- It is a small program code hidden within legitimate software.
- Unlike a virus or a worm, a Trojan horse doesn't have the ability to replicate itself but it is often a way for viruses or other malicious code such as bots to be introduced into a computer system.
- They continue to operate as legitimate software until at such a time that they are activated to cause trouble.

d) **Bots**

Are a type of malicious code that can be covertly (secretly) installed on your computer when attached to the Internet.

Once installed, the bot responds to external commands sent by the attacker, and your computer becomes a “*zombie*,” and is able to be controlled by an external third party.

NB: A **Botnet** is a group of compromised computers connected to a networks such as the Internet that are used for malicious activities such as sending spam, participating in a Distributed Denial of Service attack, stealing information from computers, and storing network traffic for later analysis.

**Other forms of malicious code include;**

e) **Time bomb**

- It is a program code that is activated when it detects a certain condition or event.
- These events can be famous days like Valentine, Fools – day, etc.

f) **Droppers**

- These are programs that have been written to perform useful tasks like compressing files, previewing video clips, etc. and in the process of performing those tasks, they introduce viruses in the system.

g) **Failedviruses**

- These are viruses that have not met there would be goals.
- This may be due to poor programming by the authors.

h) **Packagers**

- These hide the existence of a virus from virus guards by masking some codes around the actual software programs.
- It is only when the virus has been triggered off that you realize that the software had a virus.

i) **Jokes**

- A joke is a harmless program that does amusing actions on the screen.
- They can display messages like “Your computer is about to explode in five minutes. Please run away”.

j) **Test viruses**

- These are viruses written to test some virus guards (antivirus software)
- They are not harmful, just for learning purposes only.

k) **Bugs:**

- A bug is unintentional fault in a program that is normally misinterpreted as a real virus.
- Most complex software in computer systems normally contain bugs.
- Minor bugs normally cause simple inconveniences while major bugs can cause loss of data.

### **How are viruses activated?**

- By opening an infected file
- By running an infected program
- By starting up the computer with an infected floppy diskette.

### **Sources of viruses**

#### ○ **Fake games**

- \* Virus programmers utilize the ability of games spreading so fast to design fake games and attach viruses on them.
- \* These games keep infecting systems as they are installed.
- \* Such games are normally the irresistible like I LOVE YOU, HOTSEX.exe, JACKPOT.com, ROMANCE.exe etc.
- \* Through use of contaminated diskettes on several computers.
- \* Through using pirated software.
- \* Through using freeware and shareware from the internet.
- \* Since these are free, they are good grounds for distributing viruses.
- \* They also in most cases contain **bugs** which may turn into viruses unintentionally.
- \* Through software updates most especially over the internet or other networks.
- \* Through sharing of data in a network.

### **SYMPTOMS CAUSED BY VIRUSES TO SOFTWARE AND HARDWARE**

- Unfamiliar messages appearing on the computer screen.
- Programs taking longer to load than usual.
- Unusual error messages occurring more frequently.
- Reduction in memory than usual
- Flickering of the screen.
- Corrupted files
- File sizes becoming too big or too small than usual.
- Computer system slows down.
- The whole computer system may fail to start up.

### **PRECAUTIONS TO PREVENT VIRUS INFECTION**

- ④ **Do not start a computer with removable media inserted in the drives or plugged in the ports.** CD and DVD drives should be empty, USB ports should not contain a USB flash drive, etc.
- ④ Do not use media like diskettes, backup tapes, CDs from unknown sources.
- ④ **Scan all foreign media for viruses.**  
Before using any removable media, use an antivirus scan program to check the media for infection.
- ④ Isolate any media or computer suspected of having been attacked by viruses, disinfect it and investigate how it may have acquired the viruses.
- ④ **Install antivirus software;**  
Ensure that reputable anti – virus software is installed on all computers.

If employees use computers at home for business or to remotely access the network, these PCs should also have anti – virus software installed on them.

④ **Ensure that the anti – virus software is up to date;**

Every day, new computer viruses are being released and it is essential that business is protected from these viruses by keeping the anti – virus software up to date.

④ **Employ a firewall to protect networks;**

As computer viruses can spread by means other than email, it is important that unwanted traffic is blocked from entering the network by using a firewall.

For users that use computers for business away from the protection of the company’s network, such as home PCs or laptops, a personal firewall should be installed on them to ensure that the computer is protected.

④ **Filter all email traffic**

All incoming and outgoing email should be filtered for computer viruses.

Emails with certain file attachments commonly used by computer viruses to spread themselves, such as .EXE, .Com and .SCR files, should also be prevented from entering the network.

④ **Educate all users to be careful of suspicious e-mails;**

Ensure that all users know to never open an email attachment they are not expecting.

Even when the email is from a known source, caution should be exercised when opening attachments.

④ **Scan internet downloads;**

Ensure that all files downloaded from the internet are scanned for computer viruses before being used.

④ **Don’t run programs of unknown origin;**

All users should be educated to never run a computer program unless the source is known or has originated from a person or company that is trusted and has been authorized by those responsible for managing the company’s network.

④ **Make regular backups of critical data**

It is important to ensure that regular copies of important files are kept either on removable media such as CD-ROM discs or tape to ensure a trusted source for data in the event that the network is infected with a computer virus.

**A backup:** is a duplicate of a file, program or disk that can be used if the original is lost, damaged or destroyed.

## **2.Unwanted Programs:**

These are programs on the internet that install themselves on a computer without the user’s consent. They include;

- ***Adware***

It is a program that displays an online advertisement in a banner or pop-up window on Web pages, email, or other Internet services.

- ***Browser parasite***

It is a program that can monitor and change the settings of a user’s browser.

- ***Spyware***

It is a program placed on a computer without the user’s knowledge that secretly collects information about the user e.g. email address, instant messages, etc.

### **3. Phishing and Identity Theft:**

*Phishing* is any deceptive (misleading/false), online attempt by a third party to obtain confidential information for financial gain.

Some phishing email messages ask you to reply with your information; others direct you to a phony Web site, or a pop-up window that looks like a Web site, that collects the information.

### **4. Hacking and Cyber vandalism:**

A *hacker* is an individual who intends to gain unauthorized access to a computer system.

Some hackers are satisfied merely by breaking into the files of an e-commerce site. Others have more malicious intentions and commit **Cyber vandalism**, intentionally disrupting, defacing, or even destroying the site.

### **5. Credit Card Fraud/Theft:**

Theft of credit card data is one of the most feared occurrences on the Internet.

Fear that credit card information will be stolen frequently prevents users from making online purchases.

### **6. Spoofing (Pharming) and Spam (Junk) Web Sites:**

Spoofing a Web site is also called "*pharming*,"

It involves redirecting a Web link to an address different from the Intended one, with the site masquerading as the intended destination.

**Spam Web sites** are the sites that promise to offer some product or service, but in fact are a collection of advertisements for other sites, some of which contain malicious code.

### **7. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks:**

A *denial of service (DoS) attack* is an assault whose purpose is to disrupt computer access to an Internet service such as the Web or e-mail.

It may involve Perpetrators using an unsuspecting computer to send an influx of confusing data message or useless traffic to a computer network.

The victim computer network eventually jams, blocking legitimate visitors from accessing the network.

DoS attacks typically cause a Web site to shut down, making it impossible for users to access the site.

### **8. Sniffing:**

A **sniffer** is a type of eavesdropping (spying) program that monitors information traveling over a network.

When used legitimately, sniffers can help identify potential network trouble-spots, but when used for criminal purposes, they can be damaging and very difficult to detect.

Sniffers enable hackers to steal proprietary information from anywhere on a network, including email messages, company files, and confidential reports.

### **9. Back Doors and Insider Attacks:**

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.

## **HOW BACKDOORS ARE INSTALLED INTO THE COMPUTERS**

- ⌚ Some worms leave back doors, which have been used to spread other worms.

- ⌚ Programmers often build back doors into programs during system development which help them save development time because the programmer can bypass security controls while writing and testing programs.
- ⌚ A computer repair technician may install a back door while troubleshooting problems on a computer.

### **Insider attacks**

We tend to think the security threats to a business originate from outside the organization.

In fact, the largest threats to business institutions come from insiders.

Normally organizations tend to allow employees access to privileged information, and in the presence of sloppy internal security procedures, they may cause severe damage.

### **10.Spoofing:**

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

#### **Types of spoofing**

- **E-mail spoofing;**

This 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.

- **IP spoofing;**

This occurs when an intruder computer fools a network into believing that its IP address is associated with a trusted source.

Perpetrators of IP spoofing trick their victims into interacting with the phony Web site. For example, the victim may provide confidential information or download files containing viruses, worms, or other malware.

### **11.Poorly Designed Server and Client Software:**

Many security threats prey on poorly designed server and client software, sometimes in the operating system and sometimes in the application software.

Given their complexity and design objectives, all operating systems and application software have vulnerabilities or (flaw) weaknesses that hackers can exploit.

## **DEFENSE AGAINST INTERNET AND NETWORK ATTACKS**

### **□ Install a firewall;**

A **firewall** refers to either hardware or software that filters communication packets and prevents some packets from entering the network.

The firewall controls traffic to and from servers and clients, forbidding communications from untrustworthy sources, and allowing other communications from trusted sources to proceed.

### **□ Route information through a proxy server**

**Proxy servers** are software servers that handle all communications originating from or being sent to the Internet, acting as a spokesperson or bodyguard for the organization. Large companies often route all their communications through a proxy server.

Proxies act primarily to limit access of internal clients to external Internet servers, although some proxy servers act as firewalls as well.

### **□ Install intrusion detection software;**

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

Intrusion detection software automatically analyzes vulnerabilities, identifies any unauthorized intrusions, and notifies network administrators of suspicious behavior patterns or system breaches.

□ **Set of honey pots.**

A **honey pot** is a vulnerable computer that is set up to entice an intruder to break into it.

Some large organizations such as Yahoo, AT&T **use honey pots** so that they can analyze any attack being perpetrated.

These computers, which appear real to the intruder, actually are separated safely from the organization's network.

Honeypots allow the organization to learn how intruders are exploiting their network and also attempt to catch perpetrators who have been doing damage elsewhere on their network.

## 2.UNAUTHORIZED ACCESS AND USE OF COMPUTER SYSTEMS

⌚ **Unauthorized access** is the use of a computer or network without permission, e.g. an employee using a company computer to send a personal e – mail.

⌚ **Unauthorized use** is the use of a computer or its data for unapproved or possible illegal activities.

*a)* **A hacker** refers to someone who accesses a computer or network illegally. Some hackers claim the intent of their security breaches is to improve security.

*b)* **A cracker:**

Cracker 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.

*c)* **Script Kiddie:**

A script kiddie has the same intent as a cracker but does not have the technical skills and knowledge.

Script kiddies often are teenagers that use prewritten hacking and cracking programs to break into computers.

*d)* **Corporate Spies:**

They have excellent computer and network skills and are hired to break into a specific computer and steal its proprietary data and information.

*e)* **Unethical Employees:**

They break into their employer's computers for a variety of reasons.

Some simply want to exploit a security weakness. Others seek financial gains from selling confidential information.

Disgruntled employees may want revenge.

*f)* **Cyber-extortionist:**

A cyber-extortionist is someone who uses email as a vehicle for extortion.

These perpetrators send a company a threatening email message indicating they will expose confidential information, exploit a security flaw, or launch an attack that will compromise the company's network - if they are not paid a sum of money.

*g)* **Cyber terrorist:**

A cyber terrorist is someone who uses the Internet or network to destroy or damage computers for political reasons.

The extensive damage might destroy the nation's air traffic control system, electricity generating companies, or a telecommunications infrastructure.

Cyber terrorism usually requires a team of highly skilled individuals, huge sums of money, and several years of planning.

## **PREVENTION OF UNAUTHORIZED ACCESS**

Unauthorized access is prevented through use of **access controls**.

### **Definition**

An **Access control** is a security measure that defines;

- Who can access a computer
- When the users can access the computer
- What actions the users can take while accessing the computer.

Access control is normally implemented using a two phase process; i.e.

- **Identification**

This is the phase which verifies whether the user is a valid one.

- **Authentication**

This is the phase which verifies that the user is really the one he or she claims to be.

## **METHODS OF IDENTIFICATION AND AUTHENTICATION**

- **User names and passwords**
- **Possessed objects**
- **Biometric devices**
- **Callback systems**

### **i. User names and Passwords;**

A **user name**, or **user ID**, is a unique combination of characters that identifies one specific user.

A **password** is a private combination of characters associated with the user name that allows access to certain computer resources or to a network.

Most multiuser (networked) systems require that users correctly enter a **user name** and a **password** before they can access the data, computer, or a network.

NB: Some Web sites use a CAPTCHA [**Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)**] to further protect a user's password.

A CAPTCHA is a program to verify that user input is not computer generated.

A CAPTCHA displays a series of distorted characters and requires the user enter the characters correctly to continue using the Web site.

### **Characteristics of a good password**

- Should be easy to remember but not too obvious.
- Should be longer, at least eight characters.
- Should have a combination of mixed case letters and digits.
- Should be easy to type without looking at the keyboard.

## **AVOID**

- × Using **your name**, birthday, ID card number or telephone number. A
- × password of all digits or all the same letter.

### **Safeguarding your password**

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

## **ii) Possessed Objects**

A **possessed object** is any item that one must carry to gain access to a computer or computer facility.

### **Examples of possessed objects**

- ✓ Badges,
- ✓ Cards,
- ✓ Smart cards,
- ✓ Key, etc.

These objects are often used in combination with Personal Identity Numbers (PINs)

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

## **iii) Biometric devices**

A **biometric device** authenticates a person's identity by translating a personal characteristic, such as a fingerprint, into a digital code that is compared with a digital code stored in the computer verifying physical or behavioral characteristics.

### **Examples of biometric devices**

#### **◆A finger print scanner**

This captures curves and indentations of a finger print.

#### **◆A hand geometry system**

This measures the shape and size of a person's hand.

#### **◆A face recognition system**

This captures a live face image and compares it with the stored image

#### **◆A voice recognition system**

This device compares a person's live speech with their stored voice pattern.

#### **◆A signature verification system**

This device recognizes the shape of a handwritten signature of a person.

#### **◆An iris recognition system**

It reads patterns in the tiny blood vessels in the back of the eye which are as unique as a finger print.

### **Advantages of biometric devices**

- ✓ Personal characteristics are unique to persons hence give reliable information.
- ✓ These characteristics cannot be lost, forgotten or misplaced.
- ✓ They cannot be copied, duplicated or stolen as the case with possessed objects.

### **Disadvantages of biometric devices**

- Most of the devices are too expensive.
- A finger print scanner might reject a legitimate user if the user cuts his or her finger.
- Hand geometry readers can transmit germs.
- A signature might not match the one on file when the person is nervous.
- A voice recognition system might reject a legitimate user with a sore throat.

**iv) Callback systems**

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

### **3.HARDWARE AND SOFTWARE THEFT**

**Hardware theft**

This is the act of stealing computer equipment.

**Vandalism**

This is the act of destroying computer equipment.

#### **PREVENTION OF HARDWARE THEFT**

- ☞ Use physical access controls such as locked doors and windows.
- ☞ Use cables to lock the equipment to desk, cabinet or floor.
- ☞ Install alarm systems to warn you in case of any intrusion.
- ☞ Use passwords, possessed objects and biometric devices.
- ☞ Install surveillance cameras to help you in easy monitoring of the hardware.

#### **SOFTWARE THEFT**

##### **FORMS OF SOFTWARE THEFT;**

•**Physical stealing of the media** (e.g. floppy diskette, CD ROM e.t.c) that contains the software

•**Software piracy**

This is the unauthorized and illegal duplication of copyrighted software.

### **4.SYSTEM FAILURE**

This is a prolonged malfunctioning of a computer that can cause hardware, software, data or information loss.

**Causes of system failure**

- Aging hardware
- Natural disasters (such as fires, floods, storms or earthquakes etc)
- Electrical power variations

#### **Electrical power variations**

These can cause loss of data or equipment (in case of fire outbreaks)

A single power disturbance can damage multiple systems in a computer network

#### **FORMS OF POWER DISTURBANCES**

**a.Noise**

This refers to any unwanted signal which is mixed with the normal voltage entering the computer.

**b. Under voltage**

This is a situation which occurs when the electrical supply drops below the normal value (e.g. below 220V in Uganda)

**c. Over voltage (power surge)**

It is a situation which occurs when the incoming electrical power increases significantly above the normal voltage.

**d. Brown out**

Is a prolonged under voltage

**e. Black out**

Is a complete power failure

**f. Spike**

Is a momentary over voltage that occurs when the increase in power last for less than one millisecond.

**NB: A surge protector** such as Uninterruptible Power Supply is needed to protect the computer equipment against these disturbances to prevent electric damages that it might cause.

## COMPUTER ETHICS

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

**It encompasses the following areas;**

- a. Unauthorized access and use of computer systems.
- b. Software piracy
- c. Information privacy
- d. Intellectual property rights
- e. Codes of conduct

**a. Unauthorized access and use of computer systems.**

Definitions;

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

**Unauthorized use** is the use of a computer or its data for unapproved or illegal activities.

**These activities include;**

- An employee using a company's computer to send personal email without permission from the managers.
- Gaining access to a bank's computer and perform unauthorized money transfer.

**b. Software piracy**

This refers to the unauthorized and illegal duplication of copyrighted software.

This may involve duplicating someone's movie, song, book, etc, without his/her permission.

**NB:**

Whenever a consumer purchases a software, he/she is only provided with a license agreement which gives him/her the right to use the software.

### **Types of license agreements**

#### **(i) Single user or end user license agreement**

This is the most common license agreement provided to individual users after purchasing a software.

This agreement gives a user a right to; oInstall the software on only one computer Make one copy for backup.

**However, with such an agreement, a user cannot;**

- ✚ Install the software on a network
- ✚ Give away copies of the software to other users.
- ✚ Rent or lease the software.

#### **(ii) Software site license**

This agreement gives the consumer the right to install the software on multiple computers at a single site.

This site may be a school computer laboratory, a company's computer laboratory, etc.

#### **(iii) Network site license**

This allows network users to share a single copy of the software which resides on the network server.

### **Dangers (risks) associated with software piracy**

oIt increases the chance of spreading computer viruses because pirated software in most cases is a target for spreading viruses.

- o The consumer cannot receive any technical support for the software from the manufacturer.
- o It becomes expensive in the long run for all the illegal users.

### **Reasons why software piracy has persisted**

- Legal protection for software doesn't exist
- Laws for prohibiting software piracy are rarely enforced.
- Most buyers believe that they have a right to copy the software they have paid for.

### **c.Information privacy**

**Privacy** is the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state.

**Information Privacy** refers to the individual rights, companies or organizations have to deny or restrict the collection and use of information about them.

### **ONLINE TRACKING DEVICES**

These are methods used by online advertisers, online communities and online businesses to keep track of their visitors' behavior. They include;

## a) COOKIES

A **cookie** is a small text file that a Web server stores on your computer that allows a site to track the actions of its visitors.

E-commerce, Webcasting, and other Web applications often rely on cookies to identify users and track information about viewers, customers, and subscribers.

**NB; Although the cookie resides on an individual's hard drive, it does not interact with other information store on the system.**

### USES OF COOKIES

- Web sites that allow for personalization often use cookies to track user preferences. On such sites, you may be asked to fill in a form requesting personal information, such as your name, postal code, or site preferences.
- A news Web site, for example, might allow users to customize their viewing preferences to display certain stock quotes. Your preferences are stored in cookies on your hard disk.
- Many Web sites use cookies to store users' passwords, so they do not need to enter it every time they log in to the Web site.
- Online shopping sites generally use session cookies to keep track of items in your shopping cart. This way, you can start an order during one Web session and finish it on another day in another session. Session cookies usually expire after a certain time, such as a week or a month.
- Some Web sites use cookies to track how regularly you visit a site and the Web pages you visit while at the site.
- Web sites may use cookie to target advertisements. Your interests and browsing habits are stored in the cookie.

## b) Spyware and Adware

- **Spyware** is a program placed on a computer without the user's knowledge that secretly collects information about the user.

Spyware can enter a computer as a virus or as a result of a user installing a new program.

- **Adware** is a program that displays an online advertisement in a banner or pop-up window on Web pages, email, or other Internet services.
- **Web bug**, is another type of spyware hidden on Web pages or in email messages in the form of graphical images.

Web businesses use Web bugs to monitor online habits of Web site visitors.

## c) Spam

Spam is an unsolicited (unrequested) email message or newsgroup posting sent to many recipients or newsgroups at once. Spam is Internet junk (unwanted) mail.

The content of spam ranges from selling a product or service, to promoting a business opportunity, to advertising offensive material.

### Types of spams

#### i) Spim

This is a spam sent instant messaging *ii*)

#### Spit

This is a spam sent via VoIP **How**

### **to get rid of spams**

- ⌚ Some email programs have built-in settings that allow users to delete spam automatically. Users also can sign up for email filtering from their Internet service provider.
- ⌚ Email filtering is a service that blocks email messages from designated sources. These services typically collect the spam in a central location that users can view at any time.
- ⌚ Using an anti-spam program that attempts to remove spam before it reaches your inbox.

**NB:** The disadvantage of email filters and anti-spam programs is that sometimes they remove valid email messages. Thus, users should review the contents of the spam messages periodically to ensure they do contain valid messages.

### **d) Phishing**

Is a scam (a trick) in which a perpetrator sends an official looking email that attempts to obtain your personal and financial information.

A **phishing filter** is a program that warns or blocks you from potentially fraudulent or suspicious Web sites.

#### **e) Pharming**

Is a scam in which a perpetrator sends an official looking message that requests you to type a Web address in the Web browser, and then redirects you to a phony Web site that looks legitimate which requests you enter confidential information.

#### **f) Employee Monitoring**

Employee monitoring involves the use of computers to observe, record, and review an employee's use of a computer, including communications such as e-mail messages, keyboard activity, and Web sites visited.

#### **g) Content Filtering**

Content filtering is the process of restricting access to certain material on the Web.

Many businesses use content filtering to limit employees' Web access.

These businesses argue that employees are unproductive when visiting inappropriate or objectionable Web sites.

Some schools, libraries, and parents use content filtering to restrict access to minors.

### **Methods used to ensure privacy to data and information i)**

#### **Encryption**

**Encryption** is the process of transforming plain text or data into cipher (unreadable) text that cannot be read by anyone other than the sender and the receiver.

**Or**

It is the process of covering readable data into unreadable characters to prevent unauthorized access.

The receiver needs an encryption key in order to regain the original data sent over a communications channel.

#### **Methods of encrypting data**

- ③ **Transportation;** This involves switching the order of the characters.
- ③ **Substitution;** this involves replacing characters with other characters.

- ③ **Expansion insertion;** this involves inserting characters between other characters.
- ③ **Compaction;** this involves removing characters and storing them elsewhere.

NB:

**An encryption key** is a formula used to decrypt encrypted data back into its original format.

#### **TYPES OF ENCRYPTION KEYS;**

- **Private key encryption**

With this key, both the sender and the recipient use the same secret key to encrypt and decrypt the data.

- **Public key encryption**

With this key, a public key encryption software generates both the private key and the public key.

The sender uses the receiver's public key to encrypt the message and the receiver uses his or her private key to decrypt the message.

- d. **Information accuracy**

Millions and millions of information reside on websites of certain organizations. But in some instances, the website providing access to information may not be the one which created it.

Some of the information on these websites may not be 100% accurate.

Therefore, it is always good to evaluate and analyze the information provided on a web page before using it.

- e. **Intellectual property rights**

- i. **Intellectual property rights**

**Intellectual property (IP)** refers to unique and original works such as ideas, inventions, art, writings, processes, company and product names, and logos.

Intellectual property rights are the rights to which creators are entitled for their work.

- ii. **Copyright**

Is the protection given to the author of an original piece, including "literary, dramatic, musical, artistic and certain other intellectual works," whether the work has been published or not.

A copyright gives authors and artists' exclusive rights to duplicate, publish and sell their material. These material may be songs, movies or books.

However, governments of some countries have come up with copyright laws which usually give the public a fair use to copyrighted material.

- iii. **A trademark**

A trademark protects a company's logos and brand names

- f. **Codes of conduct**

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

Recognizing that individuals need specific standards for the ethical use of computers, a number of computer-related organizations have established IT codes of conduct, which helps determine whether a specific computer action is ethical or unethical;

### **SAMPLE IT CODES OF CONDUCT**

- Computers may not be used to harm other people
- Users may not interface with other's computer work
- Users may not intrude in other's computer files
- Computers may not be used to steal
- Computers may not be used to bear false witness
- Users may not copy or use software illegally
- Users may not use other's computer resources without authorization
- Users may not use other's output
- Users shall consider the social impact of programs and systems the design
- Users should always use computers in a way that demonstrates consideration and respect for other people.



### **GREEN COMPUTING**

**Green computing** is the study and practice of environmentally sustainable use of computers and related IT resources.

Or

**Green computing** is the study and practice of designing, manufacturing, using, and disposing of computers, servers, and associated subsystems such as monitors, printers, storage devices, and networking and communications systems efficiently and effectively with minimal or no impact on the environment.

### **Goals of green computing**

- ⌚ Reduce the use of hazardous materials,
- ⌚ Maximize energy efficiency during the product's lifetime,
- ⌚ Promote the recyclability or biodegradability of malfunctioning products and factory waste.

The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment.

### **Here are some steps that can be taken:**

- ❖ Create a power plan which allows the system to automatically turn off components such as monitors and hard drives after set periods of inactivity.
- ❖ Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times. Avoid using the computers for long periods of time as this may lead to health and safety problems.
- ❖ Power-up and power-down energy-intensive peripherals such as laser printers, scanners, etc. according to need.

- ❖ Use liquid-crystal-display (LCD) monitors rather than cathode-ray-tube (CRT) monitors. This is because, CRT monitors emit a lot of electromagnetic radiations.
- ❖ Use notebook computers rather than desktop computers whenever possible. Notebooks computers consume less energy, emit very little heat and other electromagnetic radiations.
- ❖ Minimize the use of paper and properly recycle waste paper.
- ❖ Recycle computing equipment as this can keep harmful materials such as lead, mercury, and hexavalent chromium out of landfills.
- ❖ Dispose of e-waste according to federal, state and local regulations.
- ❖ Implement telecommuting (in which workers can accomplish much of their work away from their standard work places preferably from home). This reduces greenhouse gases emitted during travel, increases worker satisfaction and increases profit margins as a result of lower costs for office space, heat, lighting, etc.
- ❖ Terminal servers should be used instead of standalone computers. This cuts down power consumption to around 1/8 the amount of energy of a normal workstation, resulting in a decrease of energy costs and consumption.

### Questions

1. Explain what is meant by the following terms.

- a. Phishing
- b. Pharming
- c. Spam.

## DATABASE SOFTWARE (PAPER TWO)

### A database

It is a collection of related information stored for a particular purpose.

#### Examples of databases

- Telephone books (directories)
- Customer address books
- Employee information forms
- Dictionaries
- Television guides etc.

A software one needs to create a database is called a **Database Management System(DBMS)**

### Database Management System

- It is the software which allows a user to create, access and manage a database.
- It facilitates creating and maintaining a collection of information and producing reports from it.

#### Examples of DBMS

- Dbase I, II, III, IV, V
- Microsoft access
- Oracle
- Lotus Approach
- SQL (Structured Query Language)
- Microsoft Visual FoxPro
- Lotus Approach
- Borland dBase
- Corel Paradox
- Claris File Maker pro e.t.c.

## MICROSOFT ACCESS

It is one of the most common database applications on the market today.

Features of a Microsoft Access Document

### i. A table

It is a primary element for collecting data that relates to a particular subject and it organizes data into rows (records) and columns (fields) similar to an electronic worksheet.

**Consider the table below**

Rows (record).

column(field)

No	Name	Sex	District	Allowance
1	Mary	F	Kampala	10,000/=
2	Martin	M	Masaka	20,000/=
3	John	M	Mubende	10,000/=
4	Peter	M	Tororo	30,000/=

**ii. A record**

Is a row in a table that contains information about a given person, product or event.

E.g. one which contains 1, Mary, F, Kampala, 10,000/=

**iii. A field**

It is a column in a table that contains a specific piece of information within a record. E.g. Sex, F, M, M, M.

**iv. The table structures**

Is the number of fields, field names, field lengths and data types in the database table.

**v. Field name (Field Labels)**

Is a title of a particular column (field).

E.g. titles like ID No, Name, Sex, District, Allowance.

**vi. Field Length**

Is the maximum number of characters that can be stored for data in a particular field.

**vii. Data type (Field Type)**

It specifies the type of data that the field can contain

**THE COMMON DATA TYPES**

**•Auto Number**

Is a number that is automatically assigned randomly to a particular record and never changes again.

**•Currency**

Is a numeric field automatically assigned a currency sign.

**•Date / Time**

Can hold month, day and year information.

**•Text type**

May hold letters, numbers or special characters.

**•Numbers**

Holds any figure that need to be used for calculations.

**•Memo type**

May hold text of any type or length.

Holds whole sentences up to 64,000 characters including spaces

**•Hyperlink**

Stores data types that are internet addresses

**•Look up**

Stores values that are from an external table, query or a list of specified values.

**•OLE Object (Object Linking and Embedding)**

Holds any linked object e.g. a picture, sound or a photograph.

**•Boolean type**

This may hold values that are either true or false.

**viii. Field properties**

It refers to specific characteristics of a particular field. It includes;

- Field size
- Caption
- Input mask
- Format
- Decimal places
- Required input mask
- Default value
- Allow zero length e.t.c

<b>Use this field property</b>	<b>To</b>
Field Size	Determines the amount of space that is allocated for each value. Set the maximum size for data stored as a Text, Number, or AutoNumber data type.
Format	Customize the way the field appears when displayed or printed.
Decimal Places	Specify the number of decimal places to use when displaying numbers.
New Values	Set whether an AutoNumber field is incremented or assigned a random value.
Input Mask	Display editing characters to guide data entry.
Caption	Set the text displayed by default in labels for forms, reports, and queries.
Default Value	Automatically assign a default value to a field when new records are added.
Validation Rule	Supply an expression that must be true whenever you add or change the value in this field.
Validation Text	Enter text that appears when a value violates the Validation Rule expression.
Required	Require that data be entered in a field.
Allow Zero Length	Allow entry (by setting to Yes) of a zero-length string ("") in a Text or Memo field.
Indexed	Speed up access to data in this field by creating and using an index.
Unicode Compression	Compress text stored in this field when a large amount of text is

Use this field property	To
	stored (> 4,096 characters)
IME Mode	Control conversion of characters in an Asian version of Windows.
IME Sentence Mode	Control conversion of characters in an Asian version of Windows.
Smart Tags	Attach a smart tag to this field.
Append Only	Allow versioning (by setting to Yes) of a Memo field.
Text Format	Choose Rich Text to store text as HTML and allow rich formatting. Choose Plain Text to store only text.
Text Align	Specify the default alignment of text within a control.
Precision	Specify the total number of digits allowed, including those both to the right and the left of the decimal point.
Scale	Specify the maximum number of digits that can be stored to the right of the decimal separator.

#### **ix. Queries**

These are tools used to locate specific records within the table or ask questions to your database.

#### **x. Forms**

These are tools that enable one to enter and display records from the database tables easily. They can be used to enter data in many tables at the same time.

#### **xi. Reports**

Are tools that enable one to preview and print data in a meaningful format.

#### **xii. Macros (Mini programs)**

These are tools used to automate the way one uses his database.

Macros can be used to instruct the computer to print specific reports at a given time.

#### **xiii. Modules**

These do the same work as a macro.

They enable one to automate work processes.

### **What is a primary key?**

A primary key is a field that uniquely identifies a record in a table. Before saving a table, you should insert a primary key.

### **Characteristics of a good primary key**

1. It uniquely identifies each row.
2. It is never empty or null — there is always a value.
3. It rarely (ideally never) changes. Access uses primary key fields to quickly bring together data from multiple tables.

### **Types of keys commonly known in databases**

1. Foreign key: A key used in one table to represent the value of a primary key in a related table.
2. Composite Primary Key: a primary key that is made up of more than one feature.
3. Surrogate Primary Key: a system assigned primary key generally numeric and auto-incremented
4. Candidate Key: a minimal super key that does not contain a subset of features that it itself a super key

## **CHARACTERISTICS OF DATABASES**

- ④ The data is arranged in columns (fields) and rows (columns)
- ④ Each column has similar data items.
- ④ Each row contains information belonging to a single individual.

### **Qualities of a good database**

- ③ Should make use of the computer resources
- ③ Should be fast
- ③ Should interface smoothly with existing facilities
- ③ Should be updatable
- ③ Should provide easy access to authorized users
- ③ Should preserve data integrity

- ③ Should ensure the privacy of data

## **FUNCTIONS OF DATABASES**

### **i). Sorting**

It involves organizing a set of records in a particular order

The order can be ascending or descending order and by alphabetic or numeric order.

### **ii) Browsing (searching)**

It involves the ability to extract information of general interest from a database

### **iii) . Report generation**

A report generator allows one to create formatted reports which include headings, sub – headings, columns of data from the database, columns of data that are compiled from existing fields in the database and final totals etc.

**iv)**Databases are powerful and easy to use when creating information.

**v)**They are used to organize and manage a collection of related information (data)

**vi)**They provide the user with the means of managing and manipulating large amounts of data.

## **FACTORS TO CONSIDER WHEN DESIGNING A DATABASE**

- The number of tables needed.
- The number of fields and the field names.
- Unique identifiers of fields with unique vales.
- Relationships between the tables if any.
- Practicability of the database.

## **TYPES OF DATABASES**

### **1. Flat file database**

- It is a database made up of only one table
- It is easy to set up and use

### **2. A relational database**

- It is a database which can take information from two or more database tables and combine them into a new table or report.

#### **NB: A relationship**

It determines the way in which the details in one table are related to the details in another table.

It can be a one to one relationship, one to many or many to many relationships.

### **3. Hierarchical database**

It uses a structure in which records are divided into segments.

Each record contains one root segment and a variable number of subordinate segments that define a field within a record.

### **4. The network databases (Online databases)**

- It uses a linked list structure
- Combines records with links which are called pointers

- The pointers physically establish the relationships between records.

## Other terms related to databases

### i. Validation

Is the process of checking of input data for errors (e.g. data type) before processing.

#### Examples of data validation techniques;

- Range check;** is to make sure that the data entered lies within a certain range.
- Type check;** is to make sure that the data entered is of the correct type (e.g. numeric or alphabetic)
- Length check;** is to make sure that the numbers of characters entered is within the limit
- Presence check;** is to make sure that data is actually present
- Check digit;** is an extra digit appended to a code consisting of a series of numbers or character to detect errors arising from transcription

### ii. Data verification

Is the checking for mistakes when data is copied from one place to another.

#### Examples of data verification techniques

- Visual check
- Enter the data twice by the same person or by two different persons.

### iii. Data redundancy

Is the repeating of data in more than one file.

## Advantages of database system

### ④ Reduction of data redundancy

Databases allow storing most of the data in one place. This leads to less duplication and memory needed.

### ④ Ensures data integrity

Since data is centralized, fewer updating errors can occur and greater accuracy can be maintained

### ④ Ensures data independence

- Data is entered, stored, modified and accessed by methods that are not affected by application programs.
- Changes made to data structures usually do not require changes in programs that access the database

### ④ Data sharing and integration

Database systems offer users the ability to combine data in many ways.

### ④ Centralization of security

It is easier to limit access to information if it is grouped together instead of being kept in several scattered files.

### ☺ **Improvement in access of data**

They allow users to query the database directory without necessarily using an application program.

### ☺ **Reduction of costs**

- Data entry, data storage and development of new application programs are made more economical
  - Also, elimination of data duplication minimizes costs of maintenance.

## **Disadvantages of database system**

### ③ **Complexity**

- They include sophisticated software packages that may require special hardware
- They are also difficult and time consuming to develop.

### ③ **Initial expense**

Because of their complexity and efficiency, database systems can be expensive to set up.

### ③ **Vulnerability**

Data in a database may be more susceptible to sabotage, theft or destruction

### ③ **Need for substantial conversion effort**

- Changing from a traditional file-oriented system to a database system can often involve large scale reorganization of data and programs.
- This normally creates user resistance

## **What is a query criterion?**

Criterion is a rule or an expression that identifies the records that are to be retrieved in a database. Criterion can be classified depending on the data types entered in the database.

- Criteria dealing with text data
- Criteria dealing with values/ numbers/ figures
- Criteria dealing with date/time values

Using the employee table below let's look at the different criteria

Name	Sex	Date of birth	District	Salary	Telephone. No
Abigaba	M	02/06/1988	Hoima	20000	0778452369
Barongo	M	08/04/1995	Kampala	274000	0751235689
Chellangat	F	02/02/2000	Arua	360000	0714578623
Atuhaire	F	04/04/1975	Lira	50000	0417823256
Babirye	F	03/04/1990	Hoima	560000	0772457842
Tuhaise	M	04/06/1999	Kasese	100000	0771235654
Kembabazi	F	05/06/1988	Mbale	780000	0754121000

## **TEXT CRITERIA**

<b>CRITERIA</b>	<b>RESULTS</b>
Like "Barongo"	Returns all employees called Barongo
Not "Barongo"	Returns all other names of employees apart from Barongo
Like "A*"	Returns all names of employees that begin with letter A
Not Like "A*"	Returns all names of employees that begin with other letters apart from A.
Like "*A"	Returns all employees that have names that end with letter A.
Not Like "*A"	Returns all employees whose names end with other letters other than A.
>="Atuhaire"	Returns all names beginning with Atuhaire and continuing through the end of alphabet.
Like "[A-K]*"	Returns names that start with letters A through K.
"Atuhaire" or "Babirye"	Returns records for Atuhaire and Babirye
Len([name])>6	Returns all names with more than six characters.

### VALUE CRITERIA

<b>Criteria</b>	<b>Results</b>
10000	Returns employees that earn 10000
Not 10000	Returns employees that don't earn 10000
<10000	Returns employees that earn less than 10000
>10000	Returns employees that earn more than 10000
>=10000	Returns employees that earn greater than or equal 10000
20000 or 10000	Returns employees that earn 20000 or 10000
>10000 and <50000	Returns employees that earn between 20000 and 10000
In(100, 250, 1000)	Returns employees that earn 100, 250 or 1000
Like "*600"	Returns employees that earn salary that ends with 600 eg.5600,127600, 1234600 etc
like "600*"	Returns employees that earn salary that begins with 600 eg.6000,600400, 6000000 etc

### DATE/TIME CRITERIA

For access to distinguish between text, values and date/time values a character # is added to surround the date/time value. For instance using our table;

<b>Criteria</b>	<b>results</b>
#2/4/1988#	Employee born on 2/4/1988
Not #2/2/1988#	Employees not born 2/2/1988
< #2/2/2006#	Employees born before 2/2/2006
> #2/6/2001#	Employees born after 2/6/2001
>#3/9/1995# and <#4/4/2007#	Employees born between 3/9/1995 and 4/4/2007
<#3/9/1967# or >#7/4/1996#	Born before 3/9/1967 or after 7/4/1996
DatePart ("m", [Date of birth]) = 12	Employees born in December
DatePart ("q", [Date of birth]) = 1	Employees born in the first quarter of the year i.e. Jan, Feb, march

Date()	Current date
Date()-1	A day before the current date
DateDiff ("yyyy", [Date of birth], Date()) > 22	Age greater than 22
<DateAdd("yyyy", -22, Date())	Age greater than 22

### EXAMPLES FOR PRACTICE

1. Open a database program of your choice and key in the following records. Save your project as **point\_of\_sale**. (02 marks)

ProductID	Product_Name	Section	Shelf No.	Quantity_In	Unit_Price
MSM-012	Geisha	Lower	A12	2,500	3,800
MSM-200	Roll On (Rexona)	Lower	B14	1,000	4,000
MSM-150	Sausage (500ml)	Upper	A13	3,200	800
MSM-036	Tooth pick (tins)	Lower	B17	1,000	350
MSM-100	Rotatrim (reams)	Upper	A20	470	18,000
MSM-450	Nataraj black (pkt)	Upper	B11	560	12,000
MSM-362	Back bag (pcs)	Lower	C10	150	50,000
MSM-011	Conflex (pkt)	Upper	A15	2,000	4,000
MSM-098	Pencils (pkt)	Lower	A22	1,000	2,500

- (a). Create a table saved as **point\_of\_sale**. Remember to use appropriate data types. (05 marks)
- (b). Insert *compose primary keys* in your database table. (02 marks)

- (c). Design a form you will use to enter the above records in the table. Save the form as **Point\_Form**. (02 marks)

- (d). Create *three* queries that will return products whose:

- (i). Shelf Number begins with letter A and **Quantity\_In** is less than 2,500. Save the query as **lettera**. (02 marks)

- (ii). **ProductID** is between 001 and 200. Save the query as **productid**. (02 marks)

- (iii). **UnitPrice** is more than 10,000. Save the query as **morethan**. (02 marks)

- (e). Design a report that groups products by **Section** and sorts by **Product\_Name**. Save the report as **groupandsort**. (02 marks)

### QUESTION TWO

Your school has decided to keep records of all food items to be kept in the store. You are then tasked to design a database called **Dining Records** and within your database you create the table called **Food Store** as below:

StockNo	Item	Category	ManDate	Quantity	Price
ST01	Maize Flour	Grain	22/3/2017	20	50000
ST02	Salt	Spice	12/4/2014	4	2000
ST03	Rice	Grain	14/4/2015	60	140000
ST04	Blue band	Oil	23/1/2018	7	3000
ST05	Beans	Grain	13/8/2011	24	40000
ST06	Royco	Spice	17/4/2009	13	4000
ST07	Kimbo	Oil	18/1/2018	11	6000
ST08	Ginger	Spice	16/8/2016	4	7000
ST09	Tea	Spice	14/7/2011	3	6000
ST10	Cinnamon	Spice	12/2/2010	8	8000

**Required:**

- a) Now that your Head teacher has given you a job to create the database and its table as indicated above. In the table design, ensure the following set field properties:
  - i. Select the appropriate field and make it the primary key **(01 mark)**
  - ii. Allocate appropriate data types in all fields of your table **(03 marks)**
  - iii. Set the fields **StockNo**, **Item**, **Category** to field size of **4**, **15** and **10** respectively. **(03 marks)**
  - iv. Set the **Price** field to be displayed using **UGX** monetary units. **(02mark)**
- b) Create a professional form based on your table in design view and your form should have the following
  - i. A header, using the name of your school with 18 font size. **(02 marks)**
  - ii. A closing button set at the right upper side of your form. **(01 marks)**
  - iii. A calculated **Total Price** field by taking **(Quantity \* Price)** **(02 marks)**
  - iv. Include a background color of your choice. **(01 marks)**
  - v. Save your form and name it as **SchoolEntries**. **(01 mark)**
- c) Create a query to display all spices that cost below 5000 Ugandan Shillings. Name your query as **Spice less 5000**. **(06 marks)**
- d) Use a query to calculate the Item Age from the time it was manufactured to date and your new calculated age field should be **Item Age**. Save your query as **Item time Lapse**. **(04 marks)**

**END ENDS**

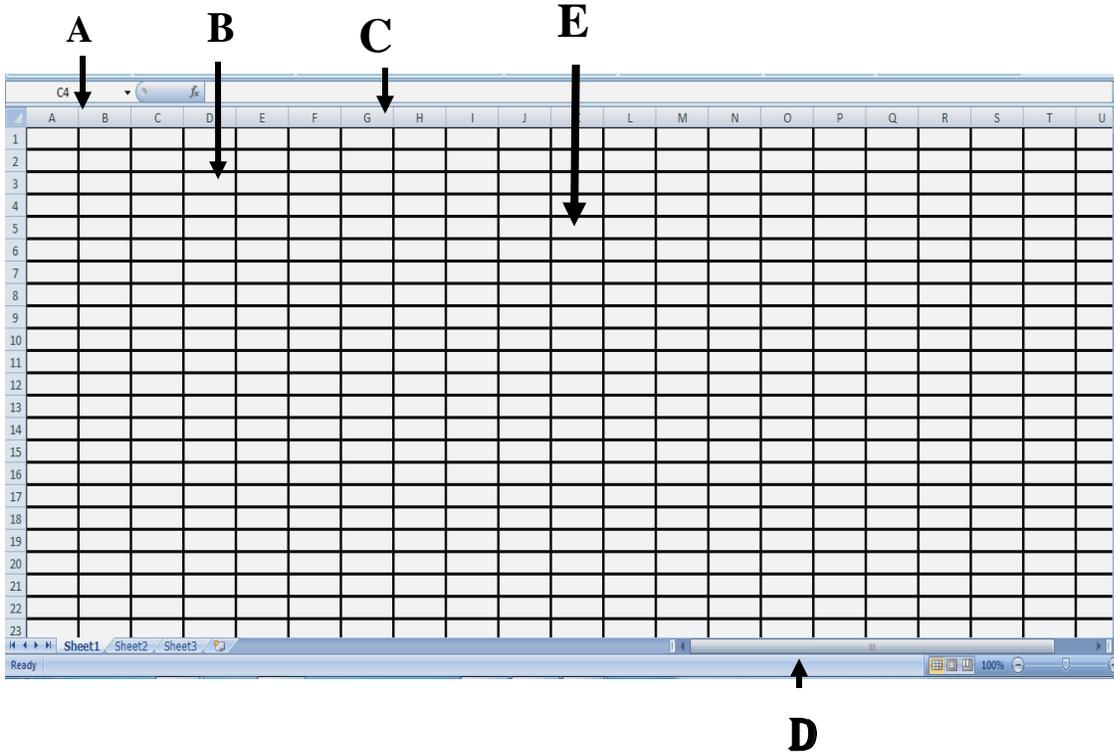
**ST. LAWRENCE ACADEMY, SCHOOLS AND COLLEGES**  
**S.4 COMPUTER STUDIES TOPICAL TEST**

**DURATION: 1HR and 45 MINS**

**INSTRUCTION:**

**Attempt all questions.**

1. Study the screen shot below and answer its related questions:



a) What is the **role** of part **A**.

**(1 mark)**

.....  
 .....

b) **Name** parts **C** and **D**.

**(2 marks)**

**C:** .....

**D:** .....

c) What is the **name** of the cell labeled **B**.

**(1 mark)**

.....  
 .....

d) Give the **absolute name** of cell labeled **E**

**(1 mark)**

.....  
 .....

e) Use the following spreadsheet chart to answer questions below:

	A	B	C	D	E	F
1	<b>Name</b>	<b>English</b>	<b>S.S.T</b>	<b>Maths</b>	<b>Science</b>	<b>Total</b>
2	Mwoso D	70	100	20	55	
3	Swabulin M.	58	64	25	15	
4	Kintu S.	65	25	88	58	
5	Wandalo D	74	77	88	25	
6	Nalweyiso A.	36	88	59	81	

(i). Write the data type used in the range B2:B6?

*(01 mark)*

.....  
 .....

(ii) write a formula to compute an average mark for Nalweyiso? *(01 mark)*

.....  
 .....

(iii) How many cells are in the range A2:C6?

*(01 mark)*

.....  
 .....

(iv). State two ways data in cell range A1:D1 can be emphasized?(2marks)

.....  
 .....

2. (a) Define the following terms as used in database programming:

(i). Record

*(01 mark)*

.....  
 .....

(ii) Field

*(01 mark)*

.....  
 .....

(iii) Database

*(01 mark)*

.....  
 .....

(b) State two advantages of using an electronic database over a manual database. (02 Marks)

.....  
 .....  
 .....  
 .....

.....  
 d).The manager of Muvule supermarket uses a database to store data about groceries they sell as reflected in the part of the database below. Use it to answer questions that follow:

BARCODE	PRODUCER	GROCERY	NUMBER IN STOCK
0049179000794	Herbot	Frozen carrots	412
0027200190653	AVet	Chicken	725
0010029000016	Uwana	Margarine	578
0014559021017	Maaa	Garlic Powder	306
00104790012133	Muawo	Pumpkin Powder	613

(i) How many records are there in this part of the database?(01 mark)

.....

(ii) How many fields are there in this part of the database?(01 mark)

.....

(iii) If the records in the database are sorted in descending order of NUMBER IN STOCK, what will be the barcode of the first record in the database after it has been sorted?  
 (01 marks)

.....  
 .....

(iv) Give the name of the field that contains numeric data. (01 mark)

.....  
 .....

(v) Explain why the manager assigned BARCODE as the primary key. (01 mark)

.....  
 .....  
 .....

3. (a) (i) What a wild card is in database management system. (02 Marks)

.....  
 .....

(ii) State any two importance of a wildcard in a query criterion. (02 Marks)

.....  
.....  
.....  
.....

(iii) Name four examples of frequently used wildcards in database. (04 Marks)

.....  
.....  
.....  
.....

(iv) Explain the following field properties as used in database design. (02 Marks)

(i) Caption.....  
.....  
.....

(ii) Input mask.....  
.....

(v). Give **three** requirement of a good primary key field in a database table. (01 mark)

.....  
.....  
.....  
.....

**QUESTION:4**

Describe the logical way of connecting the following computer tools to have a working computer system and state the step by step way of switching on the computer  
Monitor,  
mouse,  
keyboard,  
two power cables,  
uninterruptible power supply(UPS),  
system unit,  
VGA cable,  
wall socket

**END**

