COMPUTER STUDIES NOTES

FORM 2

**Data Security Threats**

This is the danger of an attack on a computer system either by a computer program, an event or a person. This causes loss of data/information and attacks the data privacy. The following are the main threats to data security: Unauthorized access, Virus and Worm attacks, Computer errors and accidents.

**Unauthorized Access**

Physical and logical unauthorized access   
  
***i) Physical unauthorized access***This involves persons have illegal entry to the building/computer room or the persons having physical access to the storage media i.e. hard disks, compact disk etc. the motive could be either to steal the computers or information or maliciously damage, change or alter, delete data/information.   
  
***ii) Logical unauthorized access***involves gaining illegal access into a computer system. It could be deliberate or accidental. Illegal access could be with an intention to steal, delete, copy, and alter data/information.   
Virus and Worms Attack

**Computer Viruses**  
A computer virus is a malicious and destructive program, hidden in an existing program. When the infected program is run, the virus code is activated and copies itself onto other files in the computer. Viruses are passed in two ways: by removable storage media and by network removable storage media. When infected media are used in different machines, they can pass on the virus to uninfected machine  
  
**Virus Infecting Machines**

When computers are networked and sharing resources there is a possibility of the virus being passed on through the network  
  
**Types of viruses**Viruses may take several forms. These may include:  
Boot-Sector virus, File virus and Macro virus.  
  
**Boot Sector Virus**These viruses affect the booting instructions of a system by replacing the instructions with their own. That is, the computer fails to start up normally.   
  
**File Virus**These viruses attach themselves to executable files. That is, those files that actually begin a program. For example, when an infected program is run, the virus gets into the main memory from where it can infect other executable files  
  
**Macro virus**These are types of computer viruses that are spread to other computers through software programs that utilize macros. For example, Microsoft Word and Microsoft Excel are two popular and widely used programs that are capable of executing macros. Macro viruses written for these programs can quickly spread by infecting other related documents each time the document is open. Because these types of files are commonly used and sent through e-mail, a computer network can be quickly infected by these viruses.  
Polymorphic Virus  
This is a type of a virus that changes its instructions each time it infects a new file. That is-it mutates. This makes it extremely difficult to detect and clean as it changes every time it copies itself.  
Trojan Horse and Logic Bomb  
Other programs that are harmful to computers are Trojan Horse and Logic Bomb  
Trojan horse are programs that are set to go off at a certain date and time resulting in the destruction of data. For example a disgruntled employee in a company created a bomb in a program that was supposed to go off two months after he left.  
Logic Bomb is a malicious program that hides itself in a harmless program in such a way that it can control and do damage to the computer system. It does this in the background as the harmless program runs without the knowledge of the user.  
  
Computer Worms  
A computer worm is a program which copies itself across a network.  
It differs from a computer virus in that it can run itself. A virus needs a host program to run, and the virus program runs as part of the host program. A computer worm can spread without a host program. Firewalls are used to prevent spread of computer worms.  
a firewall   
Email Worms   
These are worms that spread via infected email messages. Any form of attachment or link in an email may contain a link to an infected website. Infection can be in two ways that is - it can be activated when the user clicks on the attachment or it can be activated when the user clicks on the link in the email.   
  
These are worms are spread via infected email messages. Any form of attachment or link in an email may contain a link to an infected website. Infection can be in two ways i.e. it can be activated when the user clicks on the attachment or it can be activated when the user clicks on the link in the email.   
  
Instant Messaging   
These are worms spread via instant messaging applications for example -Yahoo Messenger by sending links to infected websites to everyone on the local contact list.   
  
Instant Messaging Worms  
These are worms spread via instant messaging applications e.g. Yahoo Messenger by sending links to infected websites to everyone on the local contact list.   
  
File Sharing Networks Worms   
These copy themselves into a shared folder, most likely located on the local machine. The worm will place a copy of itself in the shared folder under a harmless name. It then spreads to other computers on the network.  
  
File-sharing Networks Worms  
  
Errors and Accidents  
Listen to this story about Patriot Missile Failure  
  
On February 25, 1991, during the Gulf War, an American Patriot Missile battery in Dharan, Saudi Arabia, failed to intercept an incoming Iraqi Scud missile. The Scud struck an American Army barracks and killed 28 soldiers.  
A report of the General Accounting office, GAO/IMTEC-92-26, entitled Patriot Missile Defense: Software Problem Led to System Failure at Dhahran, Saudi Arabia reported on the cause of the failure. It turns out that the cause was an inaccurate calculation of the time since boot due to computer arithmetic errors.  
Here is another story about a Computer error linked to horrific Qantas jet plunge October 08, 2008 10:18am  
  
  
A QANTAS aircraft flying from Singapore to Perth shot up 300 feet before pitching earthward after signaling to its pilots irregularities in its elevator control system.  
The ghost in the machine'' malfunction which caused a mid-air drama leaving 46 people injured has puzzled air safety investigators who cannot recall a similar incident in aviation history.   
  
Australian Transport Safety Bureau (ATSB) director of aviation safety investigation Julian Walsh said there was no doubt the Airbus A 330-300, traveling at 37,000 feet, had briefly taken control of itself. There are other numerous reported incidences due to computer errors and accidents.Errors and accidents in computer systems may be classified as; Human errors, Procedural errors, Software errors, Electromechanical problems and Dirty data.  
Human Error   
People err. That is a fact of life. People are not precision machinery designed for accuracy. In fact, people make mistakes when entering data into the computer some of which can be fatal as indicated in the quoted stories. Wrong entry of data leads to the generation of wrong results, officially known as Garbage In Garbage Out (GIGO).Some human errors may be as a result of ignorance or lack of technical knows how.  
  
Routine Errors   
Also called procedural errors, they occur when the correct procedure or steps are not followed. It may result to breakdown of the system thereby disrupting business.  
  
Software Errors   
They are also called bugs. These are errors in a program that causes it not to work properly. It could be as a result of syntax or a missing character in the program code. Programs require a lot of debugging or removal of errors before a system is fully allowed to take over the running operations of any business or organization.  
  
Electromechanical Problems   
Mechanical systems, such as the printers, circuit boards, input devices may get dirty, overheat, wear out or could be faultily constructed leading to a system shut down. Consider a situation whereby the printer;s electric system short circuits when students report forms are being produced. This may cause the production of report forms to stop, making the students go without report forms.  
  
Dirty Data  
Dirty Data is a term used to describe typographical errors in data entered into a computer. This makes data to be incomplete, outdated and otherwise inaccurate  
  
Theft/Buglary  
Your school has just purchased Kshs 500,000 worth of new computer equipment to replace existing equipment. These computers disappear before they are installed.  
Theft is a crime against computers; it includes theft of hardware, software and computer time.  
Hardware Theft  
It can range from shoplifting of computer accessories in a computer shop, to stealing of laptops from cars, to computers from a building/room to removal of computer parts such as memories  
  
Software Theft  
Stealing software can take the form of physically taking off with someone's CDs, but it is more likely to be copying of programs. This can also be termed as piracy.   
  
Theft of Computer Time  
Some people use their employers' time to play games, send e-mails, chatting while they are supposed to be working  
  
  
Natural calamities and their Hazards   
Some natural disasters can wreck the entire system, for example, natural hazards such as floods, earth quakes, tornados, hurricanes and the like are harmful to computers and communication systems.  
  
Other Hazards  
Other hazards such as civil strife, unrest, and wars can take place leading to destructions of computers and communication systems. For example, the post election violence experienced in Kenya in January 2008 led to communications breakdown and in some cases destruction of computer systems.  
Others are acts of terrorism such as the September 2001 attack on World Trade center in New York and the bombing of the American Embassy in Kenya in August, 1998 are examples of threat to computer systems.  
  
Physical and logical unauthorized access  
  
  
  
Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner.   
Unauthorized access can be in two ways;  
This involves persons have illegal entry to the building/computer room or the persons having physical access to the storage media i.e. hard disks, compact disk etc. the motive could be either to steal the computers or information or maliciously damage, change or alter, delete data/information.  
ii) Logical unauthorized access involves gaining illegal access into a computer system. It could be deliberate or accidental. Illegal access could be with an intention to steal, delete, copy, and alter data/information.  
Controlling unauthorised access