Hardware and Networking Service

Level II

Based on March, 2022, Curriculum Version I

Module Title: Caring for Network and Computer Hardware

Module Code: EIS HNS2 M05 0322

Nominal Duration: 30 Hours

Prepared By: Ministry of Lobar and Skill

August, 2022

Addis Ababa, Ethiopia

Acknowledgement

Ministry of Labor and Skills wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM).

Table of Contents

Acronyms

RAM-Random Access Memory

CD-Compact Disk

DVD- Digital Versatile Disc

OS-Operating System

BIOS-Basic Input Output System

IBM- International Business Machines

SATA- Serial AT Attachment

RAID- Redundant Array of Independent Drives

USB- Universal Serial Bus

UPS- Uninterruptible Power Supplies

SLA-Service Level Agreement

OHS-Occupational Health Safety

Introduction to the module

This module defines the competence required to maintain computer hardware. It includes locating sitting of hardware for safe and efficient utilization and reducing risk of infection.

Module units

- Computer hardware components
- Location requirements for hardware and peripherals
- Threats of the network
- Maintenance practices

Learning objectives of the Module

At the end of this session, the trainee will able to:

- Identifying computer hardware components
- Establish location requirements for hardware and peripherals
- Monitor and control threats of the network
- Establish and Perform Maintenance practices

Module Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below.
3. Read the information written in the information Sheets
4. Accomplish the Self-checks

UNIT ONE: IDENTIFY COMPUTER HARDWARE COMPONENTS

This learning guide is developed to provide you the necessary information regarding the Following content coverage and topics –

- Hardware components and peripherals
- Internal hardware components.
- Requirements specifying by hardware manufacturers
- Quality standard of hardware and peripherals
- Relationship of Hardware and software components
- Safe work practices

This guide will also assist you to attain the learning outcome stated in the above. Specifically, upon completion of this module, you will be able to –

- External hardware components and peripherals are identified based on business requirement
- Internal hardware components are identified as needed
- Requirements specified by hardware manufacturers are reviewed, recorded and applied where appropriate.
- Quality standards of hardware components and associated peripherals are determined and recorded
- Relationship of computer hardware and software is determined and established for proper functioning of the system
- Safe work practices are determined, recorded and applied, taking into account legal and manufacturer requirements

1.1 Overview of Internal and External Hardware Peripherals

- **Hardware**

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners etc.

The internal hardware parts of a computer are often referred to as components, while external hardware devices are usually called peripherals. Together, they all fall under the category of computer hardware. Software, on the other hand, consists of the programs and applications that run on computers. Because software runs on computer hardware, software programs often have system requirements that list the minimum hardware required for the software to run.

Note: *Peripheral devices are the devices that are attached to the computer's system unit*

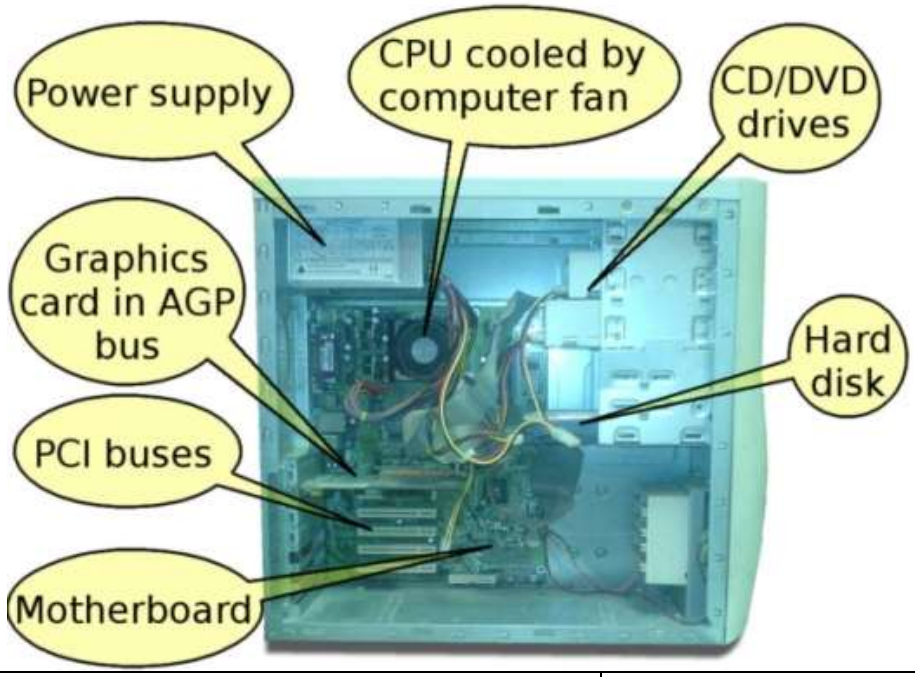
1.2 Internal Hardware Peripherals

Introduction

Computer Hardware is the physical part of a computer, as distinguished from the computer software that executes or runs on the hardware. The hardware of a computer is infrequently changed, while software and data are modified frequently. The term soft refers to readily created, modified, or erased. These are unlike the physical components within the computer which are hard.

When you think of the term computer hardware you probably think of the guts inside your personal computer at home or the one in your classroom. However, computer hardware does not specifically refer to personal computers. Instead, it is all types of computer systems. Computer hardware is in embedded systems in automobiles, microwave ovens, CD players, DVD players, and many more devices. In 2003, only 0.2% of all microprocessors sold were for personal computers. How many other things in your house or your classroom use computer hardware?

Inside Computer



Motherboard is the body or mainframe of the computer, through which all other components interface. It is the central circuit board making up a complex electronic system. A motherboard provides the electrical connections by which the other components of the system communicate. The mother board includes many components such as: central processing unit (CPU), random access memory (RAM), firmware, and internal and external buses.

Components directly attached to the motherboard include:

- The central processing unit (CPU) performs most of the calculations which enable a computer to function, and is sometimes referred to as the "brain" of the computer. It is usually cooled by a heat sink and fan. Newer CPUs include an on-die Graphics Processing Unit (GPU).

- The chip set mediates communication between the CPU and the other components of the system, including main memory.
- RAM (random-access memory) stores resident part of the current running OS (OS core and so on) and all running processes (application parts, using CPU or input/output (I/O) channels or waiting for CPU or I/O channels).
- The BIOS includes boot firmware and power management. The Basic Input Output System tasks are handled by operating system drivers. Newer motherboards use Unified Extensible Firmware Interface instead of BIOS.
- Internal buses connect the CPU to various internal components and to expansion cards for graphics and sound.

Central Processing Unit

The Central Processing Unit (CPU; sometimes just called processor) is a machine that can execute computer programs. It is sometimes referred to as the brain of the computer.

There are four steps that nearly all CPUs use in their operation: ***fetch***, ***decode***, ***execute***, and ***writeback***. The first step, fetch, involves retrieving an instruction from program memory. In the decode step, the instruction is broken up into parts that have significance to other portions of the CPU. During the execute step various portions of the CPU, such as the arithmetic logic unit (ALU) and the floating point unit (FPU) are connected so they can perform the desired operation. The final step, writeback, simply writes back the results of the execute step to some form of memory.

Power supply

Inside a custom-built computer: the power supply at the bottom has its own cooling fan.

A power supply unit (PSU) converts alternating current (AC) electric power to low-voltage DC power for the internal components of the computer. Some power supplies have a switch to change between 230 V and 115 V. Other models have automatic sensors that switch input voltage automatically, or are able to accept any voltage between those limits. Power supply units used in computers are nearly always switch mode power supplies (SMPS). The SMPS provides regulated direct current power at the several voltages required by the motherboard and accessories such as disk drives and cooling fans.

1.3 Removable media devices

CD (compact disc) The most common type of removable media, suitable for music and data**.** o CD-ROM Drive - a device used for reading data from a CD. o CD Writer - a device used for both reading and writing data to and from a CD.	
DVD (digital versatile disc) A popular type of removable media that is the same dimensions as a CD but stores up to 12 times as much information. It is the most common way of transferring digital video, and is popular for data storage. o DVD-ROM Drive - a device used for reading data from a DVD. o DVD Writer - a device used for both reading and writing data to and from a DVD. o DVD-RAM Drive - a device used for rapid writing and reading of data from a special type of DVD.	
Blu-ray Disc **a high-density optical disc format for data and high-definition video. Can store 70 times as much information as a CD.** o BD-ROM Drive - a device used for reading data from a Blu-ray disc. o BD Writer - a device used for both reading and writing data to	

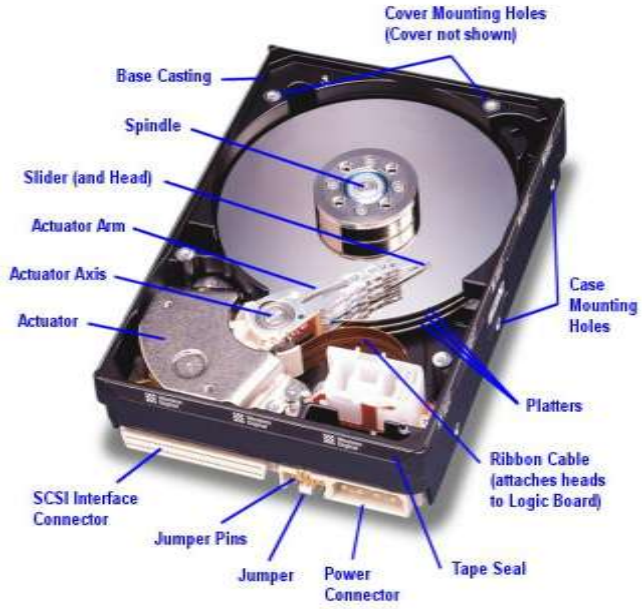
and from a Blu-ray disc.	
HD DVD (short for **High-Definition/Density DVD**) Is a discontinued high-density optical disc format for storing data and high-definition video. Supported principally by Toshiba, HD DVD was envisioned to be the successor to the standard DVD format. However, in February 2008, after a protracted high definition optical disc format war with rival Blu-ray Disc, Toshiba abandoned the format, announcing it would no longer develop or manufacture HD DVD players or drives. However, the HD DVD physical disk specifications (but not the codecs) are still in use as the basis for the CBHD (China Blue High-Definition Disc) formerly called CH-DVD. The HD DVD Promotion Group was dissolved on March 28, 2008.	
Floppy disk An outdated storage device consisting of a thin disk of a flexible magnetic storage medium. Floppies are used today mainly for loading device drivers not included with an operating system release (for example, RAID drivers).	
Iomega Zip drive An outdated medium-capacity removable disk storage system, first introduced by Iomega in 1994.	

Secondary storage

Hardware that keeps data inside the computer for later use and remains persistent even when the computer has no power.

A Hard disk drive (HDD also **hard drive** or **hard disk**) is a non-volatile, random access digital magnetic data storage device. It features rotating rigid platters on a motor-driven spindle within a protective enclosure. Data is magnetically read from and written to the platter by read/write heads that float on a film of air above the platters. Introduced by IBM in 1956, hard disk drives have decreased in cost and physical size over the years while dramatically increasing in capacity.

Hard disk drives have been the dominant device for secondary storage of data in general purpose computers since the early 1960s. They have maintained this position because advances in their recording density have kept pace with the requirements for secondary storage. Today's HDDs operate on high-speed serial interfaces; i.e., serial ATA (SATA) or serial attached SCSI (SAS).



A solid-state drive (SSD)

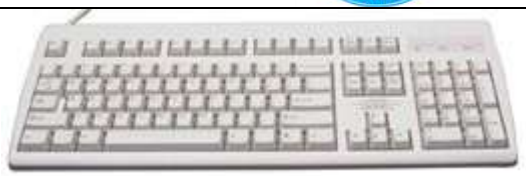
sometimes called a solid-state disk or electronic disk, is a data storage device that uses solid-state memory to store persistent data with the intention of providing access in the same manner of a traditional block i/o hard disk drive. SSDs are distinguished from traditional magnetic disks such as hard disk drives (HDDs) or floppy disk, which are electromechanical devices containing spinning disks and movable read/write heads. In contrast, SSDs use microchips which retain data in non-volatile memory chips and contain no moving parts. Compared to

electromechanical HDDs, SSDs are typically less susceptible to physical shock, are silent, have lower access time and latency, but are more expensive per gigabyte (GB). SSDs use the same interface as hard disk drives, thus easily replacing them in most applications.	
RAID array controller A device to manage several internal or external hard disks and optionally some peripherals in order to achieve performance or reliability improvement in what is called a RAID array.	
Sound card Enables the computer to output sound to audio devices, as well as accept input from a microphone. Most modern computers have sound cards built-in to the motherboard, though it is common for a user to install a separate sound card as an upgrade. Most sound cards, either built-in or added, have surround sound capabilities.	

1.4 External hardware peripherals

Examples of External hardware peripheral devices include:

Monitor A monitor, also known as a visual display unit (VDU) or screen, is like a television screen. It is measured diagonally in inches — the distance from one corner of the screen area to the opposite corner. The quality of a monitor is determined by its resolution. Resolution is calculated based on the number of pixels, which are individual dots that create the images you see on your monitor. Flat panel monitors are now becoming a popular choice due to their portability and compactness.	

Keyboard A combination of a typewriter keyboard and numeric keypad, a keyboard enables you to enter data into a computer. Computer keyboards are similar to electric typewriter keyboards but include additional keys.	

Mouse A mouse is a device that controls the movement of the cursor on a screen. A mouse is a small object you can roll along a flat surface, to help you navigate your computer. Mice also have a variety of buttons, which can have different purposes depending on what program is running. There is usually a left mouse button (which is used to select an object and perform an action), right mouse button (which typically displays a shortcut menu of options) and a scroll wheel (to help a user scroll through documents).	

Printers

A printer is a device that allows you to obtain hard copies of the data you have created on your computer system. Printers are classified by:

1 Their quality

2 The speed of printing — pages per minute

3 The print/image resolution — measured in dots per inch (dpi).

In the case of speed, the faster the better, and in the case of dpi, the higher the better. There are different types of printers due to the different methods of transferring ink to paper. Two common types for the home and office are inkjet and laser.

Inkjet printer — sprays ink onto a sheet of paper, and can produce high-quality text and photo images.	

Laser printer — produces very high-quality text and graphics, using a process similar to a photocopier to produce print. It creates dot-like images on a drum, using a laser beam light source.	

Scanner A scanner is a device that captures text or illustrations on paper and converts the information into a form the computer can use. One of the most common kinds of scanners is called a flatbed scanner. It has a glass surface on which you lay paper, magazines, or other documents that you want to scan. Sometimes scanners can be manufactured so that they are combined with a printer thus can also be used as a photocopier and fax machine.	

USB flash drive A small, portable device that plugs into a computer's USB port and operates as a portable hard drive. USB flash drives are considered to be an ideal method to transport data, as they are small enough to be carried in a pocket and can plug into any computer with a USB drive. Other names for flash drives are thumb drives, pen drives or USB drives.	

Web cam Web cams are small cameras that plug into your computer which allow the user to share a moving image of themselves with others on other computers through the Internet.	

Digital camera

Digital cameras store images digitally onto a storage device, either a memory card or a floppy disk, rather than recording them on film. Once a picture has been taken, it can be downloaded to a computer system, and then manipulated or printed.

1.5 Determine any requirements as specified by the hardware manufacturer

Warranties and support

Before acquiring hardware peripheral devices, it is vital to assess what kind of warranties, service and support, prospective suppliers will provide.

Warranties

A warranty is an agreed upon term which covers a computer or computer component. Generally, most computers have a 1- or 3-year warranty. This warranty may or may not cover the service, repair and replacement of computer parts.

An extended warranty is an available option provided by manufacturers or third-party companies that provides additional support and/or repair of a computer or other hardware devices beyond its standard warranty.

Service and support

It is important to know what kind of support services are offered by the prospective supplier. There are many questions to consider such as:

- If a device requires repairs does it have to be sent back to the supplier (called 'Return to base') or will they provide on-site visits?
- What is the average response time if service is required?
- What kinds of maintenance and repair costs could be incurred during the duration of use of the device?
- Will the device require regular servicing? If so, how many services will be necessary over a one-year period?

System specifications

It is important to find out the specifications of the computer system you are planning to connect the peripheral device to. Many newer types of peripheral devices require a specific amount of memory, CPU speed, hard disk space, and may only be compatible with certain operating systems.

You also need to be aware of the peripheral's system requirements. The manual for the peripheral device as well as the manufacturer's website will help you determine the minimum system specifications.

Compatibility

Compatibility is the ability of a system or a product to work with other systems or products without special effort on the part of the customer. One-way products achieve interoperability is to comply with industry interface standards. For example, a memory module is compatible with a motherboard because the manufacturer of the memory module and the motherboard both work to the same industry standard.

Technical specifications

Once the business requirements have been considered, the technical specifications of the hardware device need to be evaluated. Areas for evaluation include the following:

- Processing speed of the CPU
- Storage capacity of the hard drive
- Size of memory (RAM)
- Software capabilities
- Compatibility with existing systems
- Upgradeability

The technical specifications to be considered will depend on the computer hardware device to be purchased. For example, technical specifications to be considered for a printer include:

- Interface – USB or network
- Resolution – measured in dots per inch
- Printing speed – measured in pages per minute
- Memory
- Paper capacity

Warranty

When computer hardware devices are purchased, the supplier provides a guarantee that if a fault develops in the equipment within a certain time, they will repair or replace it free of charge. Organizations need to consider the warranty conditions before purchasing to ensure their business needs will be met. Common warranty conditions include:

- The length of the warranty – typically one or more years.

- The actions needed to have the repairs undertaken. Either the repairs will be done on-site or the equipment will need to be returned to the supplier, known as return-to-base.
- How long the supplier has to make good any required repairs
- Any exclusions to the warranty, such as damage caused to hardware by accidental damage.

Many computer hardware suppliers offer extended warranties at additional cost. For example, the extended warranty may extend the period of cover from one year to three years. The level of service purchased by an organization will depend on how critical the device is to the IT system.

A Service Level Agreement (SLA) is an agreement which sets out the level of service and maintenance to be provided.

Organizational policies

Some organizations have a policy of using preferred suppliers for computer hardware purchases. This ensures the quality and consistency of computer hardware devices is maintained throughout an organization.

A **standard operating environment** is a specification for computer hardware and software which organizations develop to maintain consistency and reduce support costs. Many organizations such as universities, publish their standard operating environment policies on the internet. For an example, visit the Edith Cowan University Standard Operating Environment website

Self-Check 1

Name: _____ Date: _____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

Match the most appropriate peripheral device to A column from B column.

Column A	**Column B**
1. Mouse	A. Internal hardware peripherals
2. Speakers	B. External hardware peripherals
3. Keyboard	
4. Web cam	
5. Monitor	
6. Power supply	
7. Digital Camera	
8. Data projectors	
9. External modems	
10. Printers	
11. Microphones	
12. Mother board	
13. CPU	
14. Power supply	
15. Storage Device Drives	
16. Removable Medias	

IDENTIFICATION (Acronyms)

1. USB_____
2. CPU_____
3. BIOS_____
4. CMOS_____
5. AGP_____

UNIT ONE-ANSWERS: SELF CHECK 1

Matching

1. B
2. B
3. B
4. B
5. A
6. B
7. B
8. B
9. B
10. B
11. B
12. B
13. A
14. A
15. A
16. A

IDENTIFICATION (Acronyms)

1. USB – Universal Serial Bus
2. CPU – Central Processing Unit
3. BIOS – Basic Input/ Output System
4. CMOS – Complimentary Metal-Oxide Semiconductor
5. AGP – Accelerated Graphics Port

UNIT TWO-ESTABLISH LOCATION REQUIREMENTS FOR HARDWARE AND PERIPHERALS

This learning guide is developed to provide you the necessary information regarding the Following content coverage and topics.

- Determining and applying suitable environmental conditions
- Considering orientation and proper functioning of different computer platforms
- Determining and applying System protection devices
- Determining and applying requirements when moving hardware
- Determining and applying suitable storage principle
- Considering and applying business requirements
- Considering OHS standards and environmental concerns

This guide will also assist you to attain the learning outcome stated in the above. Specifically, upon completion of this module, you will be able to –

- Suitable environmental conditions are determined and applied for hardware and peripherals
- General orientation and proper functioning of different computer platforms are considered in locating computer
- System protection devices are determined and applied to keep hardware form damage.
- Requirements are determined and applied when moving hardware.
- Suitable storage principles are determined and applied for hardware and associated peripherals and media.
- Business requirements are considered and applied in respect of hardware location
- Functions of computer hardware and associated OHS standards and environmental concerns are considered

2.1. Environmental Conditions

Just like the environmental conditions affect us as humans, computer equipment can also be affected. In order install and maintain equipment to gain the maximum useful life, the environmental conditions need to be considered-factors such as temperature extremes, humidity, dust, electromagnetic interference (EMI), and so on. The following notes are a discussion of these factors.

- **Temperature**

One of the single most important factors in prolonging the life of your computer hardware is the temperature of the components. Components that run hot, have a much shorter life than those that stay cool most of the time. To keep components cool you could use cooling equipment or ensure certain procedures or actions (discussed later). A more general approach is to provide a room environment that is appropriate for the hardware.

A rule of thumb for room temperature is that computers like the temperatures that most people like. That is temperatures between 15 and 24 degrees Celsius. Having computer equipment operating in a hot room that is over 25 degrees Celsius will make general cooling equipment, such as fans, fairly ineffectual.

Some businesses have their air-conditioners on a timer that will shut off at night. In this situation you might want to make sure that computer equipment is switched off overnight, or that a special computer room is designated with independent controls.

Obviously, most computer hardware can tolerate being at more extreme temperatures when they are not running. If you are transporting equipment or storing it, the temperature concerns are far less than if the equipment is actually in use. However, if you have equipment that has been exposed to very low temperatures and is then immediately turned on, you risk permanently damaging the equipment. It is essential that very cold equipment be brought up to room temperature slowly before use. This is called acclimation.

When receiving new equipment during very cold weather, it is worth considering that the equipment has been sitting in very cold warehouses or trucks. You may be risking permanent damage if you switch power up the equipment while still very cold. Of particular concern are monitors, hard disks, motherboards, and chips of all kinds (processor, memory, etc.) This covers most of the computer of course.

Thermal stress is a leading cause of premature failure of electronics components. This is bad enough when the components are raised from 20 degrees to 60, but when they are raised from 0 to 60 it is much worse.

Condensation can be even more destructive. Think about how moisture condensates on a cold bottle, on a warm day, when you take it out of the fridge (usually around 5 degrees Celsius). It is quite possible for this to happen with electronic equipment as well. This does not need to cause any problems, so long as you give the condensation enough time to evaporate. If your hard disk platters have moisture on them when you spin them up, you risk destroying the drive.

The colder the equipment is, the longer it needs to sit to ensure that it comes up to a reasonable temperature before turning it on. In temperatures down 5 degrees, then you might want to wait up to 12 hours. If the device has been allowed to go to below-freezing temperatures, then wait 24 hours for the device to acclimate before plugging in the power.

A more humid environment will make condensation more of a problem.

- **Humidity**

As with temperature, computers prefer moderate humidity as opposed to either extreme. While computer equipment is not as sensitive to humidity as temperature, they can still be affected by it.

Obviously, computers are best kept dry. That means keeping it away from places or things that can get it wet. Consider the inappropriate positioning near a window if it is frequently opened, and be wary of beverages placed near the computer that could spill on it and short it out.

Using computer equipment in a humid area can be problematic, if the climate is extremely humid. Using a computer in a tropical rainforest is an example of extreme humidity. Humidity leads to corrosion and possible condensation risk, which can damage equipment. It also makes cooling the computer more difficult.

Conversely, air that is too dry can cause problems in two different ways. First, it increases the amount of static electricity that is in the room, increasing the chances of a discharge. Second, it can cause faster wear on some components that dry out over time. This includes some types of capacitors, as well as rubber rollers on laser printers.

- **Dirty environments**

Computers operate best when they are used in a clean environment, and when they are cleaned regularly. Most offices and homes are clean enough that a computer requires no special treatment

other than regular cleaning as part of routine preventive maintenance. Industrial environments however can be quite destructive on computer equipment.

Computer systems that are going to be used in dirty environments should be protected or cleaned often. Cleaning would also mean taking the covers off and cleaning the inside. If you get the chance to see the inside of a system unit that has been in an industrial environment, you will be amazed how much dirt accumulates.

One easy preventive measure is to use an air cleaner in the room where the computer is located. There are also special cases and enclosures for computer hardware designed for industrial environments to safeguard against damage due to dirt. The typical office owner only has to remember to clean their equipment occasionally and no problems will generally result

Now this might be stating the obvious, but cigarette smoke is bad. The simple fact is that cigarette smoke, especially in high concentration, contaminates and damages computer equipment. The smoke particles are very small and work their way into all sorts of places that they do not belong. The most common problems relate to storage devices. The very fine particles accumulate on read/write heads and the storage media, such as floppy disks.

2.2 Electromagnetic interference (EMI)

Probably everyone at some stage has had a radio on when there is an approaching thunderstorm. You would clearly hear the crackling and noise distortion coming from the radio. That crackling is the result of electromagnetic interference, often referred to as EMI.

All electronic devices give off electromagnetic emissions. This is radiation that is a by-product of electrical or magnetic activity. Unfortunately, the emissions from one device can interfere with other devices, causing potential problems. Just like the crackling on the radio, interference can lead to data loss, picture quality degradation on monitors, and other problems with your PC, television set or other devices.

EMI emissions are a two-way problem; emitted by the computer system, and EMI received by the computer system. PCs generally do not cause very much interference with other devices. As with many other electronic devices, they should be certified as Class B compliant with the Federal Communications Commission (FCC). This certification shows that the PC conforms to standards that limit the amount of EMI that a PC can produce. As metals absorb EMI, you have to keep the metal covers on the computer.

PCs can be affected by electromagnetic interference from other devices, in two major ways. One is direct effects through proximity with other devices; another is electrical interference over the power lines.

Try this quick test:

1 Hold a mobile phone near next to an operating monitor

2 Send an SMS message to someone you know.

3 Watch the effects on picture quality.

While a more colorful test would be to place a strong magnet next to a monitor, it is not recommended as sometimes the effects can be long-lasting. Degauss is the process that demagnetizes the metal components in the cathode ray tube (CRT), eliminating image distortion that can result from magnetic charges acquired by the components. Some new monitors degauss automatically whenever you turn on your monitor.

Most PCs generally do not have many problems with EMI, but for those that do, there are things that you can do to reduce EMI:

Physical isolation: Devices that emit electromagnetic radiation should be kept a reasonable distance from your computers, peripherals and media. This includes television sets, radios, lights, kitchen appliances, and stereo speakers. Speakers designed for use with PCs are generally shielded and are much less of a problem.

Use dedicated circuits: Some office buildings have separate power circuits that are intended for use by computer equipment. Keeping your computer on a circuit that is separate from the circuit running your refrigerator, arc welder, air conditioning unit etc., means that there will be much less interference passing to the computer from the other devices. The added benefit is this will also improve the quality of the power being sent to your machine in general.

Power conditioning: The use of a line conditioner or uninterruptible power supply can filter out interference caused by other devices that share a line with your computer.

2.3 Keeping your cool

Keeping your system cool is very important. A cool system runs more reliably and lasts longer than one that runs hot. Overheating of the internal components can lead to data loss or even damage to your equipment. As processors in particular have become faster and hotter, cooling has become more important than ever.

- **Internal airflow**

The typical desktop computer system has a fan which provides overall airflow within the system case. This is normally the fan located within the power supply at the back of the case. Some newer machines, especially full-tower cases, employ more than one fan, to provide more cooling.

It's important to realize that the fan(s) used in the power supply work by establishing a flow of air through the case. There are two basic designs used. In the older baby AT style case, the power supply fan blows out the back of the power supply, and in doing so it draws air through the rest of the case and thereby, cools the components inside the case. In now more common ATX style of case and power supply, the power supply fan is on the inside of the case and blows inwards, pushing air throughout the case and drawing it in through the back of the power supply, exactly the opposite. In both cases, for the cooling to work properly, the flow of air must not be interrupted. The better, and stronger, the flow of air, the more cooling it will accomplish.

The flow of air also has an impact on keeping the inside of the case clean. In a standard baby AT case, the air is pushed out the back of the power supply, and replacement air is drawn in through all the small cracks and holes in the case. This tends to cause dust and dirt to be drawn into the case. Apparently one reason why the ATX form factor design was changed was to blow air into the case instead of out of it, is that this isolates the in-flow of air in the case to one point, making it possible to use filters and other mechanisms to reduce dirt intake into the system unit.

Here are some rules of thumb and tips that you can use to ensure that the flow of air in your system is good, and to increase airflow in your case:

Keep the cover on: It is a common fallacy to think that running the system with the case cover removed will improve cooling since the components are exposed to the outside air. In fact, this can make cooling worse. When you remove the case, the air that the power supply fan is pushing out the back of the case is replaced by air drawn from the room instead of being drawn across the components. As a result, many components will sit in stagnant air with little cooling.

Cover exposed expansion slots and holes: Any unused expansion card slots, drive bays, or other crevices in the system case should be covered with inserts, faceplates or tape, to ensure that airflow is not being short-circuited. Air will follow the path of least resistance, and if you have a big hole in your case near the power supply unit, most likely air will flow in there and right out the power supply, resulting in poor flow for the rest of the case.

Add additional fans: Some cases provide mounting positions for installing additional fans. These can be useful, depending on what they are and how you set them up, although they are not necessary for most people if they follow the other suggestions listed here. A fan on an expansion card (such as a video card) will improve airflow in the proximity of the card, but not between the case and the outside world. An extra fan venting to the outside can improve airflow and cooling.

Use a large system case: Larger cases have more room and therefore generally allow for better airflow and cooling of components.

Arranging your internal components: Devices that generate a great deal of heat should be kept as far away from each other as possible. If you install two hard disk drives in adjacent drive bays in a typical system, they may end up with less than a few millimeters separating them. This is simply not going to provide for cooling as good as if you had them several centimeters apart.

Keep the inside of the case clean: Good airflow in the box doesn't help very much if none of the cool air can reach the components because they are covered with a thick layer of dust.

- **External ventilation**

In order for system cooling to be effective, it is important that there be good airflow not only within the system case but also immediately outside it as well. If the system is located somewhere where it will not get adequate ventilation, it can overheat no matter how many fans you have on the inside of the unit.

Ventilation is closely related to ambient temperature of course, since airflow outside the box is more important in a hot room than a cool one. The best environment for the computer is one with regulated temperature settings, air conditioning, and active ventilation of the entire room. In practice, ventilation isn't a problem as long as you use common sense. The most important part of is simply making sure that you provide space for the power supply fan to blow, without blocking it off. Sometimes this happens for example when a system unit is jammed against the wall when placed on a desk.

There is also the obvious:

Don't put papers on top of the ventilating grating on your monitor.

Don't enclose the entire system unit in a box, or desk shelving, that will not let air circulate properly.

2.4 Power Conditioning

There are many issues with computers that are ultimately related to power problems. Providing a good, reliable power source to your computer, and peripheral, is another aspect of system care. We should take a look at how to avoid power problems, as well as energy conservation and other issues related to the use of power.

- **Typical power problems**

There are a number of terms related to power and problems, some of the most common are:

- **Blackouts:** When power levels drop to virtually zero, or in other words there is NO power.
- **Brownouts:** Also called sag. A brownout occurs when power levels drop below that which is supposed to be delivered, for a sustained time. For example, if you have a 230-240-volt power outlet, but the measurable level drops below 230 volts. Typically experienced in switching on of heavy equipment.
- **Surges:** Is the opposite of a brownout. It is where voltage levels increase above that which is specified at the outlet eg above 240 volts
- **Spikes:** A short sharp and very sudden increase of voltage, that also drops just as quickly eg a 240-volt supply jumps to 1000 volts or more for a period of as little as 20 milliseconds (1/50th of a second). This is typical of a lightning strike.
- **Line noise:** Line noise consists of small variations in the voltage level. A certain amount of line noise is normal (no power generation circuits are perfect) and for the most part power supplies will deal with them without difficulty. However, in some areas the power quality

is worse than others. Also, if the computer is sharing a circuit or is physically located near devices that cause electromagnetic interference (motors, heavy machinery, radio transmitters, etc.) then line noise can be a serious concern. Noise that the power supply cannot handle can cause it to malfunction and pass the problem on to your motherboard or other internal devices.

2.5 Protection from power problems

When power problems strike, they can cause permanent damage. The damage could be to your equipment or your data. The only effective way to deal with power problems is to prevent them from happening in the first place. Here are some steps you can take to greatly reduce the chances of power problems with your computer:

Use power protection devices: There are many different types of devices on the market that can be used to protect against power problems; these include surge suppressors, line conditioners and uninterruptible power supplies (UPS). Some are much better than others, and accordingly, cost much more. You can get fairly reasonable protection for your computer systems, without huge expense. You need to decide how much protection you need based on what you are willing to risk. You will need to do something. Just plugging computer equipment into the wall socket is asking for trouble.

Check protection devices regularly: At least once a year, you should inspect your power protection devices to make sure that they are functioning properly. Most good ones will have a signaling light to tell you when they are protecting your equipment properly, but it is only of use if you look at it on occasion!

Use dedicated circuits: Putting the computer on its own power circuit, so it isn't sharing the power with your air conditioner, space heater, and vacuum cleaner, greatly improves the power quality and insulates the system from power sags when these devices are turned on. It also reduces electromagnetic interference from these devices that might be carried over the power line.

Turn off power during a blackout: If you lose power, when the power comes back on the signal can initially be inconsistent, which can make things difficult for your power supply. It is not unusual to see false starts, where the power comes on and then goes off again, during storms. If you have a blackout, turn off your equipment so you can control when it comes back on, not the electricity supply company. Turn the equipment back on once you feel the power has returned and is stabilized.

Turn off and disconnect the power cord during an electrical storm: This is a simple precaution that protects your system from possible problems during a thunderstorm. While this is impractical in a business situation, the solution is to install an uninterruptible power supply (UPS).

Electrostatic discharge (ESD)

Ever stepped out of a vehicle and experienced a sudden sharp zap when touching the door handle? Or perhaps scuffed your feet along a carpeted floor wetting your fingers then gently touching someone's ear? While making yourself popular you are also demonstrating the effects of an electrostatic discharge.

Electrostatic discharge or ESD is caused by the build-up of an electrical charge on one surface that is suddenly transferred to another surface when it is touched. This discharge is actually typically several thousand volts. As there is very little current passed, the zap doesn't kill you.

While ESD won't kill you, it can certainly kill your computer components. Especially sensitive to ESD are integrated circuits: processors, memory, cache chips, and expansion cards. You can deal with ESD in two basic ways:

1 Reducing its build-up

2 Draining it away so it cannot cause any damage.

One way to reduce the build-up of ESD is to increase the relative humidity of the room where the computer is located. Static builds up more readily in dry environments than in moist ones. This is why you get zapped much more often during dry weather than in rainy weather. Another way to reduce static is to avoid doing the well-known things that cause it, such as wearing socks on carpeted floors, etc.

Draining static is usually a simple matter of touching something that is grounded, such as the metal of your case when it is plugged in. This will drain off any static build-up in your body that might cause damage to your components. Protection from ESD is important enough when performing repairs on computer systems that it is recommended that you wear an anti-static wrist strap.

Under normal working conditions it generally isn't much of a concern, since any static zapping you give your system unit will normally be drained to ground through the case.

2.6 Storage and Handling

- **Manufacturer's requirements**

When handling computer equipment, it is advisable to follow the manufacturer's guidelines on handling and storage. The most obvious place to find that information would be the User Guides/Manuals that accompany the product.

While some documentation can be difficult to find, in a cupboard full of manuals, it is also common to have no documentation for the equipment in printed form. These days, many of the manuals and manufacturer guidelines are in electronic form supplied on floppy disk or CD-ROMs.

One of the best avenues, to locate the current information, would be the Internet. If in doubt, go to the manufacturer's website. While some manufacturer's websites can be difficult to locate, there are many Internet directories that can be used to find them. For example, The Computer Information Centre at: www.compinfo-center.com/cmanuf.htm. Apart from documentation, the Internet provides user groups that discuss all manner of issues, where some will raise a question and others will provide the answers.

Your supplier is the other main avenue for valid information. A good supplier will already be aware of specific issues that relate to your product purchases. If your supplier is reluctant to provide relevant product information, find a new supplier.

2.7 Locating equipment

Sometimes when determining the most appropriate location, there are competing interests. From a security viewpoint, it may not be advisable to locate important network servers within easy access from the general public, or even unauthorized employees. But from an accessibility viewpoint, it may be convenient for service personnel to have easy and unsecured access to all equipment. Still, there are the physical services (such as power, phone, network communications etc.) where equipment could be placed in the most convenient and cost-saving location close to outlets and connectors.

- **Security**

When locating equipment, you would need to determine the priorities and adjust or compromise the competing interest accordingly. For example, if you have a network server that contains sensitive accounting and/or payroll data, you would not want general staff (meaning those that should not be handling account/payroll data) to be able to gain access. You could of course restrict access by software such as username/passwords etc., but that would not stop someone from physically taking the hard disk drive in order to steal or copy it.

Where sensitive or critically important hardware is concerned, it would be advisable to locate the equipment in a secure location, such as a lockable cupboard or room. Access can then be more traditionally controlled by security key access.

- **Accessibility**

Consider for a moment that you are a service technician where you go out on location to various businesses. You are called to fix a problem with a server or other equipment, but when you arrive you find the equipment is locked in a tiny cupboard, where the person with the key is out. When you finally gain access, you find it buried under a pile of boxes and papers etc.

When locating equipment, take into account that from time to time someone will need to physically access it. If a service person arrives to such a welcome then the chances are that that person will simply walk away without doing whatever needed to be done. It is not reasonable to expect them to perform their work under such conditions, especially when you consider they may have a dozen other jobs to go to.

So, when locating equipment, you will need to ask yourself the question 'Is this site easily accessible?'.

- **Services**

The term *services* relate to the parts of infrastructure like, general power outlets (GPO), phone, facsimile and network connections. There are of course other services more related to people's needs.

It is generally easier to design and install all the services to be located you need (want), when you are starting with an empty room or building. But that does not always happen. If there are insufficient power outlets (which is almost always the case), then you will have to use power boards. But this need not be totally negative, as this will mean you can easily ensure that equipment is protected through uninterruptible power supplies (UPS), surge protectors, line filters and other conditioning equipment.

It's an extremely bad practice to have cabling (of all sorts) running around a room, across floors, under chairs etc., rather than having it encased in a protective covering. This practice is advocating damage to equipment, communications, as well as Occupational Health and Safety issues. The cost of having wiring professionally installed is easily justified in terms of possible damage to equipment and downtime through poor network communications.

2.8 Storing equipment

You will find that manufacturers will almost invariably require that equipment should be stored in the same packaging in which it was delivered. While this is valid, in principle, often it can be impractical. Empty packaging can consume significant storage space, which may seem not justifiable on a cost basis. However, if you do not have on-site support then to return equipment to the supplier, you will need enough to cover the basics. For example, if you have five printers from one manufacturer, you may choose to keep the packaging of one printer.

Just like locating equipment, when storing equipment, you must consider the factors of temperature, humidity, dust etc. Although if equipment is not in use then such factors as temperature are less of an issue than if the equipment were in service ie in current use.

If unused or stored equipment is packaged similar to its original state, this will usually suffice. Any partially used consumables like ink or toner cartridges should not be stored, but disposed in the manner prescribed by the manufacturer. While this may seem wasteful, after a short time it is unlikely that the consumables will be in a useable state.

2.9 Protection devices

To provide protection for computer hardware devices from electrical problems, the following devices can be installed.

- **Surge protectors** – a device designed to protect against electrical surges and spikes. It provides no protection against blackouts or brownouts.
- **Uninterruptible Power Supply (UPS)** – a device designed to protect against blackouts. A UPS provides power automatically during a blackout and is designed to provide battery power for a relatively short period of time – around ten to twenty minutes. This provides time to save all data and shut down the computer correctly.

Most UPS devices also provide protection against brownouts, surges and spikes depending on their design.

- **Generators** – where an organization requires the computer hardware to be powered for an extended length of time, a generator may be installed in addition to a UPS. This is a relatively costly option and would be considered where the operation of the computer hardware is considered **critical to the organization.**

2.10 Business requirements

When selecting computer hardware, it is important to firstly identify the tasks the computer hardware is required to perform. For example, a workstation required for video editing will have

different requirements to a workstation required for standard office applications, such as word processing. Another example is a server - the processing power and storage capacity of the server will be determined by the number of users it is required to service.

Warranty

When computer hardware devices are purchased, the supplier provides a guarantee that if a fault develops in the equipment within a certain time, they will repair or replace it free of charge. Organizations need to consider the warranty conditions before purchasing to ensure their business needs will be met. Common warranty conditions include:

- The length of the warranty – typically one or more years.
- The actions needed to have the repairs undertaken. Either the repairs will be done on-site or the equipment will need to be returned to the supplier, known as return-to-base.
- How long the supplier has to make good any required repairs
- Any exclusions to the warranty, such as damage caused to hardware by accidental damage.

Many computer hardware suppliers offer extended warranties at additional cost. For example, the extended warranty may extend the period of cover from one year to three years. The level of service purchased by an organization will depend on how critical the device is to the IT system.

A Service Level Agreement (SLA) is an agreement which sets out the level of service and maintenance to be provided.

Safe electrical work practices

Computer hardware should be located close to a suitable electrical outlet. The use of long extension cords is a trip hazard. If no power outlet is available, a new fixed power outlet may need to be installed. Any fixed electrical installation is required by law to be installed by a licensed electrician.

Cables should be kept away from the floor, and a person's workspace. Cables on the floor are easily damaged by trolleys and chair castors.

Use switched power boards and not double adapters or piggy backed plugs.

Routinely inspect cables for any damage. Damaged cables should be disconnected and removed.

Testing and tagging refers to the practice of testing electrical equipment (which is designed for connection by a flexible cord), by an appropriate person. If the equipment is compliant a tag is attached which is marked with the name of the person or company who performed the test, and the test date or retest date.

Any component such as a computer power supply which has a main (240 volt) power connection can only be opened and repaired by a qualified technician. CRT monitors can have very high electrical potential levels even after they have been switched off and must only be opened by a qualified technician.

Electrical circuits for fixed wiring are protected from overload by a circuit breaker. The circuit breaker will trip if the circuit is overloaded. If this happens, it is an indication that the number of electrical appliances on that circuit should be reduced.

Self-Check 2

Name: _____ Date: _____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

Match the most appropriate peripheral device to A column from B column.

Column A	**Column B**
1. System protection	A. Generator
2. Preventive Maintenance	B. Antivirus Programs
3. Protective Device	C. Anti mal ware programs
4. Electrical Problem	D. Surge protector
5. Environmental Problem	E. User Account
	F. UPS
	G. Update
	H. Back up
	I. Cleaning
	J. Firewall
	K. Black out
	L. Brownout
	M. Temperature

True or False

1. Computer hardware should be located close to a suitable electrical outlet.
2. A Service Level Agreement (SLA) is an agreement which sets out the level of service and maintenance to be provided.
3. Universal Serial Bus (USB) – a device designed to protect against blackouts.

UNIT TWO-ANSWERS: SELF CHECK 2

Matching

1. B, and C
2. G, H, I,
3. A, D, E, F,
4. K and L
5. M

True or False

1. True
2. True
3. False

UNIT THREE-MONITOR THREATS TO THE NETWORK

This learning guide is developed to provide you the necessary information regarding the Following content coverage and topics –

- Using third-party software to evaluate and report on system security
- Identifying security threats
- Ensuring carry-out spot checks and other security strategies
- Investigating and implementing inbuilt or additional encryption facilities
- Preparing and presenting an audit report and recommendation
- Obtaining approval for recommended changes

This guide will also assist you to attain the learning outcome stated in the above. Specifically, upon completion of this module, you will be able to –

- Use third-party software or utilities to evaluate and report on system security
- Review logs and audit reports to identify security threats
- Carry-out spot checks and other security strategies to ensure that procedures are being followed
- Investigate and implement inbuilt or additional encryption facilities
- Prepare and present an audit report and recommendations to appropriate person
- Obtain approval for recommended changes to be made

3.1 Monitor threats to the network

There are different ways to monitor threats to the network. Some of them are: -

- By using software Utilities
- By using security mechanism
- By Using encryption facilities

Explain why security is important

Computer and network security help to keep data and equipment functioning and provide access only to appropriate people. Everyone in an organization should give high priority to security because everyone can be affected by a lapse in security.

Theft, loss, network intrusion, and physical damage are some of the ways a network or computer can be harmed. Damage or loss of equipment can mean a loss of productivity. Repairing and replacing equipment can cost the company time and money. Unauthorized use of a network can expose confidential information and reduce network resources.

3.2 Security threats

To successfully protect computers and the network, a technician must understand both types of threats to computer security:

- **Physical** – Events or attacks that steal, damage, or destroy equipment, such as servers, switches, and wiring
- **Data** – Events or attacks that remove, corrupt, deny access, allow access, or steal information

Threats /danger/harm to security can come from the inside or outside of an organization, and the level of potential damage can vary greatly:

- Internal – Employees have access to data, equipment, and the network
    - Malicious threats are when an employee intends to cause damage.
    - Accidental threats are when the user damages data or equipment unintentionally/by accident.
- External – Users outside of an organization that do not have authorized access to the network or resources
    - Unstructured – Attackers use available resources, such as passwords or scripts, to gain access and run programs designed to vandalize
    - Structured – Attackers use code to access operating systems and software

Physical loss or damage to equipment can be expensive, and data loss can be detrimental/harmful to your business and reputation/status. Threats against data are constantly changing as attackers find new ways to gain entry and commit their crimes.

After completing this section, you will meet these objectives:

- Define viruses, worms, and Trojans.
- Explain web security.
- Define adware, spyware, and gray ware.
- Explain Denial of Service.
- Explain social engineering.

Define viruses, worms, and Trojans

- **Viruses**

A software virus is a parasitic/freeloading program written intentionally to alter the way your computer operates without your permission or knowledge.

A virus attaches copies of itself to other files such as program files or documents and is inactive until you run an infected program or open an infected document. When activated, a virus may damage or delete files, cause erratic system behavior, display messages or even erase your hard disk.

A virus may spread through email and instant messenger attachments, through infected files on floppy disks or CD-ROMs, or by exploiting a security flaw in Microsoft Windows.

- **Worm**

A worm is a self-replicating program that is harmful to networks. A worm uses the network to duplicate its code to the hosts on a network, often without any user intervention. It is different from a virus because a worm does not need to attach to a program to infect a host. Even if the worm does not damage data or applications on the hosts it infects, it is harmful to networks because it consumes bandwidth.

- **Trojan horse**

The Trojan does not need to be attached to other software. Instead, a Trojan threat is hidden in software that appears to do one thing, and yet behind the scenes it does another. Trojans are often disguised as useful software. The Trojan program can reproduce like a virus and spread to other computers.

A Trojan horse is not a virus because it does not replicate and spread like a virus.

3.3 Web security

Web security is important because so many people visit the World Wide Web every day. Some of the features that make the web useful and entertaining can also make it harmful to a computer.

Tools that are used to make web pages more powerful and versatile are: -

- **ActiveX** – Technology created by Microsoft to control interactivity on web pages. If ActiveX is on a page, an applet or small program has to be downloaded to gain access to the full functionality.
- **Java** – Programming language that allows applets to run within a web browser. Examples of applets include a calculator or a counter.
- **JavaScript** – Programming language developed to interact with HTML source code to allow interactive websites. Examples include a rotating banner or a popup window.

Attackers may use any of these tools to install a program on a computer. To prevent against these attacks, most browsers have settings that force the computer user to authorize the downloading or use of ActiveX, Java, or JavaScript.

Define adware, spyware, and grayware

- **Adware** is a software program that displays advertising on your computer. Adware is usually distributed with downloaded software. Most often, adware is displayed in a popup window. Adware popup windows are sometimes difficult to control and will open new windows faster than users can close them.
- **Grayware** or malware is a file or program other than a virus that is potentially harmful. Many grayware attacks are phishing attacks that try to persuade the reader to unknowingly provide attackers with access to personal information. As you fill out an online form, the data is sent to the attacker. Grayware can be removed using spyware and adware removal tools.
- **Spyware**, a type of grayware, is similar to adware. It is distributed without any user intervention or knowledge. Once installed, the spyware monitors activity on the computer. The spyware then sends this information to the organization responsible for launching the spyware.

Explain Denial of Service

Denial of service (DoS) is a form of attack that prevents users from accessing normal services, such as e-mail and a web server, because the system is busy responding to abnormally large amounts of requests. DoS works by sending enough requests for a system resource that the requested service is overloaded and ceases to operate.

Common DoS attacks include the following:

- Ping of death – A series of repeated, larger than normal pings that crash the receiving computer
- E-mail bomb – A large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing it

Distributed DoS (DDoS) is another form of attack that uses many infected computers, called zombies, to launch an attack. With DDoS, the intent is to obstruct or overwhelm access to the targeted server. Zombie computers located at different geographical locations make it difficult to trace the origin of the attack.

Explain social engineering

A ***social engineer*** is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information. Often, the social engineer gains the confidence of an employee and convinces the employee to divulge username and password information.

Here are some basic precautions to help protect against social engineering:

- Never give out your password
- Always ask for the ID of unknown persons
- Restrict access of unexpected visitors
- Escort all visitors
- Never post your password in your work area
- Lock your computer when you leave your desk
- Do not let anyone follow you through a door that requires an access card

3.4 Explain the tasks required to protect physical equipment

Physical security is as important as data security. When a computer is taken, the data is also stolen. There are several methods of physically protecting computer equipment,

- Control access to facilities
- Use cable locks with equipment

- Keep telecommunication rooms locked
- Fit equipment with security screws
- Use security cages around equipment
- Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment

For access to facilities, there are several means of protection:

- Card keys that store user data, including level of access
- Berg connecters for connecting to a floppy drive
- Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
- Posted security guard
- Sensors, such as RFID tags, to monitor equipment

Describe ways to protect data

The value of physical equipment is often far less than the value of the data it contains. The loss of sensitive data to a company's competitors or to criminals may be costly. Such losses may result in a lack of confidence in the company and the dismissal of computer technicians in charge of computer security. To protect data, there are several methods of security protection that can be implemented.

Password Protection

Password protection can prevent unauthorized access to content, as shown in Figure 1. Attackers are able to gain access to unprotected computer data. All computers should be password protected. Two levels of password protection are recommended:

- BIOS – Prevents BIOS settings from being changed without the appropriate password
- Login – Prevents unauthorized access to the network

Network logins provide a means of logging activity on the network and either preventing or allowing access to resources. This makes it possible to determine what resources are being accessed. Usually, the system administrator defines a naming convention for the usernames when creating network logins. A common example of a username is the first initial of the person's first name and then the entire last name. You should keep the username naming convention simple so that people do not have a hard time remembering it.

When assigning passwords, the level of password control should match the level of protection required. A good security policy should be strictly enforced and include, but not be limited to, the following rules:

- Passwords should expire after a specific period of time.
- Passwords should contain a mixture of letters and numbers so that they cannot easily be broken.
- Password standards should prevent users from writing down passwords and leaving them unprotected from public view.
- Rules about password expiration and lockout should be defined. Lockout rules apply when an unsuccessful attempt has been made to access the system or when a specific change has been detected in the system configuration.

To simplify the process of administrating security, it is common to assign users to groups, and then to assign groups to resources. This allows the access capability of users on a network to be changed easily by assigning or removing the user from various groups. This is useful when setting up temporary accounts for visiting workers or consultants, giving you the ability to limit access to resources.

Data Encryption

Encrypting data uses codes and ciphers. Traffic between resources and computers on the network can be protected from attackers monitoring or recording transactions by implementing encryption. It may not be possible to decipher captured data in time to make any use of it.

Virtual Private Network (VPN) uses encryption to protect data. A VPN connection allows a remote user to safely access resources as if their computer is physically attached to the local network.

Port Protection

Every communication using TCP/IP is associated with a port number. HTTPS, for instance, uses port 443 by default. A firewall is a way of protecting a computer from intrusion through the ports. The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured. Data being transported on a network is called traffic.

Data Backups

Data backup procedures should be included in a security plan. Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster such as a fire or flood. Backing up

data is one of the most effective ways of protecting against data loss. Here are some considerations for data backups:

- **Frequency of backups** – Backups can take a long time. Sometimes it is easier to make a full backup monthly or weekly, and then do frequent partial backups of any data that has changed since the last full backup. However, spreading the backups over many recordings increases the amount of time needed to restore the data.
- **Storage of backups** – Backups should be transported to an approved offsite storage location for extra security. The current backup media is transported to the offsite location on a daily, weekly, or monthly rotation as required by the local organization.
- **Security of backups** – Backups can be protected with passwords. These passwords would have to be entered before the data on the backup media could be restored.

3.5 Encryption

One of the most effective ways to eliminate data loss or theft is to encrypt the data as it travels across the network. However, not all data protection solutions are created equal. While most solutions offer standard AES 256-bit encryption, there are other attributes that must be considered:

Some of encryption facilities are: -

- **Public Key Infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.[1] In cryptography, a **PKI** is an arrangement that binds public keys with respective user identities by means of a certificate authority (**CA**). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (**RA**). The RA ensures that the public key is *bound* to the individual to which it is assigned in a way that ensures non-repudiation.
- **Pretty Good Privacy (PGP)** is a popular program used to encrypt and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed in route. Available both as freeware and in a low-cost commercial version, PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations.

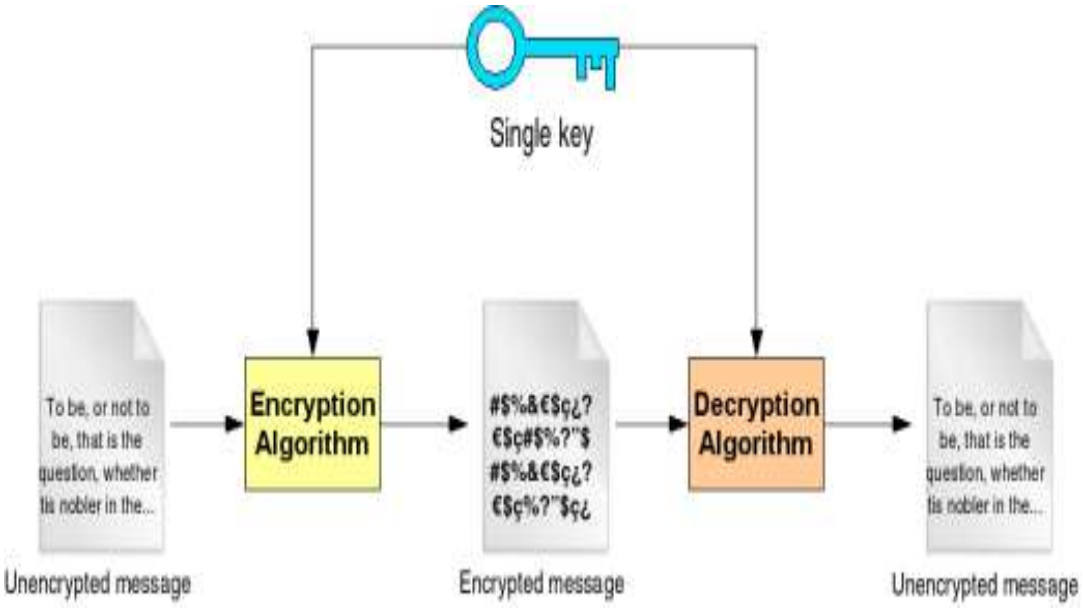
- **Symmetric and Asymmetric ciphers**

In a symmetric cipher, both parties must use the same key for encryption and decryption. This means that the encryption key must be shared between the two parties before any messages can be decrypted. Symmetric systems are also known as shared secret systems or private key systems.

Symmetric ciphers are significantly faster than asymmetric ciphers, but the requirements for key exchange make them difficult to use.

In an asymmetric cipher, the encryption key and the decryption keys are separate. In an asymmetric system, each person has two keys. One key, the public key, is shared publicly. The second key, the private key, should never be shared with anyone.

When you send a message using asymmetric cryptography, you encrypt the message using the recipients' public key. The recipient then decrypts the message using his private key. That is why the system is called asymmetric.



Because asymmetric ciphers tend to be significantly more computationally intensive, they are usually used in combination with symmetric ciphers to implement effect public key cryptography. The asymmetric cipher is used to encrypt a session key and the encrypted session key is then used to encrypt the actual message.

Symmetric ciphers are the oldest and most used cryptographic ciphers. In a symmetric cipher, the key that deciphers the cipher text is the same as (or can be easily derived from) the key enciphers the clear text. This key is often referred to as the secret key. The most widely used symmetric ciphers are DES and AES.

Unlike a symmetric cipher, an asymmetric cipher uses two keys: one key that is kept secret and known to only one person (the private key) and another key that is public and available to everyone (the public key). The two keys are mathematically interrelated, but it's impossible to derive one key from the other. Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.

Difference between AES and DES ciphers

AES	**DES**
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
The date of creation is 1999.	The date of creation is 1976.
Byte-Oriented.	Bit-Oriented.
Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.
Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
The structure is based on a substitution-permutation network.	The structure is based on a Feistel network.
The design rationale for AES is open.	The design rationale for DES is closed.
The selection process for this is secret but accepted for open public comment.	The selection process for this is secret.
AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition	The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation
AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
AES cipher is derived from an aside-channel square cipher.	DES cipher is derived from Lucifer cipher.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective.	Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.

Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems

Cryptosystems can be of two types:

- **Asymmetric** Cryptosystems
- **Symmetric** Cryptosystems

Asymmetric Cryptosystems

In an asymmetric cryptosystem (or public key cryptosystem), there are two different keys used for the encryption and decryption of data. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is impossible to derive the private key from the public key.

The transmitter and the receiver both have two keys in an asymmetric system. However, the private key is kept private and not sent over with the message to the receiver, although the public key is.

Symmetric Cryptosystems

A symmetric cryptosystem (or private key cryptosystem) uses only one key for both encryption and decryption of the data. The key used for encryption and decryption is called the private key and only people who are authorized for the encryption/decryption would know it. In a symmetric cryptosystem, the encrypted message is sent over without any public keys attached to it.

Advantages and Disadvantages of Symmetric Cryptosystems

Advantages

- A symmetric cryptosystem is faster.
- In Symmetric Cryptosystems, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.
- A symmetric cryptosystem uses password authentication to prove the receiver's identity.
- A system only which possesses the secret key can decrypt a message.

Disadvantages

- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every

means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So, the only secure way of exchanging keys would be exchanging them personally.

- Cannot provide digital signatures that cannot be repudiated

Advantages and Disadvantages of Asymmetric Cryptosystem

Advantages

- In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
- The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
- Can provide digital signatures that can be repudiated

Disadvantages

- A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.

Sniffers Monitor network data. A sniffer can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Sniffers usually act as network probes or "snoops." They examine network traffic, making a copy of the data without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels including Ethernet frames.

Secure Shell (**SSH**) Is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs, respectively). The protocol specification distinguishes two major versions that are referred to as SSH-1 and SSH-2.

Deslogin is a remote login program which may be used safely across insecure networks. With deslogin, you may log into a secure remote host from a secure local host without worry about your login password or session information being made visible across the network. Deslogin is a simple stand-alone client and server, which may be used on machines which don't have more

sophisticated security packages such as SPX or Kerberos. No centralized key distribution package is required. Unlike unix Login programs, authentication relies upon arbitrarily long pass phrases rather than eight-character user passwords.

PKZIP Is an archiving tool originally written by Phil Katz and marketed by his company PKWARE, Inc. The common "PK" prefix used in both PKZIP and PKWARE stands for "Phil Katz".

Secure Sockets Layer (SSL) a protocol for encrypting information over the Internet

A **digital signature** or **digital signature scheme** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Self-Check 3

Name: _____ Date: _____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

1. Define what virus is.
2. Define what worms is
3. Define what Trojans is
4. Define what adware is.
5. Define what spyware
6. Define what gray ware
7. Explain Denial of Service
8. Describe ways to protect data

Choose the Correct answer

_____1. Is a hardware or software device designed to block unauthorized access to or from a private computer network?

A. Firefox B. antivirus C. Firewall D. none

_____2. Software that is parasitic/freeloading program written intentionally to alter the way your computer operates without your permission or knowledge.

A. Application B. Programming C. Virus D. Operating

_____3. Is a popular program used to encrypt and decrypt e-mail over the Internet.

A. Pretty Good Privacy (PGP)
B. Public Key Infrastructure (PKI)
C. Certificate Authority (CA).
D. None

UNIT THREE-ANSWERS: SELF CHECK 3

1. **Viruses**

A software virus is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge.

A virus attaches copies of itself to other files such as program files or documents and is inactive until you run an infected program or open an infected document. When activated, a virus may damage or delete files, cause erratic system behavior, display messages or even erase your hard disk.

2. **Worm**

A worm is a self-replicating program that is harmful to networks. A worm uses the network to duplicate its code to the hosts on a network, often without any user intervention. It is different from a virus because a worm does not need to attach to a program to infect a host. Even if the worm does not damage data or applications on the hosts it infects, it is harmful to networks because it consumes bandwidth.

3. **Trojan horse**

The Trojan does not need to be attached to other software. Instead, a Trojan threat is hidden in software that appears to do one thing, and yet behind the scenes it does another. Trojans are often disguised as useful software. The Trojan program can reproduce like a virus and spread to other computers.

A Trojan horse is not a virus because it does not replicate and spread like a virus.

4. **Adware**

Adware is a software program that displays advertising on your computer. Adware is usually distributed with downloaded software. Most often, adware is displayed in a popup window. Adware popup windows are sometimes difficult to control and will open new windows faster than users can close them.

5. **Gray ware**

or malware is a file or program other than a virus that is potentially harmful. Many grayware attacks are phishing attacks that try to persuade the reader to unknowingly provide attackers with access to personal information. As you fill out an online form, the data is sent to the attacker. Gray ware can be removed using spyware and adware removal tools.

6. **Spyware**

a type of grayware, is similar to adware. It is distributed without any user intervention or knowledge. Once installed, the spyware monitors activity on the computer. The spyware then sends this information to the organization responsible for launching the spyware.

7. **Explain Denial of Service**

Denial of service (DoS) is a form of attack that prevents users from accessing normal services, such as e-mail and a web server, because the system is busy responding to abnormally large amounts of requests. DoS works by sending enough requests for a system resource that the requested service is overloaded and ceases to operate.

8. **Describe ways to protect data**

Password Protection

Data Encryption

Port Protection

Data Backups

Choose The correct answer

1. C
2. C
3. A

UNIT FOUR-ESTABLISH MAINTENANCE PRACTICES

This learning guide is developed to provide you the necessary information regarding the Following content coverage and topics

- Determining maintenance requirements specified by the equipment manufacturer.
- Producing maintenance schedules
- Performing diagnostic function
- Configuring software security settings
- Determining unserviceable components
- Using the operating system and third-party diagnostic tools

This guide will also assist you to attain the learning outcome stated in the above. Specifically, upon completion of this module, you will be able to –

- Maintenance requirements specified by the equipment manufacturer are determined.
- Maintenance schedules including removal of dust and grease build -up are produced
- Diagnostic functions including replacing suspect components with other serviceable components and reloading of associated software are performed
- Software security settings to prevent destructive software from infecting the computer are configured
- Unserviceable components are determined whether replaceable through warranty, replacement or upgrade
- Diagnostic functions are performed using the operating system and third-party diagnostic tools

4.1 Establish Maintenance practice

Maintenance requirement is the materials or tools that are important to maintain specific equipment. Maintenance requirement may include but not limited to: -

- Caution
- Attention

Attention is more than just noticing incoming stimuli. It involves a number of processes including filtering out perceptions, balancing multiple perceptions and attaching emotional significance to these perceptions.

There are two major forms of attention: ***passive*** and ***active***. *Passive* attention refers to the involuntary process directed by external events that stand out from their environment, such as a bright flash, a strong odor, or a sudden loud noise. We might say that because passive attention is involuntary, it is easy. *Active* attention is voluntary and is guided by alertness, concentration, interest and needs such as curiosity and hunger.

4.2 Scheduling Maintenance Procedures

Maintenance Schedule is a plan or procedures that are used to maintain equipment and it must be programmed with time of intervals. Maintenance schedules including removal of dust, grease build-up and etc.

Maintenance scheduling can be planed or prepared as: -

- Onsite response
- Remote diagnostic

Onsite response is one of maintenance schedule that display the plan or procedures from the internet.

Remote diagnostics refers to the ability to evaluate the current status of electronic equipment from a remote location. The process involves the establishment of some type of wired or wireless communication between the two points in order for the remote analysis to take place.

Remote diagnostics is the act of diagnosing a given symptom, issue or problem from a distance.

Diagnostic functions

It includes but not limited

- ✓ Replacing suspected components
- ✓ Upgrade components
- ✓ Reloading software’s

Replacing suspected components

Computer hardware or components that can be replaced are: -

- ✓ Motherboards
- ✓ CMOS battery
- ✓ Central processing Unit (CPU)
- ✓ Drives (floppy, hard disk, CD-ROM)
- ✓ Interface cards
- ✓ Fax, modem cards
- ✓ RAM

Upgrade components

Computer hardware or components that can be upgrade are: -

- ✓ Central processing Unit (CPU)
- ✓ RAM

How to Replace a Motherboard

Replacing a motherboard takes a moderate understanding of how the components in your computer are assembled. Before replacing the motherboard, back up all your information to ensure it won't get lost, and go to your motherboard's manufacturer to download any updated drivers that may need to be installed after you install the new motherboard. This will help ensure that changing your motherboard is a success.

Instructions

1. Unplug all power sources to your computer, and remove the casing from your computer. Set aside all screws and small pieces in a bowl so nothing will get lost.
2. Remove all the connectors to the motherboard. This may be your video card, data cables from the hard drives and adapters. Label each one before removing so you can remember exactly where they will attach on your new motherboard.
3. Take out the old motherboard carefully by removing the screws and sliding it out. There is generally little clearance on the sides of the motherboard, so use caution when removing it so nothing gets broken.
4. Compare the new and old motherboards to ensure they're the same. If the new motherboard has cut-outs for integrated sound or game ports, punch out the holes so the wires can fit through them. Do this carefully with a Phillips-head screwdriver or pliers.

5. Place the new motherboard in the case. Double-check to make sure it lines up properly in the computer case before connecting it. Use the seven screws that are included to install the motherboard.
6. Attach the adapters, drives and power connectors to the new motherboard. Locate where you labeled everything before, and install them in the exact same places.
7. Put the computer case back on and turn the power supply back on. If the computer doesn't start up properly, remove the case and double-check to ensure that all the adapters, drives and power supply cords are in the correct position and are tightened securely.

Tips & Warnings

- *Avoid creating static electricity charges while you're installing the new motherboard by wearing a static-free wristband or grounding yourself often by touching the metal case.*

How to Replace a CPU

A computer's central processing unit, or CPU, can be thought of as the computer's brain, which carries out the majority of the calculations and processes needed to make the computer run. As computers age, processors may run more slowly due to power surges, overheating and other stress-induced damage. Replacing a used CPU with a new one can often increase performance, but it is usually more common to install a CPU upgrade rather than a straight replacement.

Things you'll need

- Screwdriver(s)
- Replacement CPU
- Thermal grease or another thermal interface material

Instruction

1. Turn off the computer and unplug all plugs.
2. Open the computer's case and set it on its side.
3. Take off the CPU fan and heat sink. The CPU fan and heat sink will be easy to locate: look for a large fan on top of a fin-like network of metal attached to the motherboard. Depending on your heat sink, you may either have to unscrew it, or undo some plastic clipping mechanisms holding it in place. Sometimes removing the fan first can make removing the heat sink easier. You will likely have to unplug the fan from the motherboard.

4. Undo the securing lever on the processor mount to release the old CPU. The CPU will be held in by a mounting system that is closed when a small lever is pressed down. Left the lever up and release the CPU.
5. Remove the old CPU.
6. Put the new CPU in place, hold it down with a finger, and close the lever to lock it in. Do not exert much force on the CPU; you don't have to press hard, but you may have to wiggle it around a little bit to get it to line up properly before closing the lever.
7. Apply thermal grease liberally to the CPU. The CPU needs a thermal interface material between it and the heat sink to transfer heat effectively.
8. Reinstall the heat sink and fan, making sure the thermal grease is touching both the CPU and the heat sink. Plug the fan back into the motherboard.
9. Close the computer case.

Tips & Warnings

- ***If you are planning on installing replacement CPU that is different than the original CPU, make sure your motherboard can use it first.***
- ***The interior of a computer is susceptible to electric shock. Guard against carrying a dangerous charge. Touch the metal case of the computer at least every couple of minutes to make sure you don't shock the computer's components***

How to Upgrade a Processor

Upgrading the processor in a computer can be one of the easiest ways to give new life to an older, slower machine. While the upgrade itself will take little time or effort, there is significant work that must be done beforehand to ensure that the upgrade is completed successfully.

Instructions

1. Research the computer that is to receive the new processor. There are many different processors on the market, and they are not all compatible with a particular machine. Visit the website of the computer manufacturer. If the computer was assembled from after-market components, check the website of the company that manufactured the motherboard, or main circuit board, of the computer. Find out the processor brand, the processor family, the processor and bus speeds that the machine supports, the type of processor socket on the board and the processor cores or revisions that are compatible with the machine.

2. Shop for a compatible processor from either a local retailer or an online store. The processor must meet all the requirements that your research uncovered, otherwise it will likely be incompatible with the machine. As soon as the processor is received, check it against your original order.
3. Install the processor. Disconnect the computer cables and unplug the machine. Move it to a good work area. Open the side of the machine to obtain access to the interior. Before going any further, discharge any static electricity from your body by using a grounding wrist strap or by touching the bare metal of the computer case.
4. Find the processor. It will be one of the largest objects on the motherboard, near the center, and it will be covered by a large heat sink and fan. On each side of the heat sink, there should be a clip or some other fastener securing it to the processor socket. Gently unhook the clips, taking extreme care not to damage the processor socket, and then disconnect the power lead that runs from the fan to the motherboard. The heat sink then can be pulled away from the processor. It may take some force to separate the heat sink from the processor, depending on the type of thermal transfer compound used.
5. Examine the processor. On one side of the processor socket, there will be a metal or plastic arm that is used to secure the processor in the socket. Slide the end of this arm out from the retaining clip, and lift the arm until it is perpendicular to the motherboard. The old processor can then be gently pulled out.
6. Look at the processor socket. There should be one corner that has a small, 45-degree notch, or another distinguishing mark, cut into it. The processor should have a similar mark. Rotate the processor until the mark is in the same corner as the mark on the socket. Once the processor is orientated correctly, line up the pins and slide the processor into the socket. This should require no force at all. If force is used, the processor pins may be bent and the processor permanently damaged. With the processor seated in the socket, the retaining arm may be lowered and clipped into position.
7. Install the heat sink and fan assembly with a thin layer of thermal compound or a thermal pad between it and the processor. This step transfers heat away from the processor to the heat sink, preventing the processor from overheating. With the heat sink in place, plug the power lead from the fan back into the motherboard.

8. Close the computer. Reconnect the components and test the new upgrade. When everything is done, the computer should be noticeably faster, and it will be able to handle more robust applications and games than it could previously.

4.3 Configuring security setting

There are mechanisms that are used to configure security. Some of them are: -

- ✓ Install firewall
- ✓ Install antivirus
- ✓ Install anti-malware
- ✓ Install anti-spyware

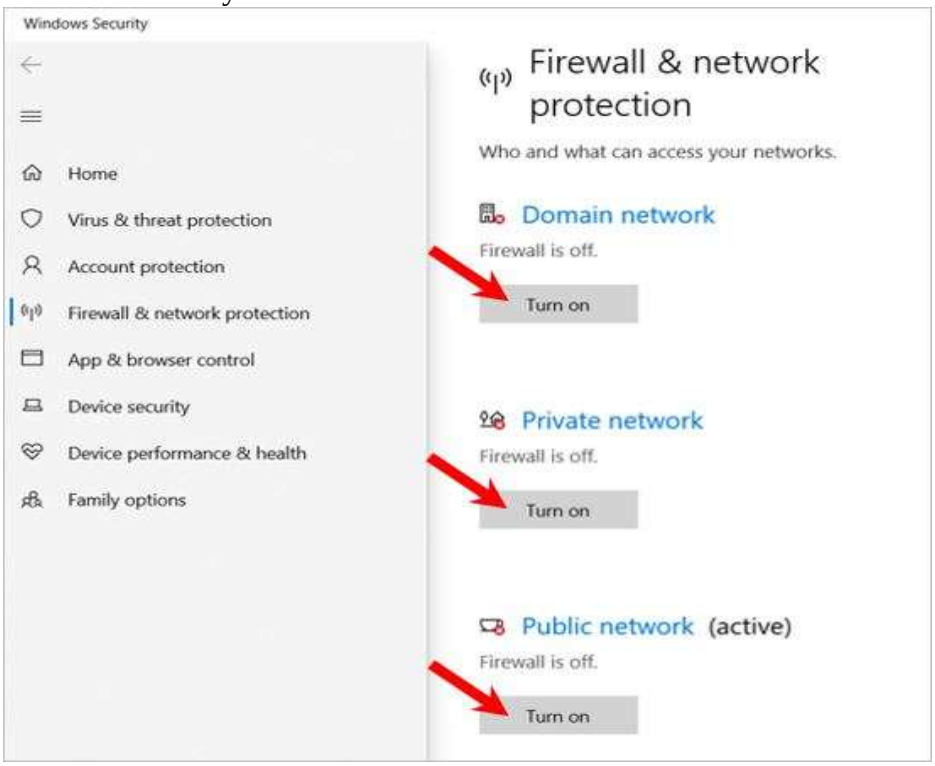
Enabling the Windows 11 firewall

Caution

Only one software firewall should be enabled at a time. If you have an antivirus or other security program installed with its firewall, make sure it is disabled first.

1. Press the Windows key, type "**Windows security**", and then press Enter.
2. In the *Windows Security* window, click the **Firewall & network protection** option on the left or right side.

3. In the next *Windows Security* window, click the **Turn on** button for the *Domain network*, *Private network*, or *Public network*, depending on which firewall profile you want to enable.



4. To turn on Windows Defender Firewall for all three network profiles, repeat step 3 above for each network profile.

Self-Check 4

Name: _____ Date: _____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

1. List the use of Diagnostic functions
2. What are the mechanisms to security?

UNIT FOUR-ANSWERS: SELF CHECK 4

1. **The Diagnostic functions**
    a. Replacing suspected components
    b. Upgrade components
    c. Reloading software's
2. **The security mechanisms are**
    a. Install firewall
    b. Install antivirus
    c. Install anti-malware
    d. Install anti-spyware

Schneidewind, N. F. (2012). *Computer, network, software, and hardware engineering with applications*. John Wiley & Sons.

Barrett, Diane. & King, Todd (2005). "Computer networking illuminated." Jones & Bartlett Learning.

Blundell, Barry (2008). "Computer hardware." Cengage Learning EMEA.

Englander, Irv (2003). "The architecture of computer hardware and systems software: An Information Technology Approach." Wiley.

Sarkar, Nurul (2006). "Tools for Teaching Computer Networking and Hardware Concepts." Information Science Pub.

Developers Profile

No	Name	Qualification (Level)	Field of Study	Organization/ Institution	Mobile number	E-mail
1	ZERIHUN ABATE	MsC (A)	IT	Sabata Poly_technic College	0911858358	Zedoabata2017@gmail.com
2	MICHAEL KASSHUN	BsC (B)	IT	Misrak Poly_technic College	0989308914	Miko3mt@gmail.com
3	SEWAYEHU W/YOHANNES	MsC (A)	IT	Sodo Poly_technic College	0911716733	Sewnet1221@gmail.com
4	YONAS BEYANE	MsC (A)	IT	EthioItaly Poly_technic College	0915007456	yonas.beyane@gmail.com
5	ABEBE MULATU	BsC (B)	IT	Daye Poly_technic College	0904834788	abebemulatumgh@gmail.com
6	SOLOMON YILMA	MsC (A)	IT	APTC (ASSOSA)	0911954729	sollangano@gmail.com
7	YOHANNES BEKELE	BsC (B)	CS	Hawassa (HPTC)	0939497218	Ybekele71@gmail.com
8	TEWDROS GIRMA	MsC (A)	IT	Sheno Poly_technic College	0911835002 0912068479	tedmutd@gmail.com
9	SUBAGADIS GIGAR	BsC	CSIT	MoLS	0920193853	subiartpromo@gmail.com