EBS 107: COMPUTER LITERACY

COURSE MATERIAL

FEBRUARY, 2019

TUMU COLLEGE OF EDUCATION

TABLE OF CONTENT

Contents

UNIT 1: INTRODUCTION TO TODAY'S TECHNOLOGIES: COMPUTERS, DEVICES, AND THE WEB

Introduction

This unit looks at the meaning of the term computer. It further looks at the range of devices that can be termed as computers. It also looks at the various criteria for classifying computers. The various classes of computers are then discussed given their advantages and disadvantages with examples as well as the field in which they are extensively used. The limitations of computers will also be discussed.

1.1 Unit Objectives

After completing this unit, you will be able to:

1. Explain the term computer
2. State the major task performed by a computer
3. Identify the criteria for classifying computers
4. Describe special and general purpose computers with examples
5. Describe analogue, digital and hybrid computers with examples
6. State the advantages and disadvantages of analogue, digital and hybrid computers
7. Describe supercomputer, mainframe computer, mini computer and microcomputers

1.2 What is a Computer?

The term computer is derived from the word compute. It is literally used to identify any device that calculates. It works under the direction and control of a program or instruction. It is capable of reading, storing, and processing data to produce meaningful results called information. The operations that it performs are based on instructions provided to it. Computers by themselves are not intelligent devices. Thus, they have no brain and cannot work on their own. They are referred to as hardware because they are composed of physical equipments made of metals and plastics. In spite of all these, they are capable of handling well-defined instructions with minimal errors at a very fast speed. They are made up of a combination of electronic and electromechanical devices. **The purpose of a computer is to speed up problem solving and increase productivity.**

A computer can therefore be defined as follows;

- An electronic device that operates under the control of instructions stored in its own memory, accept data, process the data according specified rules, produce results, and store the results for future use.

- ❖ A programmable, electronic device, that accepts data, performs operations on the data based on the instructions stored in its own memory, to produce results that can be stored for future use or sent to another device.

- ❖ An electronic data processing machine which accepts data from the outside world in the form of an input and manipulates, calculates, or computes based on the set of instructions supplied and stored in the memory and gives the required or desired results in the form of an output to the user.

From the above definition, computers are

- Electronic and Programmable devices
- Operates under the control of a set of instructions that is stored in its memory
- Accepts data that a user supplies
- Manipulates the data according to the programmed instructions
- Produces results called information
- Stores the results for future use

Being **electronic** means it is made up of components that controls the flow of electric currents for the purpose of processing information and controlling systems. Examples include **transistors** and **diodes**. These electronic components are usually small and can be grouped together into packages called integrated circuits. In another vein being **programmable**, means a computer will do whatever the instructions or program tells it to do. The program determine what task a computer is capable of performing.

The above descriptions and explanations best suits the class of computers termed general purpose computers.

1.3 Limitations of a Computer

Computers do not have brains and as such do not understand anything. They are merely a combination electronic circuits in which bits of information and data travels at lightning speed. In short, computers lack the intelligence and common sense of human beings. It is good to know that computers can only perform tasks that can be broken into programmable steps, just as the way a recipe is prepared. Computers therefore perform decision-making operations. These decision-making operations are usually made up of the programmable steps called **algorithm**. The limitations of a computer can be summarised as follows;

- ❖ Computer cannot operate or function by itself without the assistance of human beings. It is totally under the control of the user.
- ❖ Computer cannot think on its own. It has to be given instructions to perform any operation.
- ❖ It can only perform task which can be expressed in a series of finite steps.

- ❖ It does not have intuition. It cannot draw conclusion without going through all intermediate steps.
- ❖ It cannot learn from experience.
- ❖ It needs well-defined instructions to perform any operation.
- ❖ A computer can only perform what it is programmed to do.

Besides the above limitations, the computer have several **disadvantages**. These are;

- They require a clean, dust free environment with a relatively constant background temperature;
- They require specialist staff for operating and for programming;
- They normally do not question the accuracy or truth of input information, although they can be programmed to accept them only if they are within certain predetermined limits
- They are not capable of bearing creative or original thoughts
- They pose data insecurity problems

1.4 Classification of Computers

Computers vary widely in terms of their size, shape and the purpose they serve. They are used by individuals, as well as public and private organisations for a variety of applications ranging from scientific to commercial and military. Irrespective of their size, purpose, shape and location for which they are used, they serve one goal, thus, to take data and convert it into meaningful information for decision making. Computers can therefore be classified based on the following criteria:

- **Purpose**
- **Type**
- **size/capacity**

1.4.1 Classification by Purpose

Computers are designed for different purposes. Depending on how **flexible** the device or computer is in terms of the task or problems it solves or performs. It also takes into consideration how easily the device can be adapted to solve problems. With this criteria, computers fall under two main groups. These are;

- ❖ **Special purpose computers**
- ❖ **General purpose computers**

Special purpose computers

They are computers specially designed to solve or perform a **limited** number of tasks. They are **restricted** to solving a particular task. They solve a specific problem or to perform a specific task. The task or job they perform are restricted in nature. The computer program for solving the problem is built right into the computer. They respond to specific instruction in a well-

defined manner. As such they also referred to as **dedicated computers**. These instructions are incorporated into the design of their internal storage system so that it can perform the given task on a simple command. Thus the set of instructions required for it to perform the task is built into the hardware, hence cannot be used for any other application besides the one for which they have been designed to solve. Being designed for a specific task, they can provide results quickly and efficiently.

They are used in:

- **military operations** to control military weapons system and to direct the operations of spacecraft, air planes, tankers and submarines
- **in industries**
  - To control devices that process steel or chemicals, robots and automobiles.
  - Also managing thermal or chemical plants.
  - They are also used to automate some industrial processes.
- **Home/Household appliance** such as refrigerators, Television sets (TVs), Microwave oven, water heaters contain small embedded computers or microcontroller's that control them.

Examples of special purpose computes are; speedometer, electric meter, microwave, CT (computerized tomography) scanners at the hospitals, fuel dispenser. The micro controllers in digital watches, refrigerators. Below are some examples of special purpose computers.

Figure 3.2

General purpose computers

General purpose computers are designed to perform or solve a **wide range** of tasks or problems. They are computers designed to meet the needs of many different applications. The instructions required to perform a particular task are not permanently wired into the internal memory. They can easily be adapted to perform a particular task or solve problems. They have the ability to store and run different programs. This provides them with the ability to perform several tasks based on the instructions specified in those programs. These machines can be used for various applications, ranging from scientific to business applications. **They are also known as all-purpose digital computers**. They are quite flexible and considerably expensive. For example the desktop computer can be used to play music, listen to news, print letters, send messages, play games etc.

Below are some specific characteristics of general-purpose computers:

- they have memory that stores the set of instructions or programs that have been prepared
- programs designed to solve problems in different areas can be executed one after the other
- they can be given different programs to solve different types of problems can store large amount of data and the programs necessary to process them

1.4.2 Classification by Type

This criteria is based on the electronic or operating principle of the computer. Based on this principle computer systems can be classified into three main types. These are:

- **Analog computer**
- **Digital computer**
- **Hybrid computer**

Analog computers

They are a class of electronic systems that recognises data as a continuous measurement of physical quantity such as pressure, temperature or voltage along a continuous scale. They operates on the principle of measuring. Data processing in analogue computers is continuous and produce output that is usually read from a scale in the form of dial-gauge readings or graphs. The term **analogue** means continuous. The value of an analogue quantity is often open to interpretations. They are basically measuring devices or instruments. They measure the continuous variables in a physical quantity.

Examples of analogue computers are **speedometer, thermometer, and fuel pump.** With the **speedometer,** the deflection of the needle is proportional to its speed. The angular position of the needle represents the value of the speed. The **fuel pump** on the other hand has a microprocessor attached to the pump which converts the fuel flow measurements and displays

the quantity and price. They are usually used in the scientific, engineering and industrial environments to simulate various physical systems or to automatically control industrial processes in areas where temperature, pressure or flow of liquids are monitored continuously.

Advantages of Analog Computers
The major advantages of analogue computers are;

- they are usually less expensive
- have very high speed
- requires less programming effort

Disadvantages of Analog Computers
The major disadvantages of analogue computers are:

- alphanumeric information cannot be processed
- Results are not accurate. Often open to interpretation
- Very limited memory capacity. Cannot store large amount of data or information
- it gives very little precision
- very rigid and difficult to operate

Below are some of the features of analogue computers;

- its output is unusually displayed on a scale or graph
- It is difficult to operate and use.
- does not operate with the digital signals
- has low memory and fewer functions
- has a low degree of accuracy

Digital computer
They are computers designed to work on the **principle of counting**. They operates on data in the form of digits. They are electronic devices designed to manipulate physical quantities or information that are represented in digital form. The term **digital** means discrete. It refers to a type of electronic signal that is processed, sent and stored in discrete form. Digital computers can take only discrete values. They represent data in discrete numbers and process them using standard arithmetic operations. They are primarily **counting devices**.

They are high speed programmable electronic devices that perform mathematical calculations, compare values and stores the results. They recognise data by counting and converting discrete signals that represent letters, numbers and other special characters into a series of **0s** (low voltage signal) and **1s** (high voltage signal). These **0s** and **1s** are referred to as **b**inary dig**its, bits** for short**.** Digital computers use binary digits to process data. They are mostly used in commercial, administrative applications and for mathematical computations. Examples are calculator, digital clock, personal computers and etc.

Advantages of Digital Computers
The major advantages of digital computers are;

- information storage is easy
- have high level of accuracy and precision
- operations can be programmed and automated
- digital circuits are less affected by noise
- extremely reliable

Disadvantages of Digital Computers
The major disadvantages of digital computers are;

- they are very expensive
- requires significant programming effort
- requires specialized knowledge and skill to operate

Hybrid computer
They are computers that incorporates features of both analogue and digital computers. They use the analogue component to collect data and process data while the digital component are mostly used for storage of data. They have the speed of analogue computers and the accuracy of digital computers. They are mostly used in scientific applications and the field of engineering or industrial control processes. Examples are **money counting machine**, **electric meter**, **fuel pump or dispenser** and the **ATM machine**. As shown the figure below.

Difference between Analog and Digital Computers

The table below shows the difference between analogue and digital computers

ANALOGUE COMPUTER	**DIGITAL COMPUTE**R
Operates on the principle of measurement	Operates on the principle of counting
Data signals changes continuously	Data signals changes in discrete states
Outputs are read on a scale or graphs	Outputs are displayed in digits
Speed of operation is very high	Speed of operation is low
Low precision and accuracy	Very high precision and accuracy
Does not require high programming effort	Requires a very high programming effort
Limited memory for storage	Vast memory for data and program

1.4.3 Classification by Size/Capacity

The capacities of earlier computers were measures in terms of their physical size. Today physical size is not a good measure of capacity because models of computers have become more compact as a result of the development of integrated circuits. This technology have reduced the size and increased the power of computers more than the room-sized computers made several decades ago. **Capacity of computers are now expressed in terms of the volume of work that the computer can handle, the speed of processing and the functional units.** This criterion for classifying computers is based on the functional capacity such as **speed**, **memory capacity**, **performance** and **configuration**. Based on this criterion, digital computers can be classified as:

- **Supercomputer**
- **Mainframe computer**
- **Minicomputer**
- **Microcomputer**

Supercomputer

They are the fastest, most powerful and most expensive of all the computers. They have the highest processing speed at any given time. They are designed to process huge scientific data like solving scientific and engineering problems such as scientific simulations, nuclear energy research, electronic design and analysis of geographical data as in weather forecasting. They are multi-user general-purpose computer. They are capable of processing more than 135 trillion instructions per seconds.

Mainframe computer

They are large, powerful and expensive general-purpose computer that can handle hundreds or thousands of connected users or clients at the same time. They have powerful input/output, processing and storage system. This makes them capable of processing and storing large amount of data for thousands of connected users at the same time. They are used to manage large amount of centralized data and programs. They store large amount of data, instruction and information.

Mostly used by large organisations like airlines (for ticket reservation), banks (manage customer accounts), universities, government agencies and hospitals that handle very large volume of data. They are usually stored in special rooms that have a controlled climate. They are mostly accessed by means of terminals or personal computers. They are also multi-user general-purpose computer.

The main features of mainframe computers are as follows;

- have several CPUs
- support multiple operating system
- have very fast processing speed
- very large amount of storage space
- very huge internal memory
- slower, less powerful and less expensive than supercomputer
- used large and complex applications faster and more powerful than minicomputers.

The image below shows a Mainframe computer being configured for use.

Minicomputers

They make up the middle class of computers in terms of size and processing power. They are medium-sized computers that are larger and more powerful than the **microcomputers**. They are smaller and less powerful than mainframe computers. They are a scaled-down version of a mainframe computer. They are designed to handle the processing needs of smaller organisations. They also support multiple users. They are also multi-user general purpose computer. May be used as **servers or Internet servers**.

Microcomputer

They are also called **Personal Computers**, PC for short. They constitute the smallest, cheapest and less powerful of all the general purpose digital computers. They are single user and low-cost computers. A personal computer consists of a microprocessor as well as storage and an input/output unit. They are available for individual use. A personal computer (PC) is a mobile computer or desktop that can perform all of its input, processing, output, and storage activities by itself and is intended to be used by one person at a time. There are two major makes of personal or microcomputers on the market. These are the;

IBM PCs or IBM compatibles:- IBM was the first company to make and name its microcomputers as personal computers. Examples are Power PC Based Computers and the IBM series 365, Aptiva C3D computers, NetPC computers etc. The term IBM Compatible, refers to any personal computer based on the original IBM personal computer design. They are also referred to as clone computers. Companies such as Dell,Toshiba,Gateway, HP and etc. sell IBM-Compatible computers. IBM or IBM-compatible computers usually use **Windows operating system**.

Apple Mac:-(Apple PCs) computers include eMac computers, Power Book computers, iBook computers, Power Mac, G5 computers, iMac, i-Pods etc. They are not compatible with neither IBM nor the IBM-Compatible computers. Apple computers usually use a **Macintosh operating system (Mac OS)**. Steve Jobs was the brain behind Apple Computers or Mac PCs. He was the first to use PCs with mouse and graphical user interface.

Categories of Personal Computers

Personal computers are available in a variety of configurations. These configurations are based on the size and functionality of the computer or device. Personal computers can be classified as:

- Desktop computers
- Portable Computers
- Handheld Computers

Desktop computers

This are general purpose, stand-alone computers designed to be used on a desk. They are not portable, thus they are too big to be carried around. They are restricted for use at a single location. They are composed of separate **monitor** or **display unit**, **keyboard**, **mouse** and a **system unit** that is composed of a **processor, memory,hard disk drive for storage.**

They are the most common microcomputer. They are not very expensive and it is suited to the needs of single-user, business and organisations. Some of the popular companies that manufactures and sells desktop computers are Dell, Hewlett Packard(HP), Lenovo, Toshiba, Microsoft, Compaq. The main component of a desktop personal computer is the system unit. Desktop computers comes in three different designs. These are;

The tower design :- the system unit is designed to sit vertically on the floor or on a desk.

The traditional desktop design :- where the system unit is designed to sit horizontally on the desk with the monitor on top.

All-in-one desktop design :-this design incorporates the monitor and the system unit into a single piece of hardware. This design was originally popular with the Mac systems.

Portable Computers

They are a type of personal computer that can be carried from place to place. They are also referred to as mobile computers. They are small enough to be moved around easily in bags or carriers. They are battery-powered, single-user and general purpose computers. Examples of portable or mobile computers are **Notebook PCs**, **Tablet PCs** and **Netbook PCs.**

Notebook PCs :- are portable computers designed to fit on your lap. For this reason, they also called **laptop computers**. They have their keyboard fitted on top of the system unit. The monitor is attached to the system unit by means of hinges. They can operate on alternating current or battery. Have very low power consumption. A **laptop**, also called a notebook

computer, is a thin, lightweight mobile computer with a screen in its lid and a keyboard in its base.

Tablet PCs :- are a special type of portable computer integrated into a flat multi touch screen. They uses an onscreen virtual keyboard and can also accept handwritten input from the screen. Can also accept input from a stylus pen. Very useful in taken notes at lectures, meeting and conferences. They also support voice input. Can be connected or attached to a separate keyboard via cables or Bluetooth. The **iPad and Galaxy Tabs** are typical examples of tablet PCs

Netbook PCs:- a small lightweight laptop computer. They are battery-powered. They are inexpensive and relatively smaller in size than the laptop computers. They have smaller features and lesser capacities in caparison with the laptop computers (e.g Chromebook).

Handheld Computers

They are battery-powered computing device that is small enough to fit into the palm of the hand or pocket. Are pen-based and battery-powered. They are mostly referred to as **mobile devices**. They store programs and data on memory cards. They do not have have hard disk but rather used flash memory card as storage mediums. Use pen-like stylus as input device. It also accept handwritten input directly on the screen. They are not as powerful as desktop or notebook computers. Most often, they are connected to a desktop or a notebook computer to exchange information. Common examples of handled computers or mobile devices are Personal Digital Assistants(PDAs) ,smart phone and game console.

PDAs:- stand for Personal Digital Assistants. They are handheld computers that fits into the palm of the hand. Less powerful than desktop or notebook computer. They use memory card to store data and programs. Are battery-powered and comes with a screen touch and sometimes stylus pen. Some have built-in miniature keyboard, voice input as well cameras. PDAs house a microprocessor, flash ROM,RAM and various hardware components. They provide personal organiser function such as calendar, appointment book, a calculator and a notepad. They have Internet enabled feature so can be used to send and receive e-mails. Can also be used effectively as portable audio players and web browsers.

Smart phone:- these are Internet-enabled telephone that usually provides PDA capability. They combine the functionality of PDAs and a cellular telephone. It allows users to send and receive e-mails messages, access the web. They also have built-in cameras with which you can take and share photographs and video.

Game console :- are handheld or mobile computing device designed for a single-player or multi player video games. Standard game consoles use handheld controllers as input device; a television screen as an output device and hard disk, CDs, DVDs and memory cards for storage. Examples are Sony's PlayStation 3, Microsoft's Xbox 360 and Nintendo's Wii.

1.5 Advantages and Disadvantages of Computers

Advantages

- SPEED: they can accomplish large amount of tasks very fast. **Fast response**
- HIGH CAPACITY: they have the ability to handle multiple jobs at ones.
- ITERATIVE ABILITY: they are good at performing repetitive tasks such as calculations
- ACCURACY
- DEPENDABILITY
- Ability to search and sort
- Vast storage

Disadvantages

- They require a clean, dust free environment with a relatively constant background temperature;
- They require specialist staff for operating and for programming
- They normally do not question the accuracy or truth of input information, although they can be programmed to accept them only if they are within certain predetermined limits
- They are not capable of bearing creative or original thoughts
- They pose data insecurity problems

1.6 Uses of Computers in Education

Computer have wide variety of applications in education.

- Communication: teachers can use electronic whiteboards (smartboards) and projectors to improve lesson delivery. Teachers and students may use email and text messages to communicate. Communication tools such as word processing could be used to enhance the presentation of school work.
- Learning tools: several educational programs are available on the market to improve student's skills in particular areas. Computer Based Training (CBT) programs can procured for many practical subjects areas.
- Distance Learning: Videoconferencing, webcasts and VLEs (Virtual Learning Environments) allow students to log in and work from home.
- Administration: Most aspects of school administration are now handled by Computer and ICT tools. Online registration, Exams reports or results, accounts/budgeting and timetabling are some assistive areas of computers in School administration.
- Leaning Management systems: Computer Assisted Assessment, Computer based Assessment, Computer based Testing etc.

Topics for further research

i. Historical dev of Computers
ii. Generations of Computers
iii. Careers in ICT (Computer Science)

UNIT 2: CONNECTING AND COMMUNICATING ONLINE

2.1 Unit Objectives

After completing this unit, you will be able to:

1. Discuss the evolution of the Internet
2. Briefly describe various broadband Internet connections
3. Describe features of browsers and identify the components of a web address
4. Explain benefits and risks of using online social networks
5. Describe uses of various types of websites: search engines; online social networks
6. Explain how email, email lists, Internet messaging, chat rooms, online discussions, VoIP, and FTP work
7. Identify the rules of netiquette

2.2 The Internet

The **Internet** is a global network of computers. It is a worldwide collection of networks that connects millions of businesses, government agencies, educational institutions, and individuals. Each of the networks on the Internet provides resources that add to the abundance of goods, services, and information accessible via the Internet. Today, billions of home and business users around the world access a variety of services on the Internet using computers and mobile devices. The web, messaging, and video communications are some of the more widely used Internet services

Other Internet services include chat rooms, discussion forums, and file transfer. The Internet consists of many local, regional, national, and international networks. Both Public and private organizations own networks on the Internet. These networks, along with phone companies, cable and satellite companies, and the governments, all contribute toward the internal structure of the Internet.

Who owns the Internet?

No single person, company, institution, or government agency owns the Internet. Each organization on the Internet is responsible only for maintaining its own network. The **World Wide Web Consortium (W3C),** however, oversees research and sets standards and guidelines for many areas of the Internet. The mission of the W3C is to ensure the continued growth of the web. Nearly 400 organizations from around the world are members of the W3C, advising, defining standards, and addressing other issues.

What is an intranet?

Recognizing the efficiency and power of the Internet, many organizations apply Internet and web technologies to their internal networks. **An intranet** (intra means within) is an internal network that uses Internet technologies. Intranets generally make company information

accessible to employees and facilitate collaboration within an organization. Files on an intranet generally are not accessible from the Internet openly. One or more servers on an intranet host an organization's internal webpages, applications, email messages, files, and more. Users locate information, access resources, and update content on an intranet using methods similar to those used on the Internet. A company hosts its intranet on servers different from those used to host its public webpages, apps, and files. It is considered a private network.

Sometimes a company uses an **extranet** (extra means outside or beyond), which allows customers or suppliers to access part of its intranet. Package shipping companies, for example, allow customers to access their intranet via an extranet to print air bills, schedule pickups, and track shipped packages as the packages travel to their destinations.

2.2.1 Uses

Why should one connect to the internet?

i. To share information, photos and videos. **Communication**
ii. To communicate with other people and make new friends. **Social Networking**
iii. For shopping for goods and services online. **E-commerce**
iv. To do banking and investments.
v. To play games online. Listen to music, and watch videos. **Entertainment**

2.2.2 Advantages and Disadvantages of the Internet

Advantages of the Internet

1. The internet makes communication easier and faster. The uses of e-mails and other real time communication tools allow individuals and organisations to share information very fast to improve decision making.
2. Searching for information has been made easier by the internet. Search engines like Google.com, Yahoo.com are at your service through the internet. There is a huge amount of information available on the internet for just about every subject known to man, ranging from government law and services, trade fairs and conferences, market information and technical support.
3. The Internet presents individuals with endless sources of entertainment. There are numerous games on the internet that can be downloaded free. Instead of watching movies at cinema, now there are companies offering their services where you just can download or order your favourite movie and watch it with a fast internet connection.
4. Through the internet, shopping has also been enhanced greatly. There are many websites selling varieties of products online and one just needs to select or bid for the desired product and entire financial transactions can be conducts through the internet. Transfer of money is also no longer a times consuming job and with just a click of a button you can easily transfer funds to any place you wish.

Disadvantages of the Internet

- You can get addicted to internet
- Some people use the internet for fraud, which you can be robbed online.
- Children access pornographic material on the internet.
- Children spend too much time in front of their computers browsing the net instead of doing their school work.
- Viruses can be transferred from the internet to your computer.

2.2.3 Internet and Its Evolution

The Internet has its roots in a networking project started by the Pentagon's **Advanced Research Projects Agency (ARPA)**, an agency of the U.S. Department of Defense. ARPA's goal was to build a network that (1) allowed scientists at different physical locations to share information and work together on military and scientific projects and (2) could function even if part of the network were disabled or destroyed by a disaster such as a nuclear attack.
That network, called **ARPANET (Advanced Research Projects Agency Network)**, became functional in **September 1969**, linking scientific and academic researchers across the United States.

The original **ARPANET** consisted of four main computers, one each located at the University of California at Los Angeles, the University of California at Santa Barbara, the Stanford Research Institute, and the University of Utah. Each of these computers served as a host on the network. **A host computer**, more commonly known today as a **server**, is any computer that provides services and connections to other computers on a network. Hosts often use high-speed communications to transfer data and messages over a network. By 1984, ARPANET had more than 1,000 individual computers linked as hosts. Today, millions of hosts connect to this network, which is now known as the Internet.

2.3 Connecting to the Internet

Users can connect their computers and mobile devices to the Internet through **wired or wireless technology** and then access its services free or for a fee. With wired connections, a computer or device physically attaches via a cable or wire to a communications device, such as a modem or Router that transmits data and other items over transmission media to the Internet. For wireless connections, many mobile computers and devices include the necessary built-in technology so that they can transmit data and other items wirelessly. Computers without this capability can use a wireless modem or other communications device that enables wireless connectivity. A wireless modem, for example, uses a wireless communications technology (such as cellular radio, satellite, or Wi-Fi) to connect to the Internet.

Today, users often connect to the Internet via broadband Internet service because of its fast data transfer speeds and its always-on connection. Through broadband Internet service, users

can download webpages quickly, play online games, communicate in real time with others, and more.

Many public locations, such as shopping malls, coffee shops, restaurants, schools, airports, hotels, and city parks have Wi-Fi hot spots. A **hot spot** is a wireless network that provides Internet connections to mobile computers and devices. Although most hot spots enable unrestricted or open access, some require that users agree to terms of service, obtain a password (for example, from the hotel's front desk), or perform some other action in order to connect to the Internet.

Home and small business users can share and provide wireless Internet connections by creating their own Wi-Fi hot spot through a communications device in the home or business that is connected to broadband Internet service. Instead of a stationary Wi-Fi hot spot, some users opt to create mobile hot spots through mobile broadband Internet service via a separate communications device or a tethered Internet-capable device. Tethering transforms a smartphone or Internet-capable tablet into a portable communications device that shares its Internet access with other computers and devices wirelessly.

Internet Service Providers

An **Internet service provider** (**ISP**), sometimes called an Internet access provider, is a Business that provides individuals and organizations access to the Internet free or for a fee. ISPs often charge a fixed amount for an Internet connection, offering customers a variety of plans based on desired speeds, bandwidth, and services. In addition to Internet access, ISPs may include additional services, such as email and online storage. Internet service providers in Ghana include:

- **MTN Ghana**: Wireless internet via sim card. Coverage in most parts of the country
- **Vodafone Ghana**: Fixed line broadband and Wireless internet via sim card.

- **Surfline Ghana**: Wireless internet via sim card currently covering Accra, Tema and Takoradi
- **Globacom (glo)**: Wireless internet via sim card, and data hosting
- **iBurst Ghana**: Wireless internet only, no mobile phone services available.
- **Busy internet**: Offers broadband and data hosting.
- **K-NET**: Broadband service

Bandwidth represents the amount of data that travels over a network. A higher bandwidth means more data transmits. Data sizes typically are stated in terms of megabytes and gigabytes. Instead of locating a hot spot, some users prefer to subscribe to a mobile service provider, such as MTN , so that they can access the Internet wherever they have mobile phone access. A **mobile service provider**, sometimes called a wireless data provider, is an ISP that offers wireless Internet access to computers and mobile devices with the necessary built-in wireless capability (such as Wi-Fi), wireless modems, or other communications devices that enable wireless connectivity. An antenna on or built into the computer or device, wireless modem, or communications device typically sends signals through the airwaves to communicate with a mobile service provider.

The **domain name system (DNS)** is the method that the Internet uses to store domain names and their corresponding IP addresses. When you enter a domain name (i.e., google.com) in a browser, a **DNS server** translates the domain name to its associated IP address so that the request can be **routed** to the correct computer. A DNS server is a server on the Internet that usually is associated with an ISP.

2.3.1 Devices

Connecting to the internet requires the use of certain devices. These devices include **Modems** (**Mo**dular and **Dem**odulator)**, switch/hub and Routers**. Refer to unit 7 for further discussion on network devices.

2.4 World Wide Web

While the Internet was developed in the late 1960s, the World Wide Web emerged in the early1990s as an easier way to access online information using a **browser**. Since then, it has grown phenomenally to become one of the more widely used services on the Internet.

The World Wide Web (WWW), or web, consists of a worldwide collection of electronic documents. Each electronic document on the web is called a **webpage**, which can contain text, graphics, animation, audio, and video. Some webpages are **static (fixed),** others are **dynamic (changing)**.

Visitors to a static webpage all see the same content each time they view the webpage. With a dynamic webpage, by contrast, the content of the webpage generates each time a user displays it. Dynamic webpages may contain customized content, such as the current date and time of day, desired stock quotes, weather for a region, or ticket availability for flights. The time

required to download a webpage varies depending on the speed of your Internet connection and the amount of graphics and other media involved.

A website is a collection of related webpages and associated items, such as documents and photos, stored on a web server. A **web server** is a computer that delivers requested webpages to your computer or mobile device. The same web server can store multiple websites. As web technologies advanced in the mid-2000s, industry experts introduced the term **Web 2.0** to refer to websites that provide a means for users to share personal information (such as online social networks), allow users to modify website content (such as wikis), and provide applications through a browser (such as web apps).

Web Addresses

A webpage has a unique address, called a **web address** or **URL (Uniform Resource Locator**). For example, the web address of http://www.myjoyonline.com identifies Joy News online webpages. A browser retrieves a webpage using its web address. If you know the web address of a webpage, you can type it in the **address bar** of the browser.

A web address consists of a protocol, domain name, and sometimes the host name, path to a specific webpage, or file name of the webpage. The http, which stands for **Hypertext Transfer Protocol**, is a set of rules that defines how webpages transfer on the Internet. Many web addresses begin with **http://** as the protocol. The text between the protocol and the domain name, called the host name, identifies the type of Internet server or the name of the web server. The www, for example, indicates a web server.

2.4.2 Browsers

A Browser is an application program that provide access to web resources. Users with an Internet connection can use a browser to access and view webpages on a computer or mobile device. Internet-capable mobile devices such as smartphones use a special type of browser, called a mobile browser, which is designed for their smaller screens and limited computing power. When you run a browser, it may retrieve and display a starting webpage, sometimes called a home page. The initial home page that is displayed is specified in the browser. You can change your browser's home page at any time through its settings, options, or similar commands.

Another use of the term, **home page**, refers to the first page that is displayed on a website. Similar to a book cover or a table of contents, a website's home page provides information about its purpose and content. Many websites allow you to personalize the home page so that it contains areas of interest to you.

Examples of Browsers

- **Chrome:** Google's Chrome is one of the newer browser offerings, first released in 2008. This free browser is available for Windows and Mac OS and must be downloaded and installed. It includes a large number of security features. Chrome has independent tabbed browsing; if one tab develops a problem, the other tabs continue to function.

- **Firefox:** Developed by the Mozilla Corporation for computers running Windows, Mac OS, and Linux, Firefox is recognized for its extensive array of plug-ins. This free general purpose browser was first released in 2004 and must be downloaded and installed. It has enhanced privacy and security features, a spelling checker, tabbed browsing, and a password manager.

- **Internet Explorer:** Microsoft's free browser, Internet Explorer, is available primarily for Microsoft Windows and comes preinstalled. First released in 1995, the browser features the capability to rearrange tabs, protection against phishing and malware, and settings to delete information about searches performed and webpages visited.
- **Opera:** This second-oldest browser is free, fast, and small. Used on both computers and mobile devices, Opera must be downloaded and installed. It began as a research project in Norway in 1994 and introduced several features found on most of today's browsers.
- **Safari:** Preinstalled on Apple computers and mobile devices, Safari has been the default browser for Mac OS since 2003 and is relatively new to Windows. The browser is recognized for its sleek design, built-in sharing with online social networks, fast performance, parental controls, and ease of use.

Mobile Browsers

Many browsers are included by default with some mobile devices and smartphones. Their features vary greatly. Some allow users to zoom and use keyboard shortcuts with most websites, while others display only websites optimized for mobile devices. The more popular mobile browsers are Chrome, Firefox, Internet Explorer, Safari, and Opera Mini.

2.4.3 Search Engines

A web **search engine** is software that finds websites, webpages, images, videos, news, maps, and other information related to a specific topic. Some search engines, such as Bing, Google.com, Ask.com and Yahoo!, are helpful in locating information on the web for which you do not know an exact web address or are not seeking a specific website. Those that work with GPS devices or services are location based, meaning they display results related to the device's current geographical position. For example, your smartphone may be able to display all gas stations within a certain distance of your current location. Some search engines restrict searches to a specific type of information, such as jobs or recipes.

Search engines typically allow you to search for one or more of the following items:

- Images: photos, diagrams, and drawings
- Videos: home videos, music videos, television programs, and movie clips
- Maps: maps of a business or address, or driving directions to a destination
- Audio: music, songs, recordings, and sounds
- Publications: news articles, journals, and books
- People or Businesses: addresses and phone numbers
- Blogs: specific opinions and ideas of others

Search engines require that you enter a word or phrase, called **search text**, to describe the item you want to find. If you misspell search text, search engines typically correct the misspelling or identify alternative search text. Some also provide suggested search text, links, and/or images as you type your search text. Depending on your search text, search engines may respond with thousands to billions of search results, sometimes called **hits**.

2.5 Types of Websites

Online Social Network: provide avenues to engage with family and friends online. Sites as Facebook.com are used to facilitate social communications.

Other types of websites include: News sites, Educational sites, Business sites, Health and Fitness sites, Entertainment sites, Banking and Finance sites, Travel and Tourism sites, E-commerce and Sports site.

Web publishing is the creation and maintenance of websites. The process of web publishing is shown in the diagram below:

2.6 Domain Name types

A web domain name is a sequence of letters and/or numbers/hyphens separated by one or more periods (".") that act as a pointer to a unique numerical address (IP) on a computer network such as the Internet. That address may host publicly available content (e.g a web site), or may be a private intranet.

A web domain name always ends with an extension of 2 or 3 characters. These characters can signify the country the website address is associated with or the type of organization.

TLD - Top Level Domains

These are at the highest level in the DNS structure of the Internet. There are several different types of TLD's, being:

ccTLD - country code Top Level Domains

Two letter domains established for geographical locations; for example; .gh signifies Ghana. When originally designated, usually only residents of a country could register their corresponding ccTLD, but over the years quite a few countries have allowed parties outside their shores to register website names.

In Ghana, **NITA (National Information Technology Agency)** is responsible for the registration of .gh domain names. NITA has given **GHANA.COM** the rights to register .gh domain names

gTLD - generic Top Level Domain

The best known generic TLD's include .com, .net, .biz, .org and .info - these can be registered by anyone, anywhere in the world.

IDN ccTLD - internationalised country code top-level domains

A top-level name with a specially encoded format that allows it to be displayed in a non-Latin character set (i.e. special characters).

Subdomain: Part of a higher ranked domain name in DNS hierarchy; e.g. **admissions**.knust.edu.gh.

IP Addresses and Domain Names

The Internet relies on an addressing system much like the postal service to send data to a computer or device at a specific destination. An **IP address**, short for Internet Protocol address, is a sequence of numbers that uniquely identifies the location of each computer or device connected to the Internet.

The Internet uses two IP addressing schemes: IPv4 and IPv6. Due to the growth of the Internet, the original IPv4 addresses began dwindling in availability. The IPv6 scheme increased the available number of IP addresses exponentially. Because lengthy IP addresses can be difficult to remember, the Internet supports domain names. A **domain name** is a text-based name that corresponds to the IP address of a server that hosts a website. A domain name is part of the web address that you type in a browser's address bar to access a website.

The organization that approves and controls TLDs is called ICANN (pronounced EYE-can), which stands for **Internet Corporation for Assigned Names and Numbers**.

TLD	**Intended Purpose**
.com	Commercial organizations, businesses, and companies
.edu	Educational institutions
.gov	Government agencies
.mil	Military organizations
.net	Network providers or commercial companies
.org	Nonprofit organizations

2.7 Netiquette

Netiquette is the code of acceptable behaviours users should follow while on the internet. Netiquette is short for **Internet Etiquette**. It includes rules for all aspects of the internet, such as the World Wide Web, e-mail, instant messaging, chat rooms and newsgroups. Some common codes are:

i. Don't repost or forward media content without checking the authenticity of the information and the source.
ii. Check and respond to emails promptly
iii. Update relevant information that people rely upon for decision making
iv. Be polite and avoid offensive language
v. Be careful when using sarcasm or humor as it may be misinterpreted.

UNIT 3: APPLICATION SOFTWARE

3.1 Unit Objectives

After completing this unit, you will be able to:

1. Define software
2. differentiate between system software and application software
3. Identify the general categories of programs and apps
4. Describe how an operating system interacts with applications and hardware
5. Differentiate among the ways you can acquire programs and apps
6. Identify the key features of productivity applications
7. Identify the key features of security tools: personal firewall, antivirus programs, malware removers, and Internet filters

3.1 Application Software

Using programs and apps, you can accomplish a variety of tasks on computers and mobile Devices. a **program**, or **software**, consists of a series of related instructions, organized for a common purpose, that tells the computer what tasks to perform and how to perform them. An **application**, or **app**, sometimes called application software, consists of programs designed to make users more productive and/or assist them with personal tasks.

An operating system is a set of programs that coordinates all the activities among computer or mobile device hardware. Other programs, often called tools or utilities, enable you to perform maintenance-type tasks usually related to managing devices, media, and programs used by computers and mobile devices. The operating system and other tools are collectively known as **system software** because they consist of the programs that control or maintain the operations of the computer and its devices.

Role of the Operating System

To use applications, such as a browser or word processing program on a desktop or laptop, your computer must be running an operating system. Similarly, a mobile device must be running an operating system to run a mobile app, such as a navigation or payment app. Desktop operating systems include Mac OS, Windows, Linux, and Chrome OS. Mobile operating systems include Android, iOS, and Windows Phone. The operating system, therefore, serves as the interface between the user, the applications and other programs, and the computer's or mobile device's hardware. Each time you start a computer or mobile device, the operating system is loaded (copied) from the computer's hard drive or mobile device's storage media into memory. Once the operating system is loaded, it coordinates all the activities of the computer or mobile device. This includes running applications and transferring data among input and output devices and memory. While the computer or mobile device is running, the operating system remains in memory.

Obtaining Software

Software is available in a variety of forms: retail, custom, web app, mobile app, mobile web app, shareware, freeware, open source, and public domain.

- **Retail software** is mass-produced, copyrighted software that meets the needs of a wide variety of users, not just a single user or company. Some retail software, such as an operating system, is preinstalled on new computers and mobile devices. You also can purchase retail software from local stores and on the web. With online purchases, you may be able to download purchased programs immediately instead of waiting for the software to arrive by mail.
- **Custom software** performs functions specific to a business or industry. Sometimes a company cannot locate retail software that meets its unique requirements. In this case, the company may use software developers to create tailor-made custom software. Custom software usually costs more than retail software.
- **A web app** is an application stored on a web server that you access through a browser. Users typically interact with web apps directly by visiting a website, but some web apps also can be accessed locally offline. Many websites provide free access to their apps. Some charge a onetime fee, while others charge recurring monthly or annual subscription fees. You may be able to use part of a web app free and pay for access to a more comprehensive program or pay a fee when a certain action occurs.
- **A mobile app** is an application you download from a mobile device's app store such as **playstore**, sometimes called a marketplace, or other location on the Internet to a smartphone or other mobile device. Some mobile apps are preinstalled on a new mobile computer or device. Many mobile apps are free; others have a minimal cost — often less than a few dollars.
- **Shareware** is copyrighted software that is distributed at no cost for a trial period. To use a shareware program beyond that period, you send payment to the software developer or you might be billed automatically unless you cancel within a specified period of time. Some developers trust users to send payment if software use extends beyond the stated trial period. Others render the software useless if no payment is received after the trial period expires. In some cases, a scaled-down version of the software is distributed free, and payment entitles the user to the fully functional product.
- **Freeware** is copyrighted software provided at no cost by an individual or a company that retains all rights to the software. Thus, software developers typically cannot incorporate freeware in applications they intend to sell. The word, free, in freeware indicates the software has no charge.
- **Open source software** is software provided for use, modification, and redistribution. This software has no restrictions from the copyright holder regarding modification of the software's internal instructions and its redistribution. Open source software usually can be downloaded from a web server on the Internet, often at no cost. Promoters of open source software state two main advantages: users who modify the software share their improvements with others, and customers can personalize the software to meet their needs.
- **Public-domain software** has been donated for public use and has no copyright restrictions. Anyone can copy or distribute public-domain software to others at no cost.

Categories of Programs and Apps

With programs and apps, you can work on a variety of projects — such as creating letters, memos, reports, and other documents; developing presentations; preparing and filing taxes; drawing and altering images; recording and enhancing audio and video clips; obtaining directions or maps; playing games individually or with others; composing email and other messages; protecting computers and mobile devices from malware; organizing media; locating files; and much more.

Category	Types of Programs and Apps
Productivity (Business and Personal)	❖ Word Processing ❖ Presentation ❖ Spreadsheet ❖ Database ❖ Note Taking ❖ Calendar and Contact Management ❖ Project Management ❖ Accounting ❖ Personal Finance ❖ Legal ❖ Tax Preparation ❖ Document Management ❖ Support Services ❖ Enterprise Computing
Graphics and Media	❖ Computer-Aided Design (CAD) ❖ Desktop Publishing ❖ Paint/Image Editing ❖ Photo Editing and Photo Management ❖ Clip Art/Image Gallery ❖ Video and Audio Editing ❖ Multimedia and Website Authoring ❖ Media Player ❖ Disc Burning
Personal Interest	❖ Lifestyle ❖ Medical ❖ Entertainment ❖ Convenience ❖ Education
Communications	❖ Blog ❖ Browser ❖ Chat Room ❖ Online Discussion ❖ Email ❖ File Transfer

	❖ Internet Phone
	❖ Internet Messaging
	❖ Mobile Messaging
	❖ Videoconference
	❖ Web feeds
Security	➨ Personal Firewall
	➨ Antivirus
	➨ Malware Removers
	➨ Internet Filters
File, Disk, and	❖ File Manager
System	❖ Search
Management	❖ Image Viewer
	❖ Uninstaller
	❖ Disk Cleanup
	❖ Disk Defragmenter
	❖ Screen Saver
	❖ File Compression
	❖ PC Maintenance
	❖ Backup and Restore

The Programs and apps listed in one category may be used in other categories. For example, photo editing applications, which appear in the graphics and media category, often also are used for business or personal productivity. Additionally, the programs and apps in the last three categories (communications; security; and file, disk, and system management) often are used in conjunction with or to support programs and apps in the first three categories (productivity, graphics and media, and personal interest). For example, email appears in the communications category but also is a productivity application.

3.2 Productivity Software

Productivity applications can assist you in becoming more effective and efficient while performing daily activities at work, school, and home. Productivity applications include word processing, presentation, spreadsheet, database, note taking, calendar and contact management, project management, accounting, personal finance, legal, tax preparation, document management, and enterprise computing. A variety of manufacturers offer productivity apps in each of these areas, ranging from desktop to mobile to web apps. Many have a desktop version and a corresponding mobile version adapted for smaller screen sizes and/or touch screens.

Word Processors

Word processing software, sometimes called a **word processor**, is an application that allows users to create and manipulate documents containing mostly text and sometimes graphics. Millions of people use word processing software on their computers and mobile devices every

day to develop documents such as letters, memos, reports, mailing labels, newsletters, and webpages. A major advantage of using word processing software is that it enables users to change their written words easily. Word processing software also has many features to make documents look professional and visually appealing. For example, you can change the font, size, and color of characters; apply special effects, such as three-dimensional shadows; use built-in styles to format documents; and organize text in newspaper-style columns.

Most word processing software allows users to incorporate graphics, such as digital photos and clip art, in documents. With word processing software, you easily can modify the appearance of an image after inserting it in the document. As you type more lines of text than can be displayed on the screen, the top portion of the document moves upward, or scrolls, off the screen. Word processing software typically includes tools to assist you with the writing process. For example, a spelling checker reviews the spelling of individual words, sections of a document, or the entire document. A grammar checker detects passive voice, run on sentences, and grammatical errors. A format checker identifies extraneous spaces, capitalization errors, and more.

Examples of word processes include: Microsoft Office Word, Notepad, Apple Pages (iWorks), and Google Docs.

Presentation software

Presentation software is an application that allows users to create visual aids for presentations to communicate ideas, messages, and other information to a group. The presentations can be viewed as **slides**, sometimes called a slide show, that are displayed on a large monitor or on a projection screen from a computer or mobile device. Presentation software typically provides a variety of predefined presentation formats that define complementary colors for backgrounds, text, and graphical accents on the slides. This software also provides a variety of layouts for each individual slide such as a title slide, a two-column slide, and a slide with clip art, a chart, a table, or a diagram. In addition, you can enhance any text, charts, and graphics on a slide with 3-D effects, animation, and other special effects, such as shading, shadows, and textures.

Presentation software typically includes a clip gallery that provides images, photos, video clips, and audio clips to enhance presentations. Some audio and video editing applications work with presentation software, providing users with an easy means to record and insert video, music, and audio commentary in a presentation. You can view or print a finished presentation in a variety of formats, including a hard copy outline of text from each slide and handouts that show completed slides. Presentation software also incorporates features such as checking spelling, formatting, researching, and creating webpages from existing slide shows.

Examples include: MS Powerpoint, Google slides, slide rocket, slide share and corel presentation.

Spreadsheet applications

Spreadsheet software is an application that allows users to organize data in **columns and rows** and perform **calculations** on the data. These columns and rows collectively are called a **worksheet**. Most spreadsheet software has basic features to help users create, edit, and format worksheets. A spreadsheet file also is known as a **workbook** because it can contain thousands of related individual worksheets. Data is organized vertically in columns and Horizontally in rows on each worksheet. Each worksheet usually can have thousands of columns and rows. One or more letters identify each column, and a number identifies each row. Only a small fraction of these columns and rows are visible on the screen at one time.

A cell is the intersection of a column and row. The spreadsheet software identifies cells by the column and row in which they are located. For example, the intersection of column B and row 4 is referred to as cell B4.

A formula performs calculations on the data in the worksheet and displays the resulting value in a cell, usually the cell containing the formula. When creating a worksheet, you can enter your own formulas. for example, =B9+B10+B11+B12+ B13+B14+B15+B16 is a formula which would add (sum) the contents of cells B9, B10, B11, B12, B13, B14, B15, and B16.

A function is a predefined formula that performs common calculations, such as adding the Values in a group of cells or generating a value such as the time or date. For example, =SUM(B9:B16) is a function which instructs the spreadsheet application to add all of the numbers in the range of cells B9 through B16. Spreadsheet applications contain many built-in functions. One of the more powerful features of spreadsheet software is its capability to recalculate the rest of the worksheet when data in a cell changes. Spreadsheet software's capability of recalculating data also makes it a valuable budgeting, forecasting, and decision-making tool. Another standard feature of spreadsheet software is charting, which depicts the data in graphical form, such as bar charts or pie charts. A visual representation of data through charts often makes it easier for users to see at a glance the relationship among the numbers.

Examples of Spreadsheet Applications include: Microsoft Excel, Lotus 1-2-3, iWork Numbers (Apple Numbers), Libre Office_Calc, Google sheets, and Visi Calc.

Software Suite

A **software suite** is a collection of individual related applications available together as a unit. Productivity software suites typically include, at a minimum, word processing, presentation, spreadsheet, and email applications. While several productivity suites are designed to be installed on a local computer, some are web apps and/or mobile web apps that enabling you to share and collaborate with projects stored on the cloud.

An example of a software suite is the Microsoft Office program. Ms Office suite several software units such as Microsoft Word, Excel, Access, Powerpoint, Publisher, and OneNote. Microsoft office has several version including Office 2003, Office 2007, Office 2010 and Office 2016.

3.3 Graphic and Media Software

In addition to productivity applications, many people work with software designed specifically for their field of work. Power users, such as engineers, architects, desktop publishers, and graphic artists, often use sophisticated software that allows them to work with graphics and media. Many of these applications incorporate user-friendly interfaces or scaled-down versions, making it possible for the home and small business users also to create projects using these types of programs.

Graphics and media applications include computer-aided design, desktop publishing, paint/ image editing, photo editing and photo management, video and audio editing, multimedia and website authoring, media players, and disc burning.

Computer-Aided Design

Computer-aided design (CAD) software is a type of application that assists professionals and designers in creating engineering, architectural, and scientific designs and models. For example, engineers create design plans for vehicles and security systems. Architects design building structures and floor plans. Scientists design drawings of molecular structures.
Three-dimensional CAD programs allow designers to rotate designs of **3-D** objects to view them from any angle. Some CAD software even can generate material lists for building designs. Home and small business users work with less sophisticated design and modeling software. These applications usually contain thousands of predrawn plans that users can customize to meet their needs. For example, home design/landscaping software is an application that assists users with the design, remodeling, or improvement of a home, deck, or landscape. Examples: AutoCAD, Microsoft Visio, CardCAD, LibreCAD, and CAD pro

Desktop Publishing

Desktop publishing software (DTP software) is an application that enables designers to Create sophisticated publications that contain text, graphics, and many colours. Professional DTP software is ideal for the production of high-quality colour projects such as textbooks, corporate newsletters, marketing literature, product catalogues, and annual reports. Designers and graphic artists can print finished publications on a colour printer, take them to a professional printer, or post them on the web in a format that can be viewed by those without DTP software. Home and small business users create newsletters, brochures, flyers, advertisements, postcards, greeting cards, letterhead, business cards, banners, calendars, logos, and webpages using personal DTP software.

Although many word processing programs include DTP features, home and small business users often prefer to create DTP projects using DTP software because of its enhanced features. These programs typically guide you through the development of a project by asking a series of questions. Then, you can print a finished publication on a colour printer or post it on the web. Many personal DTP programs also include paint/image editing software and photo editing and photo management software, enabling users to embellish their publications with images. Examples include: Ms Publisher and Corel Draw

Paint/Image Editing

Graphic artists, multimedia professionals, technical illustrators, and desktop publishers use paint software and image editing software to create and modify graphics, such as those used in DTP projects and webpages. **Paint software**, also called illustration software, is an application that allows users to draw pictures, shapes, and other graphics with various on-screen tools, such as a pen, brush, eyedropper, and paint bucket.

Image editing software is an application that provides the capabilities of paint software and also includes the capability to enhance and modify existing photos and images. Modifications can include adjusting or enhancing image colors, adding special effects such as shadows and glows, creating animations, and image stitching (combining multiple images into a larger image). Paint/image editing software for the home or small business user provides an easy-to-use interface; includes various simplified tools that allow you to draw pictures, shapes, and other images; and provides the capability of modifying existing graphics and photos. These products also include many templates to assist you in adding images to projects, such as greeting cards, banners, calendars, signs, labels, business cards, and letterhead. Examples are Corel Draw, Photoshop, Ms Paint, and Illustrator

Video and Audio Editing

Video editing software is an application that allows professionals to modify a segment of a video, called a clip. For example, users can reduce the length of a video clip, reorder a series of clips, or add special effects such as words that move across the screen. Video editing software typically includes audio editing capabilities.

Audio editing software is an application that enables users to modify audio clips, produce studio-quality soundtracks, and add audio to video clips. Most television shows and movies are created or enhanced using video and audio editing software. Many home users work with easy-to-use video and audio editing software, which is much simpler to use than its professional counterpart, for small-scale movie making projects.

UNIT 4: THE COMPONENTS OF THE SYSTEM UNIT

4.1 Unit Objectives

After completing this unit, you will be able to:

1. Describe multi-core processors, the components of a processor, and the four steps in a machine cycle
2. Identify characteristics of various personal computer processors on the market today, and describe the ways processors are cooled
3. Define a bit, and describe how a series of bits represents data
4. Explain how program and application instructions transfer in and out of memory
5. Differentiate among the various types of memory: RAM, cache, ROM, flash memory, and CMOS
6. Describe the purpose of adapter cards and USB adapters
7. Explain the function of a bus
8. Explain the purpose of a power supply and batteries
9. Describe how to care for computers and mobile devices

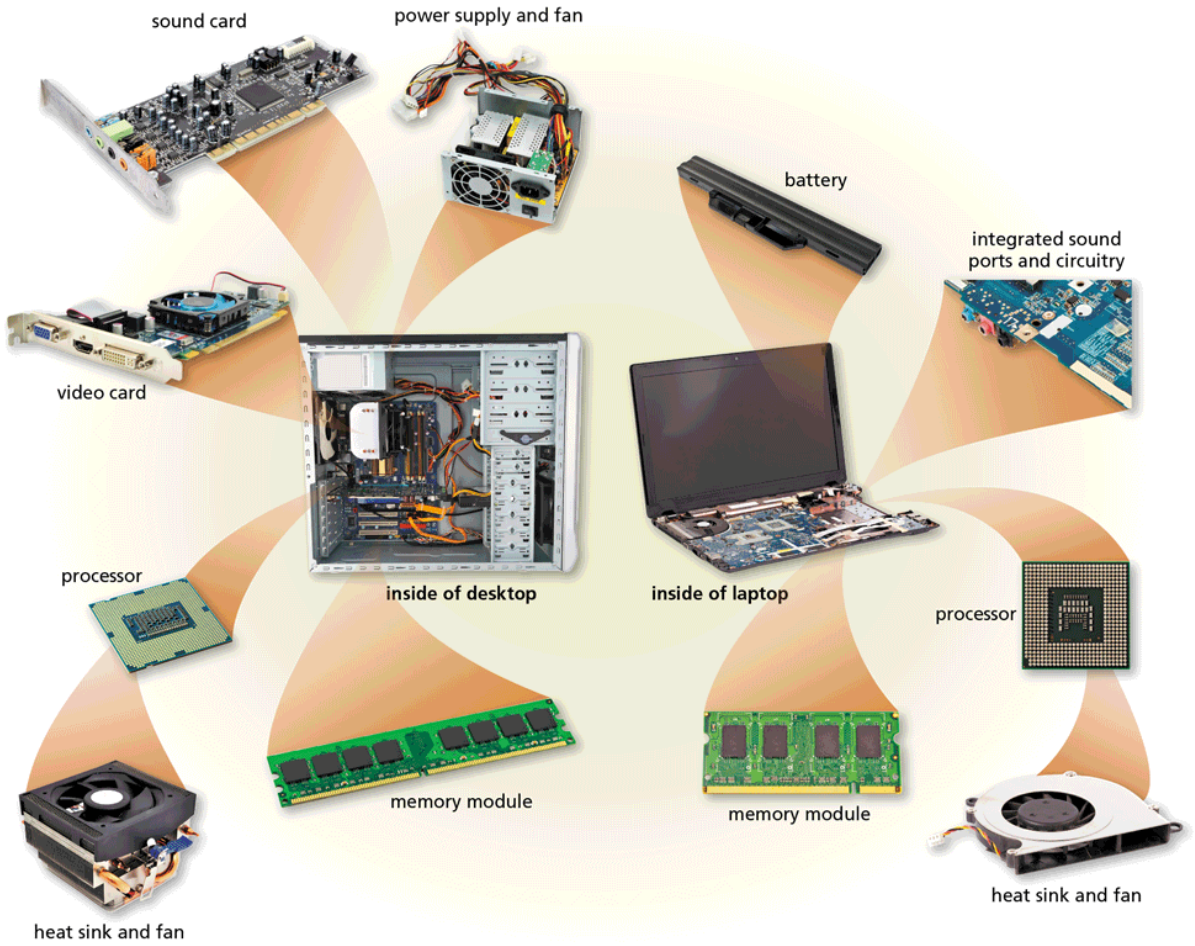
4.2 System Unit

Whether you are a home user or a business user, you most likely will purchase a new computer or mobile device, or upgrade an existing computer at some time in the future. Thus, you should understand the purpose of each component in a computer or mobile device. computers devices include components that are used for input, processing, output, storage, and communications. Many of these components are inside the case that contains and protects the electronics of the computer or mobile device from damage. These cases, which are made of metal or plastic, are available in a variety of shapes and sizes.

- **system unit (or chassis),** refers to the case on a desktop that contains and protects the motherboard, hard drive, memory, and other electronic components. Some desktops have a tower system unit that is a device separate from the monitor. Others that house the display and the system unit in the same case are called an all-in-one. Peripheral devices normally occupy space outside the system unit and communicate with the system unit using wired or wireless technology.
- On most laptops, including **ultrathin laptops**, the keyboard and pointing device often occupy the area on top of the case, and the display attaches to the case by hinges.
- With a slate tablet, which typically does not include a physical keyboard, the case is behind the display. Keyboard options for slate tablets include an on-screen keyboard, a wireless keyboard, or a keyboard that attaches to the slate via a clip, magnets, or other mechanism. On a **convertible tablet**, by contrast, the case is positioned below a keyboard, providing functionality similar to a laptop. The difference is that the display attaches to the case with a swivel-type hinge, enabling the user to rotate the display and fold it down over the keyboard to look like a slate tablet.
- With game consoles, the input and output devices, such as controllers and a television, reside outside the case.
- Like a slate tablet, the case on a smartphone often is behind the display.

❖ The case on **wearable devices**, portable media players, digital cameras, and handheld game devices typically consumes the entire device and houses the display and input devices.

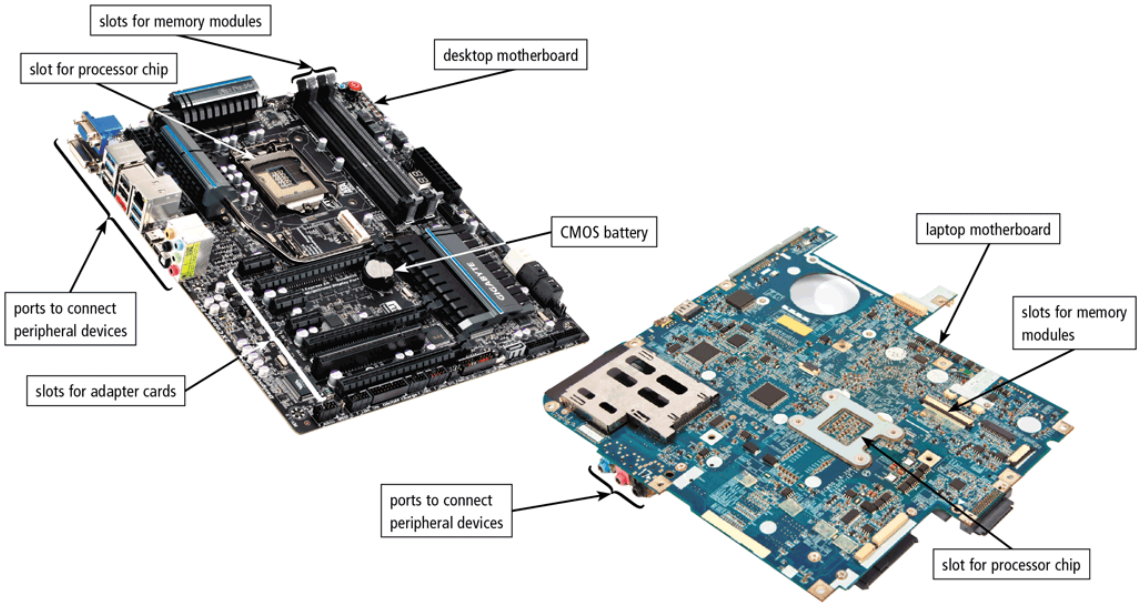
Below are some electronic components inside the computer case:



The Motherboard

The **motherboard**, sometimes called a **system board**, is the main circuit board of the computer. Many electronic components, such as the processor and memory, attach to the motherboard; others are built into it. On personal computers, the circuitry for the processor, memory, and other components reside on a computer chip(s). A computer **chip** is a small piece of semiconducting material, usually silicon, on which integrated circuits are etched. An integrated circuit contains many microscopic pathways capable of carrying electrical current. Each integrated circuit can contain millions of elements such as resistors, capacitors, and transistors. A transistor, for example, can act as an electronic switch that opens or closes the circuit for electrical charges. Today's computer chips contain millions or billions of transistors. Most chips are no bigger than one-half-inch square. Manufacturers package chips so that the chips can be attached to a circuit board, such as a motherboard.

The figure below shows desktop motherboard and a laptop motherboard.



Processors

The **processor**, also called the **central processing unit** (**CPU**), interprets and carries out the basic instructions that operate a computer. The processor significantly impacts overall computing power and manages most of a computer's operations. On larger computers, such as mainframes and supercomputers, the various functions performed by the processor extend over many separate chips and often multiple circuit boards. On a personal computer, all functions of the processor usually are on a single chip. Some computer and chip manufacturers use the term **microprocessor** to refer to a personal computer processor chip.

Most processor chip manufacturers now offer **multi-core processors**. A processor core, or simply core, contains the circuitry necessary to execute instructions. The operating system views each processor core as a separate processor. A **multi-core processor** is a single chip with two or more separate processor cores. Multi-core processors are used in all sizes of computers.

Are multi-core processors better than single-core processors?

Each processor core on a multi-core processor generally runs at a slower speed than a single-core processor, but multi-core processors typically increase overall performance. For example, although a dual-core processor does not double the processing speed of a single-core processor, it can approach those speeds. The performance increase is especially noticeable when users are running multiple programs simultaneously, such as antivirus software, spyware remover, email program, Internet messaging, media player, and photo editing software. Multi-core processors also are more energy efficient than separate multiple processors, requiring lower levels of power consumption and emitting less heat inside the case.

Processors contain a **control unit** and **an arithmetic logic unit (ALU)**. These two components work together to perform processing operations. When a user runs an application, for example, its instructions transfer from a storage device to memory. Data needed by programs and applications enters memory from either an input device or a storage device. The control unit interprets and executes instructions in memory, and the arithmetic logic unit performs

calculations on the data in memory. Resulting information is stored in memory, from which it can be sent to an output device or a storage device for future access, as needed.

The Control Unit

The **control unit** is the component of the processor that directs and coordinates most of the operations in the computer. That is, it interprets each instruction issued by a program or an application and then initiates the appropriate action to carry out the instruction. Types of internal components that the control unit directs include the arithmetic logic unit, registers, and buses.

The Arithmetic Logic Unit

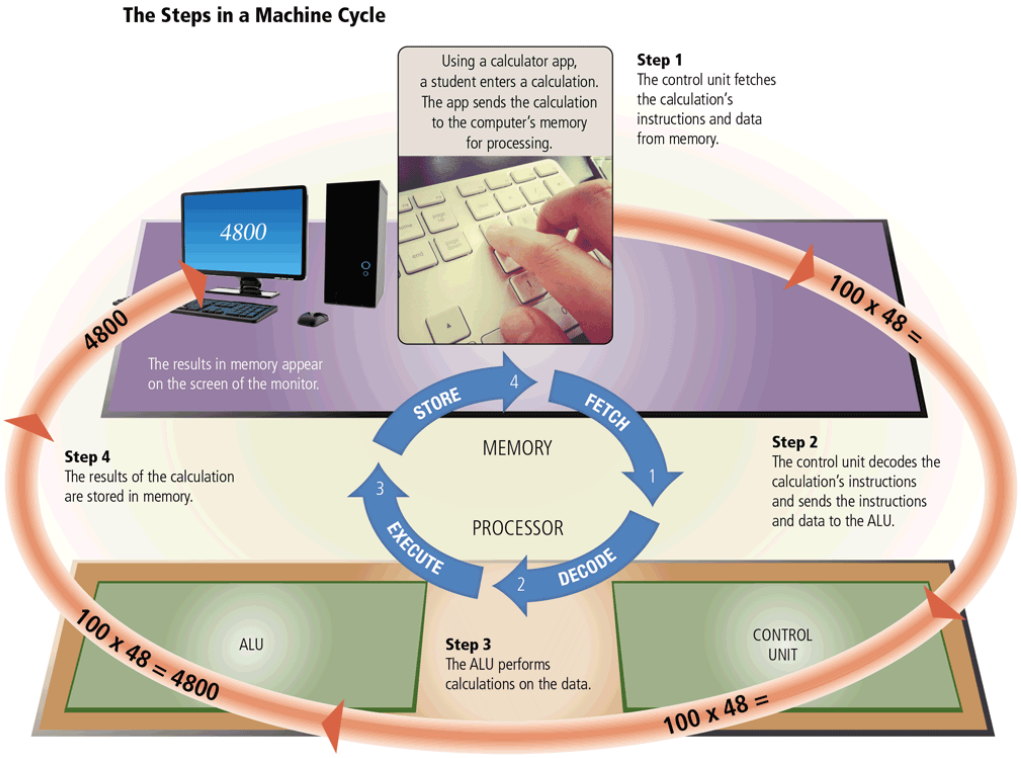
The **arithmetic logic unit** (ALU), another component of the processor, performs arithmetic, comparison, and other operations. Arithmetic operations include basic calculations, such as addition, subtraction, multiplication, and division. Comparison operations involve comparing one data item with another to determine whether the first item is greater than, equal to, or less than the other item. Depending on the result of the comparison, different actions may occur. For example, to determine if an employee should receive overtime pay, software instructs the ALU to compare the number of hours an employee worked during the week with the regular time hours allowed (e.g., 40 hours). If the hours worked exceed 40, for example, software instructs the ALU to perform calculations that compute the overtime wage.

Machine Cycle

For every instruction, a processor repeats a set of four basic operations, which comprise a machine cycle: (1) fetching, (2) decoding, (3) executing, and, if necessary, (4) storing.

- Fetching is the process of obtaining a program or an application instruction or data item from memory.
- Decoding refers to the process of translating the instruction into signals the computer can execute.
- Executing is the process of carrying out the commands.
- Storing, in this context, means writing the result to memory (not to a storage medium).

In some computers, the processor fetches, decodes, executes, and stores only one instruction at a time. With others, the processor fetches a second instruction before the first instruction completes its machine cycle, resulting in faster processing. Some use multiple processors simultaneously to increase processing times.



Registers

A processor contains small, high-speed storage locations, called registers, that temporarily hold data and instructions. Registers are part of the processor, not part of memory or a permanent storage device. Processors have many different types of registers, each with a specific storage function. Register functions include storing the location from where an instruction was fetched, storing an instruction while the control unit decodes it, storing data while the ALU calculates it, and storing the results of a calculation.

The System Clock

The processor relies on a small quartz crystal circuit called the **system clock** to control the timing of all computer operations. Just as your heart beats at a regular rate to keep your body functioning, the system clock generates regular electronic pulses, or ticks, that set the operating pace of components of the system unit. Each tick equates to a clock cycle. Processors today typically are **superscalar**, which means they can execute more than one instruction per clock cycle.

The pace of the system clock, called the **clock speed**, is measured by the number of ticks per second. Current personal computer processors have clock speeds in the gigahertz range. Giga is a prefix that stands for billion, and a hertz is one cycle per second. Thus, one **gigahertz (GHz)** equals one billion ticks of the system clock per second. A computer that operates at 3 GHz has 3 billion (giga) clock cycles in one second (hertz). The faster the clock speed, the more instructions the processor can execute per second. The speed of the system clock is just one factor that influences a computer's performance. Other factors, such as the type of processor chip, amount of cache, memory access time, bus width, and bus clock speed, are discussed later in this unit.

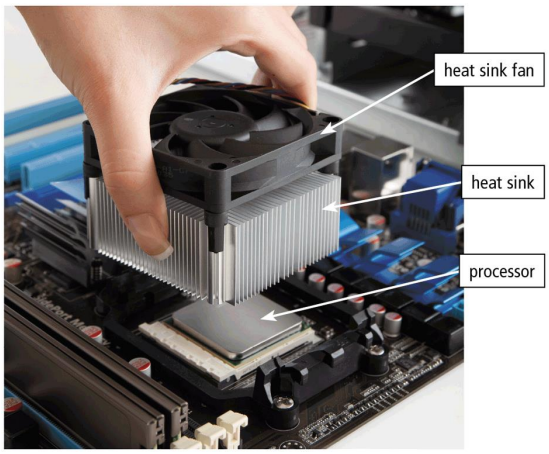
Personal Computer and Mobile Device Processors

The leading manufacturers of personal computer processor chips are **Intel and AMD**. AMD manufactures Intel-compatible processors, which have an internal design similar to Intel processors, perform the same functions, and can be as powerful, but often are less expensive. These manufacturers often identify their processor chips by a model name or model number.

In the past, chip manufacturers listed a processor's clock speed in marketing literature and advertisements. As previously mentioned, though, clock speed is only one factor that impacts processing speed in today's computers. To help consumers evaluate various processors, manufacturers such as Intel and AMD now use a numbering scheme that more accurately reflects the processing speed of their chips.

Processor Cooling

Processor chips for laptops, desktops, and servers can generate quite a bit of heat, which could cause the chip to malfunction or fail. Although the power supply on some computers contains a main fan to generate airflow, today's personal computer processors often require additional cooling. Some computer cases locate additional fans near certain components, such as a processor, to provide additional cooling. Heat sinks, liquid cooling technologies, and cooling mats often are used to help further dissipate processor heat.



A heat sink is a small ceramic or metal component with fins on its surface that absorbs and disperses heat produced by electrical components, such as a processor. Many heat sinks have fans to help distribute air dissipated by the heat sink. Some heat sinks are packaged as part of a processor chip. Others are installed on the top or the side of the chip

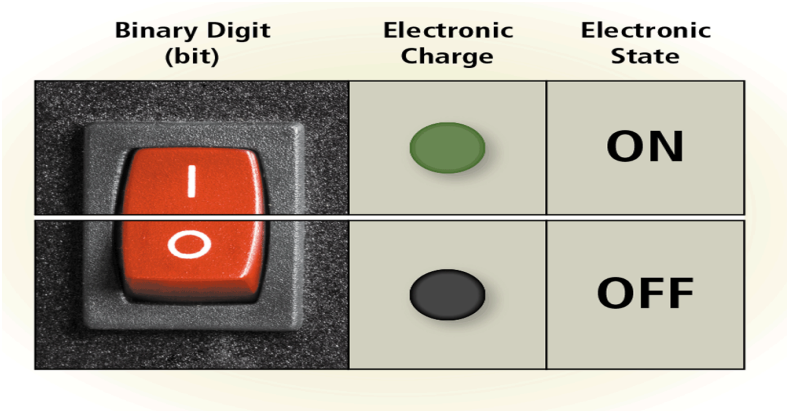
Some computers use liquid cooling technology to reduce the temperature of a processor. Liquid cooling technology uses a continuous flow of fluid(s), such as water and glycol, in a process that transfers the heated fluid away from the processor to a radiator-type grill, which cools the

liquid, and then returns the cooled fluid to the processor. Laptop users often use a **cooling pad** to help further reduce the heat generated by their computer.

A cooling pad rests below a laptop and protects the computer from overheating and also the user's lap from excessive heat. Some cooling pads contain a small fan to transfer heat away from the laptop. These types of cooling pads often draw power from a USB port. Instead of using power, other pads absorb heat through a conductive material inside the pad.

Data Representation

To understand how a computer processes data, you should know how a computer represents data. People communicate through speech by combining words into sentences. Human speech is **analogue** because it uses continuous (wave form) signals that vary in strength and quality. Most computers are **digital**. They recognize only two discrete states: on and off. This is because computers are electronic devices powered by electricity, which also has only two states: on and off.



Bits and Bytes

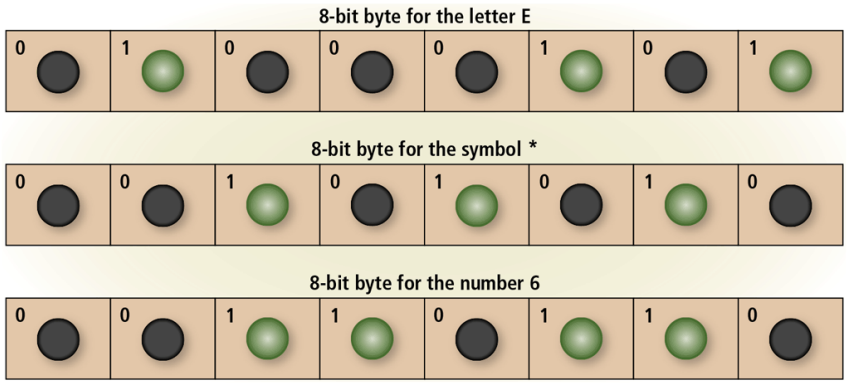
The two digits, 0 and 1, easily can represent these two states. The digit 0 represents the electronic state of off (absence of an electronic charge). The digit 1 represents the electronic state of on (presence of an electronic charge). When people count, they use the 10 digits in the decimal system (0 through 9). The computer, by contrast, uses a binary system because it recognizes only two states. The **binary system** is a number system that has just two unique digits, 0 and 1, called bits. A **bit** (short for binary digit) is the smallest unit of data the computer can process. By itself, a bit is not very informative. When 8 bits are grouped together as a unit, they form a **byte**. A byte provides enough different combinations of 0s and 1s to represent 256 different characters. These characters include numbers, uppercase and lowercase letters of the alphabet, punctuation marks, and other keyboard symbols, such as an asterisk (*), ampersand (&), and dollar sign ($).

Coding Schemes

The combinations of 0s and 1s that represent uppercase and lowercase letters, numbers, and special symbols are defined by patterns called a coding scheme. Coding schemes map a set of alphanumeric characters (letters and numbers) and special symbols to a sequence of numeric values that a computer can process. **ASCII** (pronounced ASK-ee), which stands for **American Standard Code for Information Interchange**, is the most widely used coding scheme to represent a set of characters. In the ASCII coding scheme, for example, the alphabetic character

E is represented as 01000101; the symbolic character * is represented as 00101010; the numeric character 6 is represented as 00110110

When you press a key on a keyboard, a chip in the keyboard converts the key's electronic signal into a special code, called a **scan code**, that is sent to the electronic circuitry in the computer. Then, the electronic circuitry in the computer converts the scan code into its ASCII binary form and stores it as a byte value in its memory for processing. When processing is finished, the computer converts the byte into a human-recognizable number, letter of the alphabet, or special character that is displayed on a screen or is printed. All of these conversions take place so quickly that you do not realize they are occurring.



Why are coding schemes necessary?

Computers rely on logic circuits, which are controlled by electronic switches whose state can be either on or off. Each switch's on/off state is represented by one bit, whose value is either 0 or 1. Coding schemes translate real-world data into a form that computers can process easily.

Memory

Memory consists of electronic components that store instructions waiting to be executed by the processor, data needed by those instructions, and the results of processing the data (information). Memory usually consists of one or more chips on the motherboard or some other circuit board in the computer. Memory stores three basic categories of items:

1. The operating system and other programs that control or maintain the computer and its devices.
2. Applications that carry out a specific task, such as word processing.
3. The data being processed by the applications and the resulting information

This role of memory to store both data and programs is known as the **stored program concept**.

Bytes and Addressable Memory

A byte (character) is the basic storage unit in memory. When an application's instructions and data are transferred to memory from storage devices, the instructions and data exist as bytes. Each byte resides temporarily in a location in memory that has an address. Simply put, an address is a unique number that identifies the location of a byte in memory. To access data or instructions in memory, the computer references the addresses that contain bytes of data.

Manufacturers state the size of memory in terms of the number of bytes it has available for storage. Common sizes for memory are in the gigabyte and terabyte range. A gigabyte (GB) equals approximately 1 billion bytes. A terabyte (TB) is equal to approximately 1 trillion bytes.

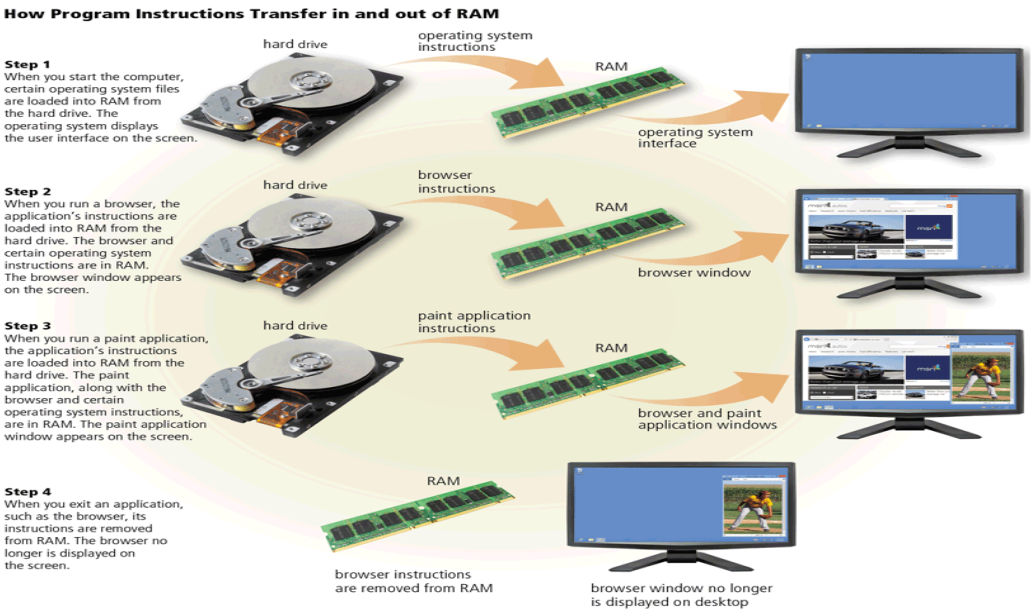
Types of Memory

Computers and mobile devices contain two types of memory: volatile and nonvolatile. When the computer's power is turned off, volatile memory loses its contents. Nonvolatile memory, by contrast, does not lose its contents when power is removed from the computer. Thus, volatile memory is temporary and nonvolatile memory is permanent. RAM is the most common type of volatile memory. Examples of nonvolatile memory include ROM, flash memory, and CMOS. The following sections discuss these types of memory.

RAM

Users typically are referring to RAM when discussing computer and mobile device memory. **RAM** (random access memory), also called main memory, consists of memory chips that can be read from and written to by the processor and other devices. When you turn on power to a computer or mobile device, certain operating system files (such as the files that determine how the desktop or home screen appears) load into RAM from a storage device such as a hard drive. These files remain in RAM as long as the computer or mobile device has continuous power. As additional applications and data are requested, they also load into RAM from storage.

The processor interprets and executes a program or application's instructions while the program or application is in RAM. During this time, the contents of RAM may change. RAM can accommodate multiple programs and applications simultaneously. Most RAM is volatile, which means it loses its contents when the power is removed from the computer. For this reason, you must save any data, instructions, and information you may need in the future. **Saving is the process of copying data, instructions, and information from RAM to a storage device such as a hard drive**.



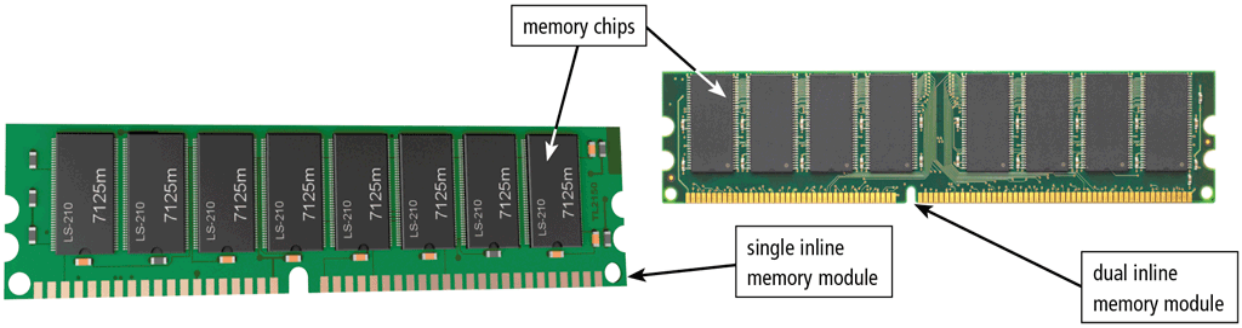
Types of RAM

Two common types of RAM are dynamic RAM and static RAM:

- Dynamic RAM (DRAM pronounced DEE-ram) chips must be reenergized constantly or they lose their contents. Many variations of DRAM chips exist, most of which are faster than the basic DRAM.
- Static RAM (SRAM pronounced ESS-ram) chips are faster and more reliable than any variation of DRAM chips. These chips do not have to be reenergized as often as DRAM chips; hence, the term, static. SRAM chips, however, are much more expensive than DRAM chips. Special applications, such as cache, use SRAM chips.

Memory Modules

RAM chips usually reside on a memory module, which is a small circuit board. Memory slots on the motherboard hold memory modules. Two types of memory modules are SIMMs and DIMMs. A SIMM (single inline memory module) has pins on opposite sides of the circuit board that connect together to form a single set of contacts. With a DIMM (dual inline memory module), by contrast, the pins on opposite sides of the circuit board do not connect and, thus, form two sets of contacts.



Cache

Most of today's computers improve their processing times with **cache** (pronounced cash), which is a temporary storage area. Two common types of cache are **memory cache and disk cache**.

Memory cache helps speed the processes of the computer because it stores frequently used instructions and data. Most personal computers today have two types of memory cache: Level 1 (L1) cache and Level 2 (L2) cache. Some also have Level 3 (L3) cache.

- L1 cache is built directly on the processor chip. L1 cache usually has a very small capacity.
- L2 cache is slightly slower than L1 cache but has a much larger capacity. Current processors include **Advanced Transfer Cache (ATC)**, a type of L2 cache built directly on the processor chip. Processors that use ATC perform at much faster rates than those that do not use it.
- L3 cache is a cache on the motherboard that is separate from the processor chip. L3 cache exists only on computers that use L2 advanced transfer cache.

When the processor needs an instruction or data, it searches memory in this order: L1 cache, then L2 cache, then L3 cache (if it exists), then RAM — with a greater delay in processing for each level of memory it must search. If the instruction or data is not found in memory, then it must search a slower speed storage medium, such as a hard drive or optical disc.

ROM

Read-only memory (**ROM** pronounced rahm) refers to memory chips storing permanent data and instructions. The data on most ROM chips cannot be modified — hence, the name read-only. ROM is nonvolatile, which means its contents are not lost when power is removed from the computer. In addition to computers and mobile devices, many peripheral devices contain ROM chips. For example, ROM chips in printers contain data for fonts.

Manufacturers of ROM chips often record data, instructions, or information on the chips when they manufacture the chips. These ROM chips, called **firmware**, contain permanently written data, instructions, or information, such as a computer or mobile device's start-up instructions.

Flash Memory

Flash memory is a type of nonvolatile memory that can be erased electronically and rewritten. Most computers use flash memory to hold their start-up instructions because it allows the computer to update its contents easily. For example, when the computer changes from standard time to daylight savings time, the contents of a flash memory chip (and the real-time clock chip) change to reflect the new time. Flash memory chips also store data and programs on many mobile devices and peripheral devices, such as smartphones, portable media players, printers, digital cameras, automotive devices, and digital voice recorders. When you enter names and addresses in a smartphone, for example, a flash memory chip stores the data. Some portable media players store music on flash memory chips; others store music on tiny hard drives or memory cards. Memory cards contain flash memory on a removable device instead of a chip.

CMOS

Some RAM chips, flash memory chips, and other memory chips use **Complementary Metal-Oxide Semiconductor** (CMOS pronounced SEE-moss) technology because it provides high speeds and consumes little power. CMOS technology uses battery power to retain information even when the power to the computer is off. Battery-backed CMOS memory chips, for example, can keep the calendar, date, and time current even when the computer is off. The flash memory chips that store a computer's start-up information often use CMOS technology.

Memory Access Times

Access time is the amount of time it takes the processor to read data, instructions, and Information from memory. A computer's access time directly affects how fast the computer Processes data. For example, accessing data in memory can be more than 200,000 times faster than accessing data on a hard disk because of the mechanical motion of the hard disk. Some use fractions of a second, which for memory occurs in nanoseconds. A nanosecond

(abbreviated ns) is one billionth of a second. A nanosecond is extremely fast. In fact, electricity travels about one foot in a nanosecond.

Adapters

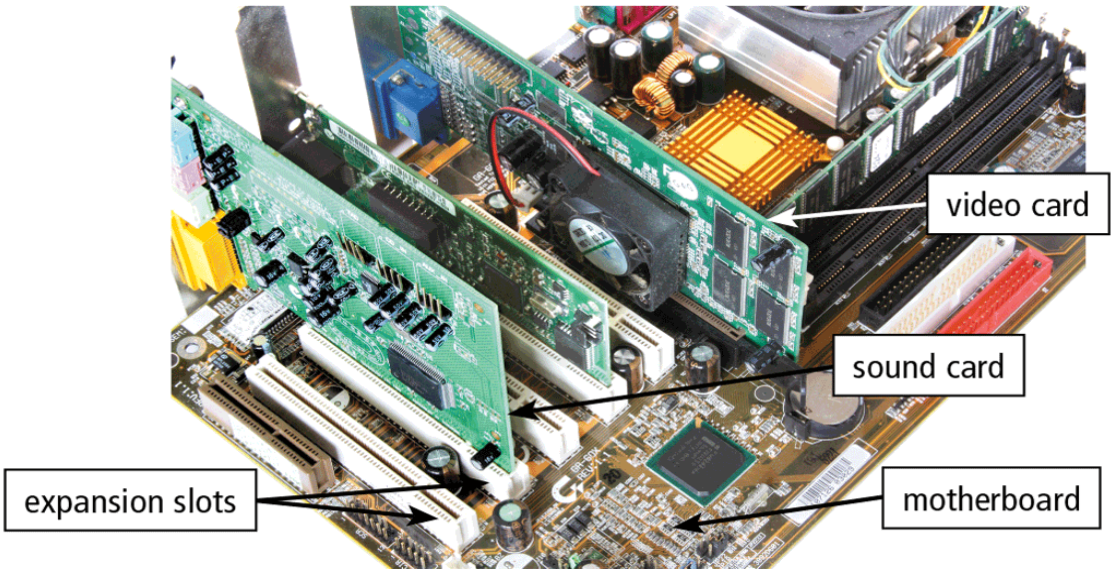
Although the circuitry in many of today's computers integrates all the necessary unctionality, some require additional capabilities in the form of adapters. Desktops and servers use adapter cards; mobile computers use USB adapters.

Adapter Cards

An **adapter card**, sometimes called an expansion card or adapter board, is a circuit board that enhances the functions of a component of a desktop or server system unit and/or provides connections to peripheral devices. An **expansion slot** is a socket on a desktop or server motherboard that can hold an adapter card.

Two popular adapter cards are sound cards and video cards. A sound card enhances the sound-generating capabilities of a personal computer by allowing sound to be input through a microphone and output through external speakers or headphones. A video card, also called a graphics card, converts computer output into a video signal that travels through a cable to the monitor, which displays an image on the screen. Sometimes, all functionality is built in the adapter card. With others, a cable connects the adapter card to a device, such as a digital video camera, outside the computer.

Today's computers support **Plug and Play** technology, which means the computer automatically can recognize peripheral devices as you install them. Plug and Play support means you can plug in a device and then immediately begin using it. The figure below shows expansion slots and adapters cards.



USB Adapters

Because of their smaller size, mobile computers typically do not have expansion slots. Instead, users can purchase a **USB adapter**, which is a dongle that plugs into a USB port, enhances functions of a mobile computer, and/or provides connections to peripheral devices.

USB adapters can be used to add memory, communications, multimedia, security, and storage capabilities to mobile computers. A USB flash drive is a common USB adapter that provides computers and mobile devices with additional storage capability as long as it is plugged in.

Unlike adapter cards that require you to open the system unit and install the card on the motherboard, you can change a removable flash memory device without having to open the system unit or restart the computer. This feature, called **hot plugging**, allows you to insert and remove a device while the computer is running (be sure, though, to stop or eject the device before removing it).

Buses

As explained earlier in this unit, a computer processes and stores data as a series of electronic bits. These bits transfer internally within the circuitry of the computer along electrical channels. Each channel, called a **bus**, allows the various devices both inside and attached to the system unit to communicate with one another. Just as vehicles travel on a highway to move from one destination to another, bits travel on a bus Buses are used to transfer bits from input devices to memory, from memory to the processor, from the processor to memory, and from memory to output or storage devices. Buses consist of a **data bus and an address bus**. The data bus is used to transfer actual data, and the address bus is used to transfer information about where the data should reside in memory.

Bus Width

The size of a bus, called the bus width, determines the number of bits that the computer can transmit at one time. For example, a 32-bit bus can transmit 32 bits (4 bytes) at a time. On a 64-bit bus, bits transmit from one location to another 64 bits (8 bytes) at a time. The larger the number of bits handled by the bus, the faster the computer transfers data. Using the highway analogy again, assume that one lane on a highway can carry one bit. A 32-bit bus is like a 32-lane highway. A 64-bit bus is like a 64-lane highway. If a number in memory occupies 8 bytes, or 64 bits, the computer must transmit it in two separate steps when using a 32-bit bus: once for the first 32 bits and once for the second 32 bits. Using a 64-bit bus, the computer can

transmit the number in a single step, transferring all 64 bits at once. The wider the bus, the fewer number of transfer steps required and the faster the transfer of data. Most personal computers today use a 64-bit bus. In conjunction with the bus width, many computer professionals refer to a computer's word size. **Word size** is the number of bits the processor can interpret and execute at a given time. That is, a 64-bit processor can manipulate 64 bits at a time. Computers with a larger word size can process more data in the same amount of time than computers with a smaller word size. In most computers, the word size is the same as the bus width.

Types of Buses

A computer has a system bus, possibly a backside bus, and an expansion bus.

- A system bus, also called the front side bus (FSB), is part of the motherboard and connects the processor to main memory.
- A backside bus (BSB) connects the processor to cache.
- An expansion bus allows the processor to communicate with peripheral devices. When computer professionals use the term, bus, by itself, they usually are referring to the system bus.

Power Supply and Batteries

Many personal computers plug in standard wall outlets, which supply an alternating current (AC) of 115 to 120 volts. This type of power is unsuitable for use with a computer or mobile device, which requires a direct current (DC) ranging from 5 to more than 15 volts. The **power supply** or laptop AC adapter converts the wall outlet AC power into DC power. Different motherboards and computers require different wattages on the power supply. If a power supply is not providing the necessary power, the computer will not function properly.

Built into the power supply is a fan that keeps the power supply cool. Some have variable speed fans that change speed or stop running, depending on temperature in the case. Many newer computers have additional fans near certain components in the system unit, such as the processor, hard drive, and ports. Some users install more fans to help dissipate heat generated by the components of the computer.

Some external peripheral devices, such as a cable modem, speakers, or a printer, have an AC adapter, which is an external power supply. One end of the AC adapter plugs in the wall outlet and the other end attaches to the peripheral. The AC adapter converts the AC power into the DC power that the peripheral requires, and also often charges the battery in a mobile computer or device.

Mobile computers and devices can run using either a power supply or batteries. The batteries typically are rechargeable lithium-ion batteries. Some mobile devices and computers, such as some ultrathin laptops, do not have removable batteries.

UNIT 5: INPUT DEVICES

5.1 Unit of Objectives

After completing this unit, you will be able to:

1. Differentiate among various types of keyboards: standard, compact, on-screen, virtual, ergonomic, gaming, and wireless
2. Describe characteristics of various pointing devices: mouse, touchpad, and trackball
3. Describe various uses of touch screens
4. Describe various types of pen input: stylus, digital pen, and graphics tablet
5. Describe various uses of motion input, voice input, and video input
6. Differentiate among various scanners and reading devices: optical scanners, optical readers, bar code readers, magstripe readers, MICR readers, and data collection devices

5.2 Definitions

Input is data, programs, commands and user responses entered into the main memory of the computer for processing. It is the act of entering data, programs or commands into the computer. People have a variety of options for entering data and instructions into a computer. **Data is a collection of unprocessed items, including text, numbers, images, audio, and video.** Once data is in memory, a computer or mobile device interprets and executes instructions to process the data into information. Instructions that a computer or mobile device processes can be in the form of software (programs and apps), commands, and user responses.

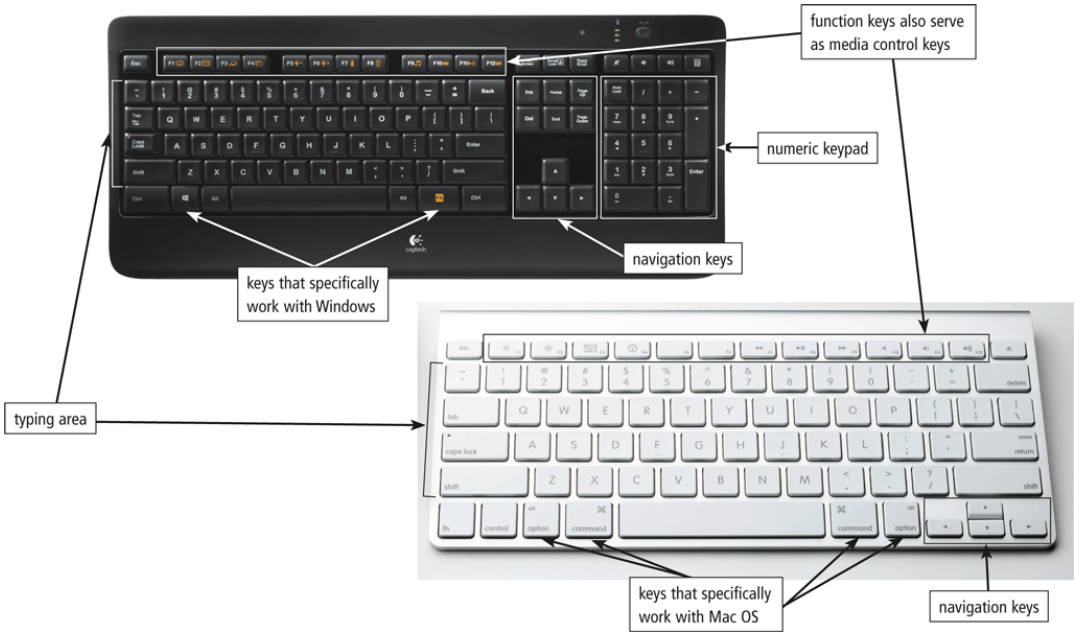
- **Software** is a series of related instructions, organized for a common purpose, that tells a computer or mobile device what tasks to perform and how to perform them. When software developers write programs or apps, they usually enter the instructions into the computer or mobile device by using a keyboard, mouse, or other input method. The software developer then stores the program in a file that a user can execute (run). When a user runs a program or app, the computer or mobile device loads the program or app from a storage medium into memory.
- **A command** is an instruction that causes a program or app to perform a specific action. Programs and apps respond to commands that a user issues. Users issue commands by touching an area on a screen, pressing keys on the keyboard, clicking a mouse button to control a pointer on the screen, or speaking into a microphone. A response to the message instructs the program or app to perform certain actions. For example, when a program or app asks the question, 'Do you want to save the changes made to this file?', and you respond with the instruction of 'Yes', the program will save the file with the changes you made. If you respond with the instruction of 'No', the program will not save your changes before exiting. Commonly used input methods include the keyboard, pointing devices, touch screens, pen input, motion input, voice input, video input, and scanners and reading devices. This chapter discusses each of these input methods.

5.3 Examples and Uses

Keyboards

Most computers and mobile devices include a keyboard or keyboarding capabilities. A **keyboard** is an input device that contains keys you press to enter data and instructions into a computer or mobile device. Nearly all keyboards have a typing area, function keys, toggle keys, and navigation keys. Many also include media control buttons, Internet control buttons, and other special keys. Others may include a fingerprint reader or a pointing device.

- The **typing area** includes letters of the alphabet, numbers, punctuation marks, and other basic keys.
- **Function keys**, which are labeled with the letter F followed by a number, are special keys programmed to issue commands to a computer. The command associated with a function key may vary, depending on the program you are using.
- A **toggle key** is a key that switches between two states each time a user presses the key. Caps lock and num lock are examples of toggle keys. Many mobile devices have keys that toggle the display of alphabetic, numeric, and symbols on touch keyboards in order to display more characters and symbols on a keyboard with fewer keys.
- Users can press the **navigation keys**, such as arrow keys and page up/pg up and page down/pg dn on the keyboard, to move the insertion point in an application left, right, up, or down.
- A keyboard shortcut is one or more keyboard keys that you press to perform an operating system or application-related task. Some keyboard shortcuts are unique to a particular application or operating system.
- **Media control buttons** allow you to control a media player program, access the computer's optical disc drive, and adjust speaker volume.
- **Internet control buttons** allow you to run an email application, run a browser, and search the web.



Types of Keyboards

Desktops include a **standard keyboard**. Standard keyboards typically have from 101 to 105 keys, which include function keys along the top and a numeric keypad on the right. The standard layout of letters, numbers and punctuations is known as a QWERTY keyboard because the first six keys on the top row letters spell QWERTY. The QWERT keyboard was designed in the 1800s for mechanical typewriters. The Dvorak Keyboard was designed in 1930 by August Dvorak to enhance typing speed.

You have a variety of keyboard options for mobile computers and devices. These devices often use a **compact keyboard**, which is smaller than a standard keyboard and usually does not include the numeric keypad or navigation keys. Typically, the keys on a compact keyboard serve two or three purposes in order to provide the same functionality as standard keyboards. Some compact keyboards are built into the computer or mobile device and/or are permanently attached with hinges, a sliding mechanism, or some other technique. Other compact keyboards are separate devices that communicate wirelessly or attach to the computer or device with a magnet, clip, or other mechanism. Some users prefer to work with on-screen or virtual keyboards instead of a physical keyboard. Others, however, prefer to use a standard keyboard with their mobile devices because these keyboards provide added functionality and tactile comfort.

An ergonomic keyboard has a design that reduces the chance of **repetitive strain injuries (RSIs)** of wrist and hand. Recall that the goal of ergonomics is to incorporate comfort, efficiency, and safety in the design of the workplace. Even

keyboards that are not ergonomically designed attempt to offer a user more comfort by including a wrist rest.

A **gaming keyboard** is a keyboard designed specifically for users who enjoy playing games on the computer. Gaming keyboards typically include programmable keys so that gamer scan customize the keyboard to the game being played. The keys on gaming keyboards light up so that the keys are visible in all lighting conditions. Some have small displays that show important game statistics, such as time or targets remaining.

Other types of the Keyboard

- **Multimedia Keyboard**

It is a type of keyboard, which includes multimedia buttons which help you to control your media only by a single tap. Usually, a multimedia keyboard includes additional buttons or keys like play, pause, stop, next, previous, volume up, volume down, mute and a special button to launch the default music player in your PC. You can also use these buttons for controlling video playback. A standard Multimedia keyboard contains these buttons also.

- **Mechanical keyboard**

This is somewhat a primitive type of keyboard but preferred by many. The mechanical keyboard uses real physical buttons below each key. When you press a key, the button pushes down. Then there occurs the completion of an electric circuit sending an electric signal to the PC, and you see the desired result on the monitor. That's how a mechanical keyboard works.

- **Wireless Keyboard**

It makes use of Radio Frequency, Bluetooth or Infra Red technology. Portability is the vital feature of these computer keyboards. We can use it away from the parental device. If you have strong Wi- Fi connection, you can type on your PC by sitting even 50 meters far from it. You can use this keyboard type with any of your gadgets like PC, mobile phone, tablet or laptop that supports wireless technology. Some wireless keyboards reduce the usage of a mouse by integrating a trackpad into it.

There must be two parts (apart from the keyboards) for this type of keyboard. A transmitter and a trans- receiver. The transmitter is attached to the keyboard itself and the receiver, to the parent device. Strokes from the keyboard are converted into radio waves and transmitted into the air using the transmitter. Trans- receiver attached to the PC or laptop senses these waves. Then, it gives the desired action.

- **Virtual Keyboard**

It is not a physical keyboard but allows us to input keys. The virtual keyboard is not a hardware but can be a software or parts of the software. This is the type of keyboard found on smartphone touchscreen for typing. We use our fingers to make inputs. There is no need to carry a physical object. Virtual keyboards appear for our needs and disappear after satisfying us.

- **USB Keyboard**

The invention of **Universal Serial Bus** (USB) was a massive leap in the history of computers. Today, we have USB keyboards, mouse, speakers, monitors and headphones also. This type of keyboard uses the USB interface as a way of connecting with the host. Means, we get a wire with a USB stick at the end with this keyboard. Just insert it into the USB port of your computer.

Earlier there were **PS2 keyboards**. PS2 was a particular type of port for mice and keyboards. You may face a major issue if you use a USB keyboard.

What is the rationale for the arrangement of keys in the typing area?

The keys originally were arranged on old mechanical typewriters to separate frequently used keys, which caused typists to slow down. This arrangement, called a QWERTY keyboard because the six first letters on the top row of letter keys spell QWERTY, reduced the frequency with which the mechanical levers jammed.

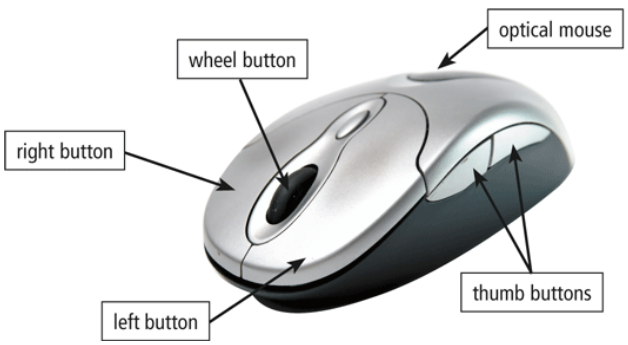
Pointing Devices

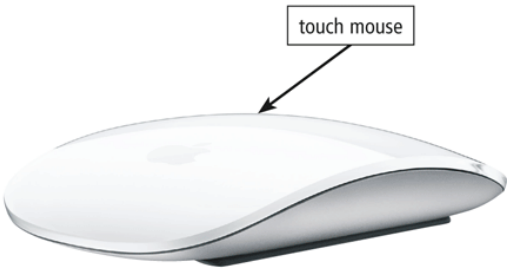
In a graphical user interface, a **pointer** is a small symbol on the screen whose location and shape change as a user moves a pointing device. A pointing device can enable you to select text, graphics, and other objects, such as buttons, icons, links, and menu commands. The following pages discuss a variety of pointing devices.

Mouse

A **mouse** is a pointing device that fits under the palm of your hand comfortably. As you move a mouse, the pointer on the screen also moves. The bottom of a mouse is flat and contains a mechanism that detects movement of the mouse. Desktop users have an optical mouse or a touch mouse, both of which can be placed on nearly all types of flat surfaces. An optical mouse uses optical sensors that emit and sense light to detect the mouse's movement.

Similarly, a laser mouse uses laser sensors that emit and sense light to detect the mouse's movement. Some mouse devices use a combination of both technologies. The top and sides of an optical or laser mouse may have one to four buttons; some may also have a small wheel. Some are more sensitive than others for users requiring more precision, such as graphic artists, engineers, or game players.





A **touch mouse** is a touch-sensitive mouse that recognizes touch gestures, in addition to detecting movement of the mouse and traditional click and scroll operations. For example, you press a location on a touch mouse to simulate a click, sweep your thumb on the mouse to scroll pages, or slide multiple fingers across the mouse to zoom. As with keyboards, you can purchase an ergonomic mouse to help reduce the chance of **RSIs** or to reduce pain and discomfort associated with RSIs.

Basic Mouse Operations

i. **Pointing** is to move the pointer to the desired spot on the screen
ii. **Click** is to press and release a mouse button once without moving the mouse. Clicking is used for selection and de-selection
iii. **Double click** is to press the left mouse button twice but quickly without moving the mouse. It is a means of selecting and activating a programme or program feature. For example to open a program.
iv. **Dragging** is to move the mouse while holding down the left mouse button so that an image or icon can be relocated.
v. **Drop** is to release of the mouse button after dragging
vi. is to bring up (pop up) a set of option (also called menu) by pressing the right button. This menu that pops up contains sensitive selection.

Touchpad

A **touchpad** is a small, flat, rectangular pointing device that is sensitive to pressure and motion. Touchpads are found most often on laptops and convertible tablets. Desktop users who prefer the convenience of a touchpad can purchase a separate touchpad, which usually communicates wirelessly with the computer. To move the pointer using a touchpad, slide your fingertip across the surface of the pad. Some touchpads have one or more buttons around the edge of the pad that work like mouse buttons; others have no buttons. On most touchpads, you also can tap the pad's surface to imitate mouse operations, such as clicking. Some touchpads also recognize touch gestures, such as swipe, pinch, and stretch motions.

Trackball

A **trackball** is a stationary pointing device with a ball on its top or side. The ball in most
trackballs is about the size of a Ping-Pong ball. Some devices, called a trackball mouse, combine the functionality of both a trackball and a mouse. To move the pointer using a trackball, you rotate the ball with your thumb, fingers, or the palm of your hand. In addition to the ball, a trackball usually has one or more buttons that work like mouse buttons.

For users who have limited desk space, a trackball is a good alternative to a mouse because the device is stationary. Keep in mind, however, that a trackball requires frequent cleaning because it picks up oils from fingers and dust from the environment.

Touch Screens

A **touch screen** is a touch-sensitive display. Touch screens are convenient because they do not require a separate device for input. Smartphones and tablets, and many laptops and all-in-ones computer offer touch screens. You can interact with a touch screen by touching areas of the screen with your finger or a stylus to make selections or to begin typing. Many touch screens also respond to gestures. A gesture is a motion you make on a touch screen with the tip of one or more fingers or your hand. For example, you can slide your finger to drag an object or pinch your fingers to zoom out. Touch screens that recognize multiple points of contact at the same time are known as **multi-touch**. Because gestures often require the use of multiple fingers (points of contact), touch screens that support gestures are multi-touch. Touch Input Devices that utilize touch input include monitors for desktops and screens on laptops and tablets, smartphones, wearable devices, portable media players, digital cameras, tablets, kiosks, and navigation systems.

Smartphones

Smartphones are becoming more functional, lighter weight, and now often do not include a physical keyboard. Touch input can help smartphone manufacturers achieve all these goals. The gestures you might perform on a smartphone that supports touch input include tapping to run an app, sliding or swiping to scroll, and pinching and stretching to zoom. The absence of a physical keyboard makes it more difficult to type without looking at the screen, so it is not advisable to use a smartphone when performing actions that require undivided attention, such as driving a car or walking.

Wearable Devices

Wearable devices, such as smartwatches, do not have room for a physical keyboard, so they mainly rely on touch input. The gestures you might perform on a wearable device include tapping to make a selection, and sliding or swiping to scroll through the various screens.

Portable Media Players

Portable media players widely use touch as the primary method of input so that the size of the screen on the device is maximized. That is, space on the device does not have to be dedicated

to other controls, such as buttons or click wheels. Users slide and swipe to browse their music libraries on their portable media players and then tap to select the song they want to play. While songs are playing, users can tap the screen to display controls so that they can pause or stop the song, navigate to another song, or adjust the volume.

Digital Cameras

As digital cameras start to include built-in features to browse through and edit photos without requiring a computer, touch input helps digital camera users perform these functions with greater accuracy. For example, you can perform gestures such as swiping left and right on the screen to browse your photos, tapping the screen to identify the area on which you wish to focus when taking a picture, pinching and stretching to zoom while viewing photos, tapping areas of photos to remove red-eye, and dragging borders of photos to crop them.

Navigation Systems

Navigation systems in cars and other vehicles use touch input because typing on a separate keyboard is not wise while in a vehicle. Navigation system users can perform actions such as tapping to enter a destination address, dragging to display different areas of the map, or pinching and stretching to zoom. Operating a navigation system with touch input requires you to take your eyes off the road to interact with the device, so you should operate a navigation system only while your vehicle is parked or stopped. To reduce the chances of driver distraction, some built-in navigation systems reduce functionality while the vehicle is in motion.

Pen Input

Some displays and mobile devices support pen input. With **pen input**, you touch a stylus or digital pen on a flat surface to write, draw, or make selections.

Stylus

A **stylus** is a small metal or plastic device that looks like a tiny ink pen but uses pressure instead of ink. Nearly all tablets and mobile devices, some laptop screens, and a few desktop monitors have touch screens that support pen input, in addition to touch input. These computers and devices may include a stylus. Some stylus designs include buttons you can press to simulate clicking a mouse.

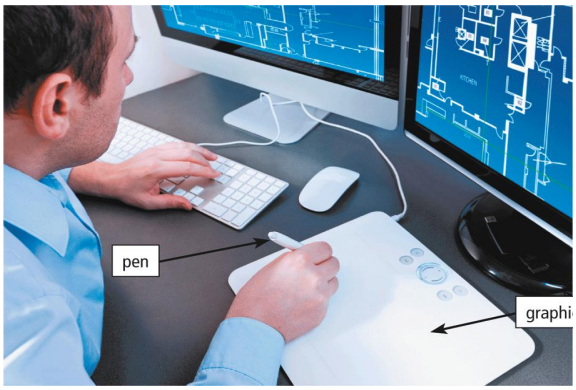
To capture a handwritten signature, a user writes his or her name on a **signature capture pad** with a stylus that is attached to the device. Software then transmits the signature to a central computer, where the signature is stored. Retailers use signature capture pads to record purchasers' signatures. **Signature capture pads** often work with **POS** terminals and include a magnetic stripe card reader.

Digital Pen

A digital pen, which is slightly larger than a stylus, is an input device that captures and converts a user's handwriting or drawings into a digital format, which users can upload (transfer) to a computer or mobile device. Some require the user to write or draw on special paper or a tablet; others can write or draw on any surface. Once uploaded, handwriting recognition software on the computer or mobile device translates the handwritten letters and symbols created on the screen into typed text or objects that the computer or device can process. For this reason, digital pens most often are used for taking notes. Some are battery operated or USB powered; others use wireless technology, such as Bluetooth.

Graphics Tablet

To use pen input on a computer that does not have a touch screen, you can attach a graphics tablet to the computer. A **graphics tablet,** also called a **digitizer**, is an electronic plastic board that detects and converts movements of a stylus or digital pen into digital signals that are sent to the computer. Each location on the graphics tablet corresponds to a specific location on the screen. Architects, mapmakers, designers, and artists, for example, use graphics tablets to create images, sketches, or designs.



MOTION, VOICE, AND VIDEO INPUT

Many of today's computers, mobile devices, and game devices support motion, voice, and video input. The following sections discuss each of these input methods. With motion input, sometimes called **gesture recognition**, users can guide on-screen elements using air gestures. Air gestures involve moving your body or a handheld input device through the air. With motion input, a device containing a camera detects your gesture and then converts it to a digital signal that is sent to a computer, mobile, or game device. For example, gamers can swing their arm or a controller to simulate rolling a bowling ball down a lane toward the pins.

Motion Input

The entertainment industry (such as for gaming and animating movies), the military, athletics, and the medical field have found uses for motion input. Motion-sensing devices communicate with a game console or a personal computer using wired or wireless technology. The console or computer translates a player's natural gestures, facial movements, and full-body motion into input. Although these devices originally were intended for gaming, developers are working on adapting them or using similar technology outside of the gaming and entertainment industries.

- **Entertainment**

  Motion-sensing game controllers enable a user to guide on-screen elements by moving a handheld input device through the air. Examples include handheld devices that enable gamers to use sweeping arm movements to simulate sports activities, such as a golf swing and remote control attachments, such as a steering wheel used to guide a car along a race course.

  Some controllers track peripheral motion within a specific area. With these devices, users can move their finger to draw or move their whole body to dance or exercise. Some use a device that can track small finger gestures, enabling users to be more precise in their movements. **Facial motion capture** converts people's facial movements into a digital format while they talk, smile, and more. Animators, for example, use the digital data to simulate facial movements to create realistic gaming avatars, or computer-generated characters in movies. Facial movements, however, are more subtle and difficult to detect. Thus, the technology used for capturing facial motions requires more precision and a higher resolution than that required by gaming devices.

- **Military**

  Military uses of motion input include training, such as flight simulation or weapon usage. To ensure safety, trainees maneuver a helicopter or other device using motion input from a remote location. Motion input also aids in physical rehabilitation for wounded soldiers by providing a method for conducting physical therapy exercises outside of a military hospital. Another use of motion input is to assist in recovery from post-traumatic stress disorder. Sufferers of this ailment can use avatars and simulators to work through scenarios in a comfortable environment.

- **Athletics**

  Coaches and sports trainers use motion input to improve athletes' performance and to correct inefficient or injury-causing motions. Analyzing the arc of a pitcher's arm, and factoring the speed of the motion and the trajectory of the ball, can help improve a pitcher's accuracy and speed. Combining the athlete's motion input with complex algorithms can pinpoint areas in which the athlete can improve.

- **Medical Field**

  The medical field also uses motion input for training. For example, surgeons can practice new technologies in a simulated environment. Using motion input that

enhances movements, surgeons also can operate less invasively. Surgeons even operate remotely, enabling experts to manipulate surgical devices and share their expertise to save lives around the world. Sports medicine specialists use motion input to assess injuries, determine treatment, and assist in physical therapy.

Voice and Audio Input

Voice input is the process of entering input by speaking into a **microphone**. The microphone may be built in the computer or device, in a headset, or an external peripheral device that sits on top of a desk or other surface. Some external microphones have a cable that attaches to a port on a computer; others communicate using wireless technology, such as Bluetooth. Uses of voice input include Internet messaging that supports voice conversations, chat rooms that support voice chats, video calls, videoconferencing, VoIP, and voice recognition. VoIP enables users to speak to other users via their Internet connection.

Voice recognition, also called **speech recognition**, is the computer or mobile device's capability of distinguishing spoken words. Some computers and mobile devices make use of built-in and third-party voice recognition applications, which have a natural language interface. A **voice recognition application** allows users to dictate text and enter instructions by speaking into a microphone. On mobile devices, these applications allow users to speak simple, task-based instructions to the device, such as setting an alarm, entering a calendar appointment, or making a call.

Some mobile devices have a **speech-to-text** feature, which recognizes a user's spoken words and enters them into email messages, text messages, or other applications that support typed text entry.

Audio Input

Voice input is part of a larger category of input called audio input. Audio input is the process of entering any sound into the computer, such as speech, music, and sound effects. To enter high-quality sound into computer, the computer uses a sound card or integrated sound capability. Users enter sound into computers and mobile devices via devices such as microphones, CD/DVD Disc players, or radios, each of which plugs in a port on the computer or device.

Some users also record live music and other sound effects into a computer by connecting external music devices, such as an electronic keyboard, guitar, drums, harmonica, and microphones, to a computer. Music production software allows users to record, compose, mix, and edit music and sounds. For example, music production software enables you to change the speed, add notes, or rearrange the score to produce an entirely new arrangement. Google.com accept voice commands for search.

VIDEO Input

Video input is the process of capturing full-motion images and storing them on a computer or mobile device's storage medium, such as a hard disk or optical disc. A **digital video** (**DV**) **camera** records video as digital signals, which you can transfer directly to a computer or mobile device with the appropriate connection. Everywhere you look, people are capturing videos using DV (digital video) cameras and mobile devices with built-in digital cameras. Using **DV technology**, you can input, edit, manage, publish, and share your videos. You can enhance digital videos by adding scrolling titles and transitions, cutting out or adding scenes, and adding background music and voice-over narration.

Webcams and Integrated DV Cameras

A **webcam** is a type of DV camera that enables you to capture video and still images, and usually audio input, for viewing or manipulation on a computer or mobile device. Some webcams are separate peripheral devices, which usually attach to the top of a desktop monitor. Many laptops, tablets, and smartphones have built-in webcams. Smartphones and other mobile devices have **built-in integrated DV cameras**. Using a webcam or integrated DV camera, you can send email messages with video attachments, broadcast live images or video over the Internet, conduct videoconferences, and make video calls.

During a **video call**, all parties see one another as they communicate over the Internet. Where video calls usually are for personal use, videoconferences typically are for business use. A **videoconference** is a meeting between two or more geographically separated people who use a network or the Internet to transmit audio and video data. To participate in a videoconference using a computer, you need videoconferencing software or access to a videoconferencing web app, along with a microphone, speakers, and a video camera attached to or built into a computer. As you speak, members of the meeting hear your voice on their speakers. Any image in front of the video camera, such as a person's face, appears in a window on each participant's screen.

You can configure some webcams to display the images they capture remotely on a webpage, or via an app on a mobile device (e.g Facebook live). This use of a webcam attracts website visitors by showing images that change regularly. Home or small business users might use webcams to show a work in progress, weather and traffic information, or employees at work; they also might use it as a security system. Some websites have live webcams that display still pictures and update the displayed image at a specified time or time intervals, such as every 15 seconds. A streaming cam has the illusion of moving images because it sends a continual stream of still images.

Scanners and Reading Devices

Some input devices save users time by capturing data directly from a source document, which is the original form of the data. Examples of source documents include time cards, order forms, invoices, paychecks, advertisements, brochures, photos, inventory tags, or any other document that contains data to be processed.

Devices that can capture data directly from a source document include **optical scanners**, Optical readers, bar code readers, magnetic stripe card readers, and **MICR (magnetic-ink character recognition) readers**.

Optical Scanners

An optical scanner, usually called a **scanner**, is a light-sensing input device that reads printed text and graphics and then translates the results into a form the computer can process. A flatbed scanner works in a manner similar to a copy machine except it creates a file of the document in memory instead of a paper copy. Once you scan a picture or document, you can display the

scanned object on the screen, modify its appearance, store it on a storage medium, print it, attach it to an email message, include it in another document, or post it on a website or photo community for everyone to see.

The quality of a scanner is measured by its resolution, that is, the number of bits it stores in a pixel and the number of pixels per inch. The higher each number, the better the quality, but the more expensive the scanner. Many scanners include **OCR (optical character recognition)** software, which can read and convert text documents into electronic files. OCR software converts a scanned image into a text file that can be edited, for example, with a word processing application.

Optical Readers

An optical reader is a device that uses a light source to read characters, marks, and codes and then converts them into digital data that a computer can process. Two technologies used by optical readers are optical character recognition (OCR) and optical mark recognition (OMR).

- Most **OCR devices** include a small optical scanner for reading characters and sophisticated software to analyze what is read. OCR devices range from large machines that can read thousands of documents per minute to handheld wands that read one document at a time. OCR devices read printed characters in a special font.
- **OMR devices** read hand-drawn marks, such as small circles or rectangles. A person places these marks on a form, such as a test, survey, or questionnaire answer sheet

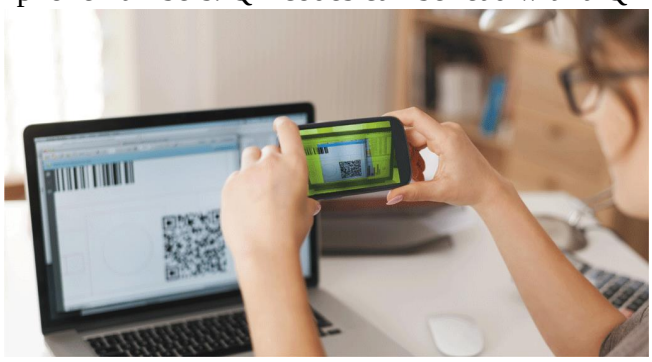
Bar Code Readers

A **bar code reader**, also called a **bar code scanner**, is an optical reader that uses laser beams to read bar codes. A **bar code** is an identification code that consists of either a set of vertical lines and spaces of different widths or a two-dimensional pattern of dots, squares, and other images. The bar code represents data that identifies the manufacturer and the item.

Manufacturers print a bar code either on a product's package or on a label that is affixed to a product, such as groceries, books, clothing, vehicles, mail, and packages. Each industry uses its own type of bar code.

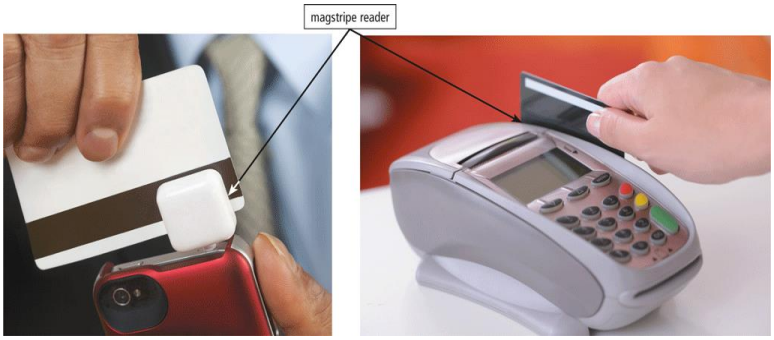
QR Code Reader

A **QR code** (quick response code) is known as a 2-D bar code because it stores information in both a vertical and horizontal direction. The information it stores can orrespond to a web address or other content, such as contacts or phone numbers. QR codes can be read with a QR bar code reader or a QR code reader app on a smartphone or other mobile device. All types of material, from posters to textbooks to merchandise, include QR codes that consumers scan to obtain additional information, which may be in the form of a website or may display text for the user to read.



Magstripe Readers

A **magstripe reader**, short for **magnetic stripe card reader**, reads the magnetic stripe on the back of credit cards, entertainment cards, bank cards, identification cards, and other similar cards. The stripe contains information identifying you and the card issuer. Some information stored in the stripe may include your name, account number, the card's expiration date, and a country code.



Most magstripe readers are separate devices that communicate with a POS (point-of-sale) terminal, such as those in retail stores. Home or small business users, however, may attach a small plastic magstripe reader to a smartphone or tablet so that they can accept payments using a mobile app. When a credit card is swiped through a magstripe reader, it reads the information stored on the magnetic stripe on the card.

MICR Readers

MICR (magnetic-ink character recognition) devices read text printed with magnetized ink. An MICR reader converts MICR characters into a form the computer can process. The banking industry almost exclusively uses MICR for **check processing**. Each check in your check book has precoded MICR characters beginning at the lower-left edge. When a bank receives a check for payment, it uses an MICR inscriber to print the amount of the check in MICR characters in the lower-right corner. Each check is inserted in an MICR reader, which sends the check information — including the amount of the check — to a computer for processing.

Data Collection Devices

Instead of reading or scanning data from a source document, a data collection device obtains data directly at the location where the transaction or event takes place. For example, employees use bar code readers, handheld computers, or other mobile devices to collect data wirelessly. These types of data collection devices are used in restaurants, grocery stores, factories, warehouses, the outdoors, or other locations where heat, humidity, and cleanliness are not easy to control. For example, factories and retail stores use data collection devices to take inventory and order products. Data collection devices and many mobile computers and devices have the capability of wirelessly transmitting data over a network or the Internet. Increasingly more users today send data wirelessly to central office computers using these devices.

UNIT 6: OUTPUT DEVICES

6.1 Unit Objectives

After completing this unit, you will be able to:

1. Identify the types of output
2. Explain the characteristics of various displays
3. Summarize the various types of printers
4. Identify the purpose and features of speakers, headphones, data projectors etc.
5. Identify various assistive technology input and output methods

6.2 Definition

Output is data that has been processed into a useful form. Computers process data (input) into information (output). The form of output varies, depending on the hardware and software being used and the requirements of the user. Users view or watch output on a screen, print it, or hear it through speakers, headphones, or earbuds. While working with a computer or mobile device, a user encounters four basic types of output: text, graphics, audio, and video. Very often, a single form of output, such as a webpage, includes more than one of these types of output.

Text: Examples of output that primarily contain text are text messages, Internet messages, memos, letters, press releases, reports, classified advertisements, envelopes, and mailing labels. On the web, users read blogs, news and magazine articles, books, television show transcripts, stock quotes, speeches, and lectures.

Graphics: Many forms of output include graphics to enhance visual appeal and convey information. Business letters have logos. Reports include charts. Newsletters use drawings, clip art, and photos. Users print high-quality photos taken with a digital camera. Many websites use animations.

Audio: Users download their favorite songs and listen to the music. Software, such as games,

encyclopedias, and simulations, often include musical accompaniments and audio clips, such as narrations and speeches. On the web, users listen to radio broadcasts, audio clips, podcasts, sporting events, news, music, and concerts. They also use VoIP.

Video: As with audio, software and websites often include video clips and video blogs. Users watch news reports, movies, sporting events, weather conditions, and live performances on a computer or mobile device. They attach a video camera to a computer or mobile device to watch video or programs. Common methods of output include displays, printers, speakers, headphones and earbuds, data projectors, interactive whiteboards, and force-feedback game controllers and tactile output. The following sections discuss each of these output devices.

6.3 Examples and Uses

Displays

A display device, or simply **display**, is an output device that visually conveys text, graphics, and video information. Sometimes called soft copy, information on a display exists electronically and appears for a temporary period. Displays consist of a screen and the components that produce the information on the screen. Most current displays are a type of flat-panel display, which means they have a shallow depth and a flat screen. Desktops often use a monitor as their display.

A **monitor** is a display that is packaged as a separate peripheral device. Some monitors have a tilt-and-swivel base, which allows you to adjust the angle of the screen to minimize neck strain and reduce glare from overhead lighting. With some, you also can rotate the screen. Adjustable monitor stands allow you to adjust the height of the monitor. Monitor controls enable you to adjust the brightness, contrast, positioning, height, and width of images. Some have touch screens, integrated speakers, and/or a built-in webcam.

Most mobile computers and devices integrate the display and other components into the case. Size of these displays varies depending on the mobile computer or device. Some mobile computers and many mobile devices have touch screens. Traditional laptops have a display that attaches with a hinge to the case. Tablets are available with two types of displays: one that attaches with a hinge and one built into the top of the case. Some smartphone and digital camera displays also attach with a hinge to the device. On other smartphones and most portable media players, digital cameras, and handheld game consoles, the display is built into the case.

Newer vehicles integrate a display in the dashboard, enabling drivers to control audio, video, navigation, temperature, and other settings.

Display Technologies

Many desktop monitors, along with the screens on mobile computers and devices, use some type of LCD technology. A liquid crystal display (**LCD**) sandwiches a liquid compound between two sheets of material that presents sharp, flicker-free images on a screen when illuminated. The light source, called the backlight, often uses either CCFL (cold cathode fluorescent lamp) or LED (light-emitting diode) technology. A display that uses LED for the backlight often is called an LED display or an LED LCD display.

LED displays consume less power, last longer, and are thinner, lighter, and brighter than a display that uses CCFL technology, but they also may be more expensive. Screens in laptops and mobile devices often use LED backlight technology. LCD displays typically produce colour using active-matrix, or TFT (thin-film transistor), technology, which uses a separate transistor to apply charges to each liquid crystal cell and, thus, displays high-quality colour that is viewable from all angles. Several types of active matrix displays, or panels, are available, with some providing higher quality than others.

VDU

VDU stands for "**Visual Display Unit**." A VDU displays images generated by a computer or other electronic device. The term VDU is often used synonymously with "monitor," but it can also refer to other types of displays, such as a digital projector. Visual display units may be peripheral devices or may be integrated with the other components. For example, the Apple iMac uses an all-in-one design, in which the screen and computer are built into a single unit. Early VDUs were primarily **cathode ray tube** (CRT) displays and typically had a diagonal size of 13 inches or less. During the 1990s, 15" and 17" displays became standard, and some manufacturers began producing displays over 20" in size.

Display Quality

The quality of a display depends primarily on its resolution, response time, brightness, dot pitch, and contrast ratio.

- **Resolution** is the number of horizontal and vertical pixels in a display. For example, a monitor or screen that has a 1600 3 900 resolution displays up to 1600 pixels per horizontal row and 900 pixels per vertical row, for a total of 1,440,000 pixels to create a screen image. A higher resolution uses a greater number of pixels and, thus, provides a smoother, sharper, and clearer image. As the resolution increases, however, some items on the screen appear smaller. Displays are optimized for a specific resolution, called the native resolution. Although you can change the resolution to any setting, for best results, use the monitor or screen's native resolution setting.
- **Response time** of a display refers to the time in milliseconds (ms) that it takes to turn a pixel on or off. Response times of displays range from 2 to 16 ms. The lower the number, the faster the response time.

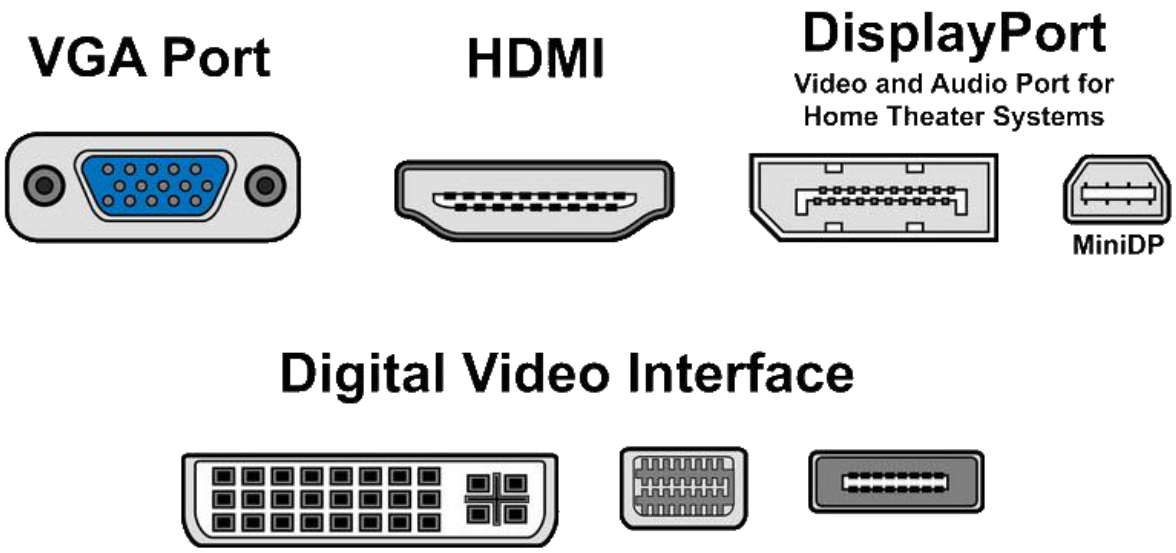
- **Brightness** of a display is measured in **nits**. A **nit** is a unit of visible light intensity equal to one candela (formerly called candlepower) per square meter. The candela is the standard unit of luminous intensity. Displays today range from 250 to 550 nits. The higher the nits, the brighter the images.
- **Dot pitch**, sometimes called **pixel pitch**, is the distance in millimeters between pixels on a display. Text created with a smaller dot pitch is easier to read. Advertisements normally specify a display's dot pitch or pixel pitch. Average dot pitch on a display should be .30 mm or lower. The lower the number, the sharper the image.
- **Contrast ratio** describes the difference in light intensity between the brightest white and darkest black that can be produced on a display. Contrast ratios today range from 500:1 to 2000:1. Higher contrast ratios represent colours better.

Graphics Chips, Ports, and Flat-Panel Monitors

A cable on a monitor plugs in a port on the computer, which enables communications from a graphics chip. This chip, called the graphics processing unit (GPU), controls the manipulation and display of graphics on a display device. The GPU either is integrated on the motherboard or resides on a video card in a slot on the motherboard.

Today's monitors use a digital signal to produce a picture. To display the highest quality images, the monitor should plug in a **DVI port, an HDMI port, a VGA port, or a DisplayPort**.

- A **DVI (Digital Video Interface)** port enables digital signals to transmit directly to a monitor.
- An **HDMI (High-Definition Media Interface)** port combines DVI with high-definition (HD) television, audio, and video. Some ultrathin laptops have mini-HDMI ports that require the use of an adapter (or dongle) when connecting to a standard-size HDMI display.
- A **DisplayPort** is an alternative to DVI that also supports high-definition audio and video. Over the years, several video standards have been developed to define the resolution, aspect ratio, number of colours, and other display properties. The aspect ratio defines a display's width relative to its height. A 2:1 aspect ratio, for example, means the display is twice as wide as it is tall. The aspect ratio for a widescreen monitor is 16:9 or 16:10. Some displays support multiple video standards.
- A **Video Graphics Array** (**VGA**) connector is a three-row 15-pin connector. The 15-pin **VGA** connector is on many video cards, computer monitors, laptop computers, projectors, and high definition television sets.



DTVs and Smart TVs

Home users sometimes use a **digital television (DTV)** as a display. Gamers also use a television as their output device. They plug one end of a cable in the game console and the other end in the video port on the television.

HDTV (**high-definition television**) is the most advanced form of digital television, working with digital broadcast signals, transmitting digital sound, supporting wide screens, and providing high resolutions. A Smart TV is an Internet-enabled HDTV from which you can browse the web, stream video from online media services, listen to Internet radio, communicate with others on online social media, play online games, and more — all while watching a television show. Using a SmartTV, you can stream content from the TV to other Internetenabled devices, such as a tablet or smartphone, and use cloud storage services to share content.

DTVs often use LCD, LED, or plasma technology. A plasma display uses gas plasma technology, which sandwiches a layer of gas between two glass plates. When voltage is applied,

the gas releases **ultraviolet (UV)** light. This UV light causes the pixels on the screen to glow and form an image.

Printers

A **printer** is an output device that produces text and graphics on a physical medium, such as paper. Printed information **(hard copy**) exists physically and is a more permanent form of output than that presented on a display (**soft copy**). A hard copy, also called a printout, is either in portrait or landscape orientation. A printout in **portrait orientation** is taller than it is wide, with information printed across the shorter width of the paper. A printout in **landscape orientation** is wider than it is tall, with information printed across the widest part of the paper. Letters, reports, and books typically use portrait orientation. Spreadsheets, slide shows, and graphics often use landscape orientation.

To meet the range of printing needs from home users to enterprise users, many different types and styles of printers exist with varying speeds, capabilities, and printing methods.

Nonimpact Printers

A **nonimpact printer** forms characters and graphics on a piece of paper without actually contacting the paper. Some spray ink, while others use heat or pressure to create images. Commonly used nonimpact printers are ink-jet printers, photo printers, laser printers, all-in-one printers, thermal printers, mobile printers, label printers, plotters, and large-format printers.

Ink-Jet Printers

An **ink-jet printer** is a type of nonimpact printer that forms characters and graphics by spraying tiny drops of liquid ink onto a piece of paper. Ink-jet printers have become a popular type of colour printer for use in the home. Ink-jet printers produce text and graphics in both black-and-white and colour on a variety of paper types and sizes. These printers normally use individual sheets of paper stored in one or two removable or stationary trays.

Most ink-jet printers can print lab-quality photos. Ink-jet printers also print on other materials, such as envelopes, labels, index cards, greeting card paper (card stock), transparencies, and iron-on T-shirt transfers. Many ink-jet printers include software for creating greeting cards, banners, business cards, and letterhead. The speed of an ink-jet printer is measured by the number of **pages per minute (ppm)** it can print. Graphics and colours print at a slower rate than text.

Ink Cartridges

The printhead mechanism in an ink-jet printer contains ink-filled cartridges.

Each cartridge has fifty to several hundred small ink holes, or nozzles. The ink propels through any combination of the nozzles to form a character or image on the paper. When the cartridge runs out of ink, you simply replace the cartridge. Most ink-jet printers use two or more ink cartridges, one containing black ink and the other(s) containing colours. Some colour cartridges contain a variety of ink colours; others contain only a single colour. Consider the number of ink cartridges a printer requires, along with the cost of the cartridges, when purchasing a printer. To reduce the expense of purchasing cartridges, some users opt to purchase refilled cartridges or have empty cartridges refilled by a third-party vendor.

Photo Printers

A **photo printer** is a colour printer that produces lab-quality photos. Generally, the more sizes the printer prints, the more expensive the printer. Many photo printers use ink-jet technology. With models that can print letter-sized documents, users connect the photo printer to their computer and use it for all their printing needs. For a few hundred dollars, this type of photo printer is ideal for the home or small business user. Some photo printers are PictBridge enabled, so that you can print photos without a computer. PictBridge is a standard technology that allows you to print photos directly from a digital camera by connecting a cable from the digital camera to a USB port on the printer. Photo printers also usually have a built-in card slot(s) so that the printer can print digital photos directly from a memory card.

Laser Printers

A **laser printer** is a high-speed, high-quality nonimpact printer. Laser printers are available in both black-and-white and colour models. A laser printer for personal computers ordinarily uses individual A4 sheets of paper stored in one or more removable trays that slide in the printer case. Laser printers print text and graphics in high-Quality resolutions. While laser printers usually cost more than ink-jet printers, many models are available at affordable prices for the home user. Laser printers usually print at faster speeds than ink-jet printers.

When printing a document, laser printers process and store the entire page before they actually print it. For this reason, laser printers sometimes are called page printers. Storing a page before

printing requires that the laser printer has a certain amount of memory in the device. The more memory in the printer, the faster it usually can print.

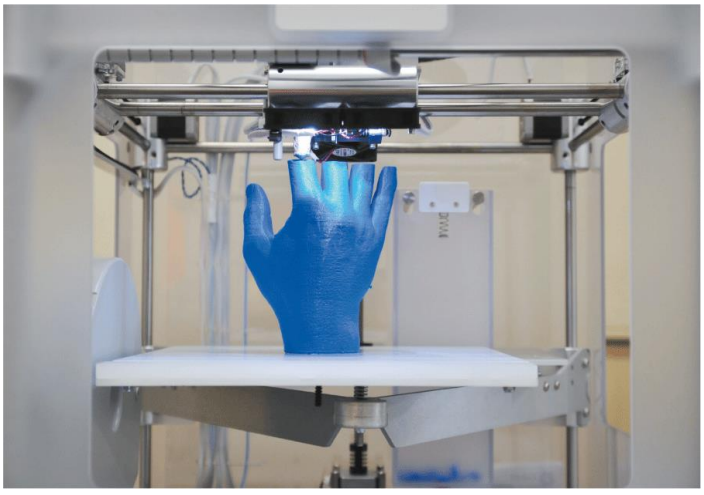
Operating in a manner similar to a copy machine, a laser printer creates images using a laser beam and powdered ink, called toner. The laser beam produces an image on a drum inside the printer. The light of the laser alters the electrical charge on the drum wherever it hits. When this occurs, the toner sticks to the drum and then transfers to the paper through a combination of pressure and heat. When the toner runs out, you replace the toner cartridge.

All-in-One Printers

An all-in-one printer, also called a **multifunction printer (MFP)**, is a single device that looks like a printer or a copy machine but provides the functionality of a printer, scanner, copy machine, and perhaps a fax machine. Some use colour ink-jet printer technology, while others use laser technology.

3-D Printers

A **3-D printer** uses a process called additive manufacturing to create an object by adding material to a three-dimensional object, one horizontal layer at a time. 3-D printers can print solid objects, such as clothing, prosthetics, eyewear, implants, toys, parts, prototypes, and more. Using a digital model created with **CAD (computer-aided design)** software, 3-D printers begin creating an object



at the bottom and add layers of material to the object until it is complete. Depending on the type of printer, the layers are built with liquid polymer, gel, or resin. In the past, 3-D printers were quite expensive and used only by large corporations. Today, home and small business users work with more affordable desktop 3-D printers.

Mobile Printers

A **mobile printer** is a small, lightweight, battery-powered printer that allows a mobile user to print from a laptop, smartphone, or other mobile device while traveling. Barely wider than the paper on which they print, mobile printers fit easily in a briefcase alongside a laptop. Mobile printers mainly use ink-jet or thermal technology. Many connect to a USB port. Others have a built-in wireless port through which they communicate with the computer.

Label Printers

A **label printer** is a small printer that prints on an adhesive-type material that can be placed on a variety of items, such as envelopes, packages, optical discs, photos, and file folders. Most label printers also print bar codes. Label printers typically use thermal technology.

Plotters and Large-Format Printers

Plotters are sophisticated printers used to produce high-quality drawings, such as blueprints, maps, and circuit diagrams. These printers are used in specialized fields such as engineering and drafting and usually are very costly. Current plotters use a row of charged wires (called styli) to draw an electrostatic pattern on specially coated paper and then fuse toner to the pattern. The printed image consists of a series of very small dots, which provides high-quality output. Using ink-jet printer technology, but on a much larger scale, a **large-format printer** creates photo-realistic-quality color prints. Graphic artists

use these high-cost, high-performance printers for signs, posters, and other professional quality displays

Impact Printers

An **impact printer** forms characters and graphics on a piece of paper by striking a mechanism against an inked ribbon that physically contacts the paper. Impact printers characteristically are noisy because of this striking activity. Impact printers are ideal for printing multipart forms because they print through many layers of paper easily. Factories, warehouses, and retail counters may use impact printers because these printers withstand dusty environments, vibrations, and extreme temperatures.

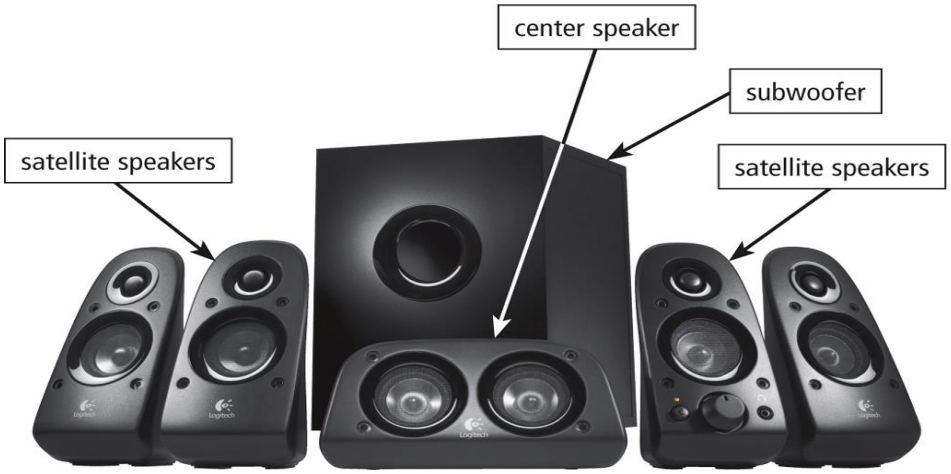
Other Output Devices

In addition to displays and printers, other output devices are available for specific uses and applications. These include speakers, headphones and earbuds, data projectors, interactive whiteboards, and force-feedback game controllers and tactile output.

Speakers

Most personal computers and mobile devices have a small internal speaker that usually emits only low-quality sound. Thus, many users attach surround sound speakers or speaker systems to their computers, game consoles, and mobile devices to generate higher-quality sounds for playing games, interacting with multimedia presentations, listening to music, and viewing movies.

Most surround sound computer speaker systems include one or two center speakers and two or more satellite speakers that are positioned so that sound emits from all directions. Speakers typically have tone and volume controls, allowing users to adjust settings. To boost the low bass sounds, surround sound speaker systems also include a subwoofer. In some configurations, a cable connects the speakers or the subwoofer to a port on the computer or device. With wireless speakers, however, a transmitter connects to a port on the computer, which wirelessly communicates with the speakers.



Headphones and Earbuds

When using speakers, anyone in listening distance can hear the output. In a computer laboratory or other crowded environment, speakers might not be practical. Instead, users can listen through headphones or earbuds so that only the individual wearing the headphones or earbuds hears the sound from the computer. The difference is that **headphones** cover or are placed outside of the ear, whereas **earbuds** rest inside the ear canal. Both headphones and earbuds usually include noise-cancelling technology to reduce the interference of sounds from the surrounding environment.

A **headset** is a device that functions as both headphones and a microphone. Computer and smartphone users wear a headset to free their hands for typing and other activities while talking or listening to audio output. Many headsets communicate wirelessly with the computer or mobile device. As an alternative to headphones, earbuds, or headsets, you can listen to audio from mobile devices, such as a portable media player or smartphone, through speakers in a vehicle or on a stereo system at home or work. Or, you can purchase speakers specifically designed to play audio from the device.

Data Projectors

A **data projector** is a device that projects the text and images displaying on a computer or mobile device screen on a larger screen so that an audience can see the image clearly. For example, many classrooms use data projectors so that all students can easily see an instructor's presentation on the screen. Some data projectors are large devices that attach to a ceiling or wall in an auditorium. Others, designed for the mobile user, are small portable devices that can be transported easily. Two types of smaller, lower-cost units **are LCD projectors and DLP projectors.**

- An LCD projector, which uses liquid crystal display technology, attaches directly to a computer or mobile device and uses its own light source to display the information shown on the computer screen. Because LCD projectors tend to produce lower-quality images, users often prefer DLP projectors for their sharper, brighter images.
- A digital light processing (DLP) projector uses tiny mirrors to reflect light, which produces crisp, bright, colorful images that remain in focus and can be seen clearly, even in a well-lit room. Some newer televisions use DLP instead of LCD or plasma technology.

Interactive Whiteboards

An **interactive whiteboard** is a touch-sensitive device, resembling a dry-erase board, that displays the image on a connected computer screen, usually via a projector. A presenter controls the program by clicking a remote control, touching the whiteboard, drawing on or erasing the whiteboard with a special digital pen and eraser, or writing on a special tablet. Notes written on the interactive whiteboard can be saved directly on the computer and/or printed. Interactive whiteboards are used frequently in classrooms as a teaching tool, during meetings as a collaboration tool, and to enhance delivery of presentations.

Force-Feedback Game Controllers and Tactile Output

Joysticks, wheels, gamepads, and motion-sensing game controllers are input devices used to control movements and actions of a player or object in computer games, simulations, and video games. These devices also function as output devices when they include force feedback, which is a technology that sends resistance to the device in response to actions of the user. For example, as you use the simulation software to drive from a smooth road onto a gravel alley, the steering wheel trembles or vibrates, making the driving experience as realistic as possible. These devices also are used in practical training applications, such as in the military and aviation. Some input devices, such as a mouse, and mobile devices, such as a smartphone, include tactile output that provides the user with a physical response from the device. For example, users may sense a bumping feeling on their hand while scrolling through a smartphone's contact list.

Assistive Technology Input and Output

The ever-increasing presence of computers in everyone's lives has generated an awareness of the need to address computing requirements for those who have or may develop physical limitations.

Besides voice recognition, which is ideal for **blind or visually impaired users**, several other input options are available. Users with limited hand mobility who want to use a keyboard can use an on-screen keyboard or a keyboard with larger keys. Users with limited hand movement can use a head-mounted pointer to control the pointer or insertion point. To simulate the functions of a mouse button, a user works with switches that control the pointer.

The switch might be a hand pad, a foot pedal, a receptor that detects facial motions, or a pneumatic instrument controlled by puffs of air.

For users with mobility, hearing, or vision disabilities, many different types of output options are available. Hearing-impaired users, for example, can instruct programs to display words instead of sounds. Visually impaired users can change screen settings, such as increasing the size or changing the colour of the text to make the words easier to read. Instead of using a monitor, blind users can work with voice output. That is, the computer speaks aloud the information that appears on the screen. Another alternative is a *Braille* **printer,** which prints information on paper in Braille

UNIT 7: COMMUNICATIONS AND NETWORKS

7.1 Unit Objectives

After completing this chapter, you will be able to:

1. Discuss the purpose of components required for successful communications
2. Identify various sending and receiving devices.
3. Differentiate among LANs, MANs, WANs, and PANs
4. Differentiate between client/server and peer-to-peer networks
5. Explain the purpose of communications software
6. Describe various network communications standards and protocols
7. Describe various types of communications lines
8. Describe commonly used communications devices
9. Discuss ways to set up and configure a home network
10. Differentiate among physical transmission media
11. Differentiate among wireless transmission media

Communications

The process in which two or more computers or devices transfer data, instructions, and Information is known as digital communications. Today, even the smallest computers and devices can communicate directly with one another, with hundreds of computers on a corporate network, or with millions of other computers around the globe — often via the Internet.

Some communications involve cables and wires; others are sent wirelessly through the air. For successful communications, you need the following:

- A **sending device** that initiates an instruction to transmit data, instructions, or information
- A communications device that connects the sending device to transmission media
- **Transmission media**, or a communications channel, on which the data, instructions, or information travel
- A communications device that connects the transmission media to a receiving device
- A **receiving device** that accepts the transmission of data, instructions, or information

All types of computers and mobile devices serve as sending and receiving devices in a communications system. This includes servers, desktops, laptops, tablets, smartphones, portable media players, handheld game devices, and GPS receivers. Communications devices, such as modems, wireless access points, and routers, connect transmission media to a sending or receiving device. Transmission media can be wired or wireless.

This unit presents types of networks, along with various types of communications lines and devices, and transmission media.

7.2 Network

A **network** is a collection of computers and other devices connected together via communications devices and transmission media. A network can be internal to an organization or span the world by connecting to the Internet. Many home and business users create a network to facilitate communications, share hardware, share data and information, share software, and transfer funds.

7.2.2 Types of Computer Networks

Computer Networks can be classified based on the extend of geographical space they cover. Networks usually are classified as a local area network (LAN), metropolitan area network (MAN), wide area Network (WAN), or personal area network (PAN).

LAN

A **local area network** (**LAN**) is a network that connects computers and devices in a limited geographical area, such as a home, school, office building, or closely positioned group of buildings. Each computer or device on the network, called a **node**, often shares resources, such as printers, large hard drives, and programs. Often, the nodes are connected via cables. Computers and devices on different floors access the same LAN in an office building. Computers and devices on the network often are identified as **nodes.**

A **wireless LAN** (**WLAN**) is a LAN that uses no physical wires. Computers and devices that access a wireless LAN must have built-in wireless capability or the appropriate wireless network card, USB adapter, or other wireless device. A WLAN may communicate with a wired LAN for access to its resources, such as software, hardware, and the Internet.

MAN

A metropolitan area network (MAN) is a high-speed network that connects local area networks in a metropolitan area, such as a city or town, and handles the bulk of communications activity across that region. A MAN typically includes one or more LANs, but covers a smaller geographic area than a WAN. A MAN usually is managed by a consortium of users or by a single network provider that sells the service to the users. Local and state governments, for example, regulate some MANs. Phone companies, cable television providers, and other organizations provide users with connections to the MAN.

WAN

A **wide area network** (**WAN**) is a network that covers a large geographic area (such as a city, country, or the world) using a variety of wired and wireless transmission media. A WAN can

be one large network or can consist of multiple LANs connected together. The Internet is the world's largest WAN.

PAN

A **personal area network** (**PAN**) is a network that connects computers and devices in an individual's workspace using wired and wireless technology. Devices include smartphones, digital cameras, printers, and more. A PAN may connect devices through a router using network cables or directly using special USB cables. PANs also may use Bluetooth or Wi-Fi technology. **A body area network (BAN),** sometimes called a **body sensor network (BSN)**, is a type of PAN that wirelessly connects sensors worn by, carried by, implanted in, or attached to a human body.

BAN

A **body area network**, also referred to as a wireless body area network or a body sensor network or a medical body area network, is a wireless network of wearable computing devices. A **medical body area network (MBAN)** is a special-purpose **BAN** that provides telehealth services through **remote patient monitoring (RPM)** and can initiate alerts and even care, such as the delivery of medication. By wearing, carrying, implanting, or attaching small devices to a person's body, medical professionals can track vital signs and monitor heart rhythms, breathing rates, and much more via a BAN, which uses low powered sensors to collect data. The BAN sends the collected data wirelessly to an Internet-connected device, which relays the data to a medical data server. In some cases, the data transmits directly to emergency services.

Some devices also automatically can dispense medications based on the data collected. Because of these devices, a patient may not have to visit a medical facility to receive treatment. Heart patients, diabetics, or those with asthma or other similar conditions can perform regular daily activities while wearing the device. If it collects any unusual data, the patient can receive medical resources immediately. First responders also use these devices. A fire chief, for example, can monitor firefighters' body temperature and oxygen levels as they battle a fire.

The disadvantages of BANs include data validity and security. What happens if a device stops working or its data becomes corrupt? Serious health complications could result if the patient is not monitoring conditions via another technique. For example, devices that administer medication could cause an overdose or underdose if not working properly. Medical data is highly sensitive. An unscrupulous individual could intercept vital signs and other personal data during transfer, violating a patient's confidentiality. Privacy advocates also have concerns about nonmedical uses of BANs.

NETWORK ARCHITECTURES

The configuration of computers, devices, and media on a network is sometimes called the network architecture. Two examples of network architectures are client/server or peer-to-peer.

Client/Server.

On a **client/server network**, one or more computers act as a server, and the other computers on the network request services from the server. A **server**, sometimes called a host computer, controls access to the hardware, software, and other resources on the network and provides a centralized storage area for programs, data, and information. The **clients** are other computers and mobile devices on the network that rely on the server for its resources. For example, a server might store an organization's email messages. Clients on the network, which include any users' connected computers or mobile devices, access email messages on the server. Both wired and wireless networks can be configured as a client/server network.

Although it can connect a smaller number of computers, a client/server network architecture typically provides an efficient means to connect 10 or more computers. Most client/server networks require a person to serve as a network administrator because of the large size of the network. Some servers are dedicated servers that perform a specific task. For example, a network server manages network traffic (activity), and a web server delivers requested webpages to computers or mobile devices.

Peer-to-Peer

A peer-to-peer (P2P) network is a simple, inexpensive network architecture that typically connects fewer than 10 computers. Each computer or mobile device, called a peer, has **equal responsibilities and capabilities**, sharing hardware (such as a printer), data, or information with other computers and mobile devices on the peer-to-peer network. Peer-to-peer networks allow users to share resources and files located on their computers and to access shared resources found on other computers on the network. Peer-to-peer networks do not have a common file server. Instead, all computers can use any of the resources available on other computers on the network. For example, you might set up a P2P network between an Android tablet and a Windows laptop so that they can share files using Bluetooth or so that you can print from the tablet to a printer accessible to all devices on the network. Both wired and wireless networks can be configured as a peer-to-peer network. P2P networks are ideal for very small businesses and home users. Some operating systems include a P2P networking tool that allows users to set up a peer-to-peer network. Many businesses also see an advantage to using P2P. That is, companies and employees can exchange files using P2P, freeing the company from maintaining a network server for this purpose.

What is P2P file sharing?

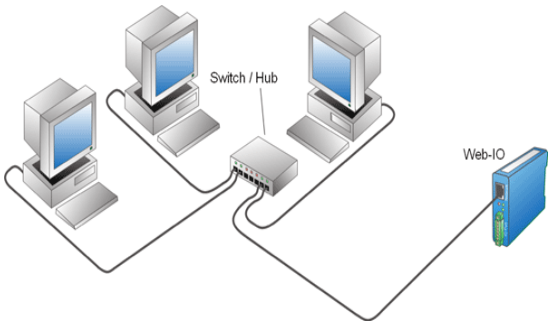
P2P file sharing, sometimes called a file sharing network, describes a network configuration on which users access one another's hard drives and exchange files directly via a file sharing program such as Xender. As more users connect to the network, each user has access to shared files on other users' hard drives. When users sign out of the network, others no longer have access to their hard drives.

Network Topologies

Network topology can either be logical or physical. Logical topology is the conceptual flow of data between the devices in the network. Physical topology is the physical arrangement of devices on a network. **We shall consider various physical network topologies here**. There are four categories: **Star topology**, **Bus topology**, **Ring topology** and **Mesh topology**. **Hybrid** combinations of these topologies also exist. **Star topology** – all computers and devices are connected to a main **hub** or switch. The **hub** or switch amasses and disburses the flow of data within the network.

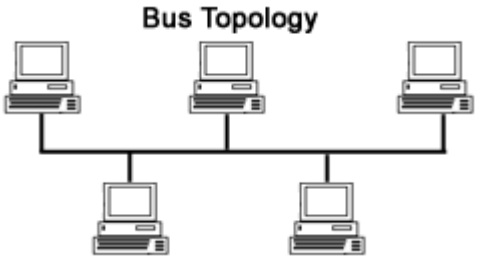
Star Topology

The devices are arranged such that all of them are connected to a centralized device. The central connection point might not necessarily be a server. Its advantage is that the failure of any link will not affect the rest the network. One major disadvantage is that when the central device fails the whole network collapses, it also consumes a lot of cable making it expensive except if it is wireless.



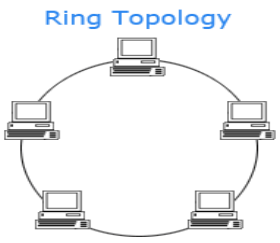
Bus Topology

Uses a common backbone to connect all network devices. The backbone (central cord) functions as a shared communication link, which carries network data. It works better with a few devices. When the backbone fails, the entire network becomes unusable.

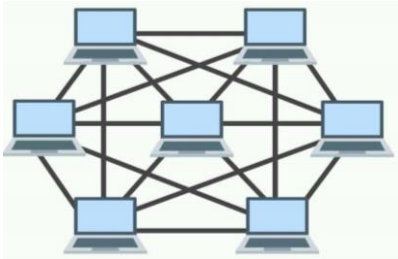


Ring Topology

Connects all devices in a circle, with each device having two neigbours. This topology minimizes cabling, but failure of one of any one device can take down the entire network.



Mesh Topology:
Connect each network device to many other network devices. Data travelling on a mesh network can take any of the several possible paths from its source to its destination. Even though it may seem expensive to install, mesh topology is very robust, even if several links fail, data can follow alternative functioning links to reach its destination.



7.2.3 Uses of Computer Network

Computer networks are used to:

i. Facilitate communications. Using a network, people communicate efficiently and easily via email, Internet messaging, chat rooms, blogs, online social networks, video calls, online meetings, videoconferences, VoIP, text messaging, and more. Some of these communications occur within an internal network or globally over the Internet.

ii. Share hardware. Each computer or device on a network can be provided access to hardware on the network. For example, each computer and mobile device user can access a printer on the network, as they need it. Thus, home and business users create networks to save money on hardware expenses.

iii. Share data and information. Any authorized user can access data and information stored on a network. A large company, for example, might have a database of customer information. Any authorized employee can access the database using a computer or mobile device connected to the network. Most businesses use a standard, such as **EDI (electronic data interchange)**, that defines how Business documents travel across transmission media. For example, businesses use EDI to send bids and proposals, place and track orders, and send invoices.

iv. Share software. Users connected to a network can access software on the network. To support multiple users' software access, vendors often sell versions of their software designed to run on a network or as a web app on the Internet. These network and Internet subscription versions usually cost less than buying individual copies of the software for each computer. The license fees for these programs typically are based on the number of users or the number of computers or mobile devices attached to the network.

v. Transfer funds. Electronic funds transfer (EFT) allows users connected to a network to exchange money from one account to another via transmission media. Both businesses and consumers use EFT. Examples include wire transfers, use of credit cards and debit cards, direct deposit of funds into bank accounts, online banking, and online bill payment. Instead of using the Internet or investing in and administering an internal network, some companies hire a value-added network provider for network functions. **A value-added network (VAN)** provider is a third-party business that provides networking services such as EDI services, secure data and

information transfer, storage, or email. Some VANs, such as PayPal, charge an annual or monthly fee; others charge by the service used.

Communications Software

Communications software consists of programs and apps that (1) help users establish a connection to another computer, mobile device, or network; (2) manage the transmission of data, instructions, and information; and (3) provide an interface for users to communicate with one another. The first two often are provided by or included as tools with an operating system or bundled with a communications device. The third is provided by applications such as email, FTP, browsers, discussion boards, chat rooms, Internet messaging, videoconferencing, and VoIP.

Sometimes, communications devices are pre-programmed to accomplish communications tasks. Some routers, for example, contain firmware for various protocols. Other communications devices require separate communications software to ensure proper transmission of data. Communications software works with the network standards and protocols to ensure data moves through the network or the Internet correctly.

Examples of Communication Software

Some commonly used communication software include skype, Imo, WhatsApp, Facebook Messenger and Twitter.

7.3 Network Communication Standards and Protocols

Today's networks connect terminals, devices, and computers from many different manufacturers across many types of networks. For the different devices on various types of networks to be able to communicate, the network must use similar techniques of moving data through the network from one application to another. To alleviate the problems of incompatibility and ensure that hardware and software Components can be integrated into any network, various organizations such as **ANSI (American National Standards Institute**) and **IEEE (Institute of Electrical and Electronics Engineers)** propose, develop, and approve network standards.

A network standard defines guidelines that specify the way computers access the medium to which they are connected, the type(s) of medium used, the speeds used on different types of networks, and the type(s) of physical cable and/or the wireless technology used. Hardware and software manufacturers design their products to meet the guidelines specified in a particular standard, so that their devices can communicate with the network. A standard that outlines characteristics of how two devices communicate on a network is called a protocol. Specifically, a protocol may define data format, coding schemes, error handling, and the sequence in which data transfers over a network. Protocols are rules that determine how communications devices and media work over a network.

Network Communications Standards and Protocols

Name	Type	Sample Usage
Ethernet	Standard	LAN
Token Ring	Standard	LAN
TCP/IP	Protocol	Internet
Wi-Fi	Standard	Hot Spots
Bluetooth	Protocol	Wireless Headset
UWB	Standard	Inventory Tracking
IrDA	Standard	Remote Control
RFID	Protocol	Tollbooth
NFC	Protocol	Mobile Phone Payment
LTE	Standard	Mobile Phones

Network standards and protocols often work together to move data through a network. Some of these standards define how a network is arranged physically, while others specify how messages travel along a network. Thus, as data moves through a network from one program to another, it may use one or more of these standards.

Ethernet

Ethernet is a network standard that specifies no central computer or device on the network (nodes) should control when data can be transmitted. That is, each node attempts to transmit data when it determines the network is available to receive communications. If two computers or devices on an Ethernet network attempt to send data at the same time, a collision will occur.

When this happens, the computers or devices resend their messages until data transfer is successful. The Ethernet standard defines guidelines for the physical configuration of a network (e.g., cabling, network devices, and nodes). Ethernet currently is the most popular network standard for LANs because it is relatively inexpensive and easy to install and maintain. Depending on the transmission media used, Ethernet networks have data transfer rates that range from 10 Mbps for home/small office users to 100 Gbps for enterprise users.

Token Ring

The **token ring** standard specifies that computers and devices on the network share or pass a special signal, called a token, in a unidirectional manner and in a preset order. A token is a special series of bits that function like a ticket. The device with the token can transmit data over the network. Only one token exists per network. This ensures that only one computer transmits data at a time. Although token ring is not as widely used today, many networks use the concept of a token. The token ring standard defines guidelines for the physical configuration of a network (e.g., cabling, network cards, and devices). Some token ring networks connect up to 72 devices. The data transfer rate on a token ring network ranges from 4 Mbps to 1 Gbps.

TCP/IP

Short for **Transmission Control Protocol/Internet Protocol, TCP/IP** is a network protocol that defines how messages (data) are routed from one end of a network to the other, ensuring the data arrives correctly. TCP/IP describes rules for dividing messages into small pieces, called packets; providing addresses for each packet; checking for and detecting errors; sequencing packets; and regulating the flow of messages along the network.

TCP/IP has been adopted as the network standard for Internet communications. Thus, all hosts on the Internet follow the rules defined in this standard. When a computer sends data over the Internet, the data is divided into packets. Each packet contains the data, as well as the recipient (destination), the origin (sender), and the sequence information used to reassemble the data at the destination. Each packet travels along the fastest individual available path to the recipient's computer or mobile device via routers. This technique of breaking a message into individual packets, sending the packets along the best route available, and then reassembling the data is called **packet switching**.

Wi-Fi

Computers and devices that have the appropriate wireless capability can communicate via radio waves with other computers or devices using **Wi-Fi (wireless fidelity)**, which identifies any network based on the 802.11 standards. Developed by IEEE, **802.11** is a series of network standards that specify how two wireless devices communicate over the air with each other. Common standards include 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad, and 802.11af, with data transfer rates ranging from 11 Mbps to 7 Gbps. Many devices support multiple standards. For example, a designation of 802.11 ac/b/g/n on a computer, router, or other device indicates it supports those four standards (ac, b, g, and n).

Wi-Fi sometimes is referred to as **wireless Ethernet** because it uses techniques similar to the Ethernet standard to specify how physically to configure a wireless network. Thus, Wi-Fi networks easily can be integrated with wired Ethernet networks. When a Wi-Fi network accesses the Internet, it works in conjunction with the TCP/IP network standard. One popular use of the Wi-Fi network standard is in hot spots that offer mobile users the ability to connect to the Internet with their Wi-Fi-enabled wireless computers and devices.

Many homes and small businesses also use Wi-Fi to network computers and devices wirelessly. In open or outdoor areas free from interference, the computers or devices should be within 300 feet of a wireless access point or hot spot. In closed areas, the wireless network range is about 100 feet. To obtain communications at the maximum distances, you may need to install extra hardware to extend or strengthen a wireless signal.

LTE

LTE (Long Term Evolution) is a network standard that defines how high-speed cellular transmissions use broadcast radio to transmit data for mobile communications. Developed by

the Third Generation Partnership Project (3GPP), LTE has the potential of 100 Mbps downstream Rate (receiving data) and 30 Mbps upstream rate (sending data). Based on the TCP/IP network standard, LTE supports data, messaging, voice, and video transmissions. Two competing standards for LTE are WiMax (Worldwide Interoperability for Microwave Access) and UMB (Ultra Mobile Broadband).

Bluetooth

Bluetooth is a network protocol that defines how two Bluetooth devices use short-range radio waves to transmit data. The data transfers between devices at a rate of up to 3 Mbps. To communicate with each other, Bluetooth devices often must be within about 33 feet but can be extended to about 325 feet with additional equipment. A Bluetooth device contains a small chip that allows it to communicate with other Bluetooth devices. For computers and devices not Bluetooth-enabled, you can purchase a Bluetooth wireless port adapter that will convert an existing USB port into a Bluetooth port. Most current operating systems have built-in Bluetooth support. When connecting two devices using Bluetooth, the originating device sends a code to the connecting device. The codes must match to establish the connection.

Devices that share a Bluetooth connection are said to be paired. Most mobile devices and computers manufactured today are equipped with Bluetooth capability. One of the earliest and most popular uses of Bluetooth is to connect hands-free headsets to a mobile phone. Bluetooth has many additional uses, and device manufacturers are increasingly including Bluetooth technology.

Uses

You can use Bluetooth-enabled or Bluetooth-enhanced devices in many ways, including the following:

- Connect devices, such as mobile phones, portable media players, or GPS devices, with vehicle stereos, which use the vehicle's speakers to project.
- Use GPS receivers to send directions to a mobile phone or GPS-enabled device.
- Transfer photos wirelessly from a digital camera to a laptop or server.
- Play music on a smartphone through the speakers on a computer or other Bluetooth-enabled device.
- Send signals between video game accessories, video game devices, and a television.
- Establish a **PAN (personal area network).**
- Allow communications between a computer and devices, such as a keyboard, printer, Smart TV, or mobile phone. Connecting these devices enables you to print documents, share calendar appointments, and more.
- Replace wired communications devices, such as bar code readers, with wireless devices to enhance portability.
- Transmit data from a medical device, such as a blood glucose monitor, to a mobile phone or other device.
- Change the channel, pause a program, or schedule a recording using a Bluetooth-compatible or Bluetooth enabled television and remote control.

- ❖ Track objects that include tags or nodes used to send wireless signals read by a real-time location system.

UWB

UWB, which stands for **ultra-wideband**, is a network standard that specifies how two UWB devices use short-range radio waves to communicate at high speeds with each other. At distances of about 33 feet, the data transfer rate is 110 Mbps. At closer distances, such as about 6.5 feet, the transfer rate is at least 480 Mbps. UWB can transmit signals through doors and other obstacles.

Because of its high transfer rates, UWB is best suited for transmission of large files, such as video, graphics, and audio. Examples of UWB uses include locating and tracking inventory, equipment, or personnel (especially in remote or dangerous areas).

IrDA

Some devices, such as television remote controls, use the **IrDA (Infrared Data Association)** standard to transmit data wirelessly to each other via infrared (IR) light waves. The devices transfer data at rates from 115 Kbps (thousand bits per second) to 4 Mbps between their IrDA ports. Infrared requires line-of-sight transmission; that is, the sending device and the receiving device must be in line with each other so that nothing obstructs the path of the infrared light wave. Because Bluetooth and UWB do not require line-of-sight transmission, these technologies are more widespread than IrDA.

RFID

RFID (radio frequency identification) is a protocol that defines how a network uses radio signals to communicate with a tag placed in or attached to an object, an animal, or a person. The tag, called a transponder, consists of an antenna and a memory chip that contains the information to be transmitted via radio waves. Through an antenna, an RFID reader, also called a transceiver, reads the radio signals and transfers the information to a computer or computing device.

Depending on the type of RFID reader, the distance between the tag and the reader ranges from 5 inches to 300 feet or more. Readers can be handheld or embedded in an object, such as a doorway or a tollbooth.

NFC

NFC (near field communications) is a protocol, based on RFID, that defines how a network uses close-range radio signals to communicate between two devices or objects equipped with NFC technology. Examples of NFC-enabled devices include smartphones, digital cameras, televisions, and terminals. Credit cards, tickets, and NFC tags are examples of objects that also use NFC technology. An NFC tag is a chip that can store small amounts of data. NFC tags are

in a variety of objects, such as posters, ski lift tickets, business cards, stickers, and wristbands. For successful communications, the devices or objects touch or are placed within an inch or two of each other.

For example, you can touch two NFC-enabled phones together to transfer contacts, touch an NFC-enabled phone to an NFC tag to display a map, or hold an NFC-enabled phone near a parking meter to pay for parking. Contactless payment, such as the parking meter example, is a popular use of NFC technology.

NETWORK COMMUNICATIONS LINES

Dedicated Line. A **dedicated line** is a type of always-on physical connection that is established between two communications devices. Businesses often use dedicated lines to connect geographically distant offices. Dedicated lines can be either analogue or digital. Digital lines increasingly are connecting home and business users to networks around the globe because they transmit data and information at faster rates than analogue lines.

Digital dedicated lines include cable television lines, DSL, ISDN lines, FTTP, T-carrier lines, and ATM.

Cable

The **cable television (CATV)** network provides high-speed Internet connections, called cable Internet service. The CATV signal enters a building through a single line, usually a coaxial cable. This cable connects to a modem, which typically attaches to your computer via an Ethernet cable. Home and small business users often subscribe to cable Internet service.

DSL

DSL (Digital Subscriber Line) transmits on existing standard copper phone wiring. Some DSL installations include a dial tone, providing users with both voice and data communications. These DSL installations often require that filters be installed to reduce noise interference when voice communications share the same line. DSL is a popular digital line alternative for the small business or home user. ADSL is a popular type of DSL. As shown in, **ADSL (asymmetric digital subscriber line)** is a type of DSL that supports faster downstream rates than upstream rates. ADSL is ideal for Internet access because most users download more information from the Internet than they upload.

ISDN

Not as widely used today as in the past, **ISDN (Integrated Services Digital Network)** is a set of standards for digital transmission of data over standard copper phone lines. With ISDN, the same phone line that could carry only one computer signal now can carry three or more signals at once through the same line, using a technique called multiplexing.

FTTP

FTTP, which stands for **Fiber to the Premises**, uses fiber-optic cable to provide extremely

high-speed Internet access to a user's physical permanent location.

- **FTTH (Fiber to the Home)** provides home users with Internet access via fiber-optic cable.
- **FTTB (Fiber to the Building)** refers to small businesses that use fiber-optic cables to access the Internet.

With FTTP service, an optical terminal at your location receives the signals and transfers them to a router connected to a computer. As the cost of installing fiber decreases, more homes and businesses are expected to choose FTTP.

T-Carrier

A **T-carrier line** is any of several types of long-distance digital phone lines that carry multiple signals over a single communications line. Whereas a standard phone line carries only one signal, digital T-carrier lines use multiplexing so that multiple signals share the line. T-carrier lines provide very fast data transfer rates. Only medium to large companies usually can afford the investment in T-carrier lines because these lines are so expensive. The most popular T-carrier line is the T1 line. Businesses often use T1 lines to connect to the Internet. Home and small business users purchase fractional T1, in which they share a connection to the T1 line with other users. Fractional T1 is slower than a dedicated T1 line, but it also is less expensive. Users who do not have other high-speed Internet access in their areas can opt for fractional T1. With fractional T1 lines, the data transfer rates become slower as additional users are added.

A T3 line is equal in speed to 28 T1 lines. T3 lines are quite expensive. Main users of T3 lines include large corporations, phone companies, and ISPs connecting to the Internet backbone. The Internet backbone itself also uses T3 lines.

ATM

ATM (Asynchronous Transfer Mode) is a service that carries voice, data, video, and media at very high speeds. Phone networks, the Internet, and other networks with large amounts of traffic use ATM. Some experts predict that ATM eventually will become the Internet standard for data transmission, replacing T3 lines.

7.4 Communication Devices

A **communications device** is any type of hardware capable of transmitting data, instructions, and information between a sending device and a receiving device. **They are electronic devices that are used to transmit network data, to boost signals or to route data to their destination.** At the sending end, a communications device sends the data, instructions, or information from the sending device to transmission media. At the receiving end, a communications device receives the signals from the transmission media.

The following pages describe a variety of communications devices: modems, wireless access points, routers, network cards, and hubs and switches.

Modems

A broadband modem, also called a **digital modem**, is a communications device that sends and receives data and information to and from a digital line. Modem stands for **Mo**dulator and **Dem**odulator. Data in a computer are formatted as digital signals. However, because telephone lines were designed to transmit the human voice, they format data as analogue signals. For communication between computers to take place over telephone lines, the digital signals must be converted to an analogue signal before it is transmitted. After its journey over the telephone lines, the analogue signals must be reconverted back to a digital signal so that it can be used by the receiving computer. The process of converting digital signals to analogue signals is called **modulation**. **Demodulation** is the process of reconverting the analogue signals back to digital signals.

Three types of broadband modems are cable modems, DSL modems, and ISDN modems. These modems typically include built-in Wi-Fi connectivity. A **cable modem** is a broadband modem that sends and receives digital data over the CATV network. To access the Internet using the CATV service, the CATV provider installs a splitter inside your house. From the splitter, one part of the cable runs to your televisions and the other part connects to the cable modem. Many CATV providers include a cable modem as part of the installation; some offer a rental plan, and others require that you purchase one separately. A cable modem usually is an external device, in which one end of a cable connects to a CATV wall outlet and the other end plugs in a port on a computer.

A **DSL modem** is a broadband modem that sends digital data and information from a computer to a DSL line and receives digital data and information from a DSL line. Similarly, an **ISDN modem** is a broadband modem that sends digital data and information from a computer to an ISDN line and receives digital data and information from an ISDN line. DSL and ISDN modems usually are external devices, in which one end connects to the phone line and the other end connects to a port on the computer.

Other kinds of Modems include **Ethernet modems** that plug into the network card in the computer, and **wireless modems** that connect to a computer using a **wireless** LAN (WLAN). Some modems offer dual Ethernet and **USB** connection. There are also routers with integrated **ADSL** modem.

Wireless Modems

Some mobile users have a wireless modem that uses a mobile service provider's network to connect to the Internet wirelessly from a computer or mobile device. Wireless modems, which have an external or built-in antenna, are available as USB adapters and other devices. Some smartphones also can function as a wireless modem, called a mobile hot spot, when tethered to a personal computer or mobile device.

Wireless Access Points

A wireless access point (**WAP**) is a central communications device that allows computers and devices to transfer data wirelessly among themselves or to a wired network using wireless technologies, such as Wi-Fi. Wireless access points have high-quality internal or external antennas for optimal signals. For the best signal, some manufacturers suggest positioning the wireless access point at the highest possible location and using a device to strengthen your wireless signal.

Routers

A router is a communications device that connects multiple computers or other routers together and transmits data to its correct destination on a network. A router can be used on a network of any size. On the largest scale, routers along the Internet backbone forward data packets to their destination using the fastest available path. For smaller business and home networks, a router allows multiple computers and mobile devices to share a single broadband Internet connection, such as through a cable modem or DSL modem.

If the network has a separate router, it connects to the router via a cable. Similarly, if the network has a separate wireless access point, it connects to the router via a cable. Many users, however, opt for routers that provide additional functionality.

- A wireless router is a device that performs the functions of a router and also a wireless access point.
- A broadband router is a device that performs the functions of a router and also a broadband modem.
- A broadband wireless router is a device that performs the functions of a router, a wireless access point, and a cable or DSL modem.

- A mobile broadband wireless router is a device that performs the functions of a router, a wireless access point, and a wireless modem. Consumers use mobile broadband wireless routers to create a mobile hot spot.

Gateways

It is a generic term for any device or software used to join two dissimilar networks by converting data sent from one network to a format compatible to the receiving network. A gateway is a node in a computer network, a key stopping point for data on its way to or from other networks. By using gateways, we are able to communicate and send data back and forth.

Bridge

A device used to connect or join two similar networks.

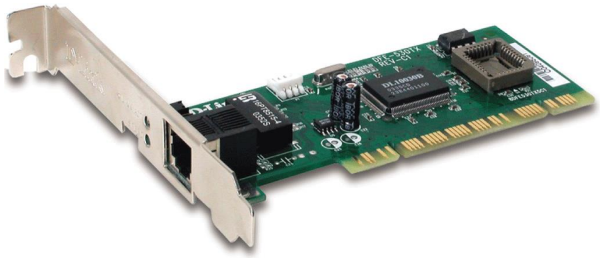
Repeaters

A network device that can boost the strength of the signal that carries data over a network topology when distance between two nodes exceeds the range of their connecting links. For instance, a CAT5 twisted pair network cable has signal strength of up to 100m and a Cat6 twisted pair network cable

Network Cards

A network card, sometimes called a **network interface card (NIC** pronounced nick), is a communications device that enables a computer or device that does not have built-in networking capability to access a network. The network card coordinates the transmission and receipt of data, instructions, and information to and from the computer or device containing the network card. Network cards are available in a variety of styles. A network card for a desktop is an adapter card that has a port to which a cable connects.

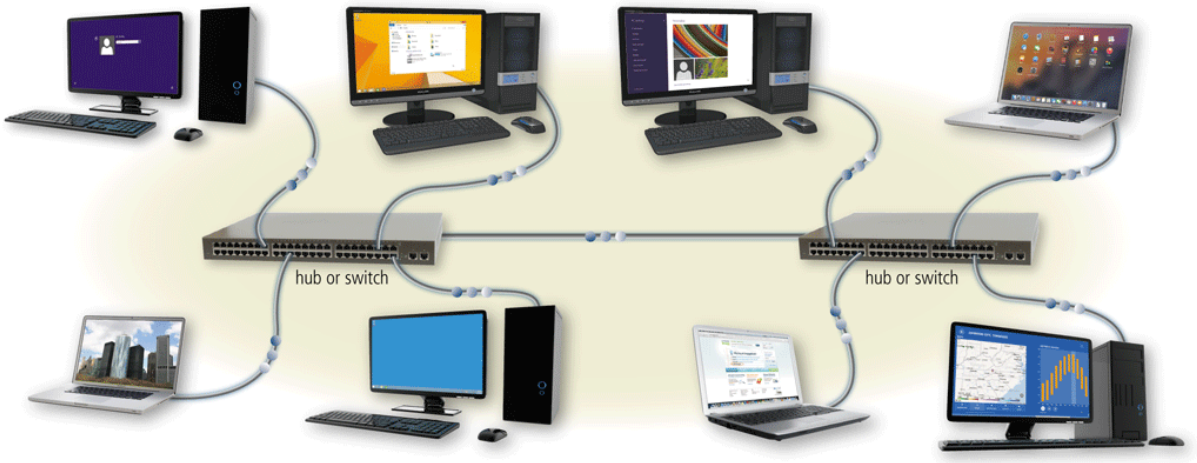
A network card for mobile computers and devices is in the form of a USB adapter or other device. A network card follows the guidelines of a particular network communications standard, such as Ethernet or token ring.



Hubs and Switches

Today, thousands of computer networks exist, ranging from small networks operated by home users to global networks operated by widespread telecommunications firms. Interconnecting these many types of networks requires various types of communications devices. A hub or switch is a device that provides a central point for cables in a network. Larger networks typically use a hub, while smaller networks use a switch. Some hubs and/or switches include

routers. That is, the hub or switch receives data from many directions and then forwards it to one or more destinations.



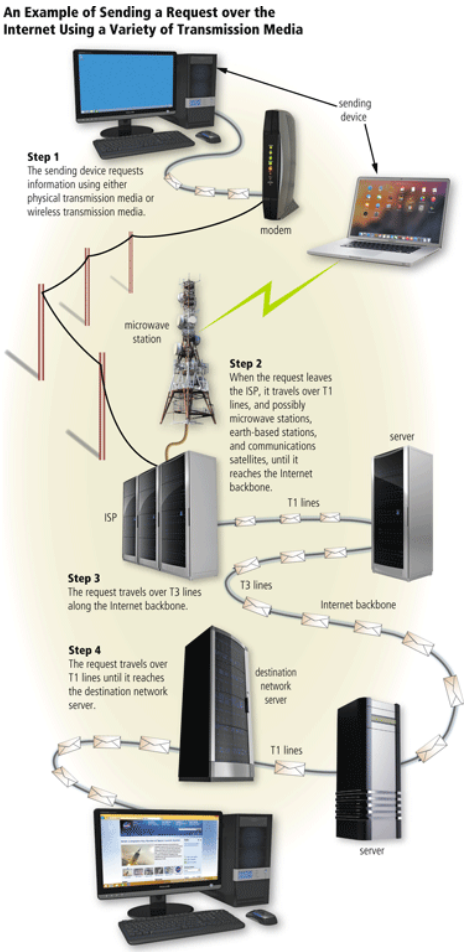
Planning and Designing Your Home Network

A home network enables you to use a common Internet connection among many computers and mobile devices. Other uses include connecting entertainment devices, such as digital video recorders (DVRs) and televisions, to the Internet and establishing a connection between devices in order to play multiplayer games. Before purchasing hardware, or contracting network expert to set up your network, consider how your network will be used, and by whom. Ask yourself the following questions:

- What devices will connect to the network? The number of devices, as well as the operating system or platform on which the devices operate will determine the speed and strength needed to run your wireless network.
- How large of a range do you need, and where will most of the use take place? If you have a small apartment, your needs will differ from those with a large home.
- How many users typically will be using the network, how will they use it, and for what purposes? The number of users affects the capabilities of the network and determines whether you need to define permissions for certain users or devices.
- How secure do you need your network? Hiding the network name, requiring passwords, or having a user with network administration capabilities can help ensure your network is safe from unauthorized use.

7.5 Transmission Media

Transmission media consist of materials or substances capable of carrying one or more communications signals. When you send data from a computer or mobile device, the signal that carries the data may travel over various transmission media. This is especially true when the transmission spans a long distance. Although many media and devices are involved, the entire communications process could take less than one second.

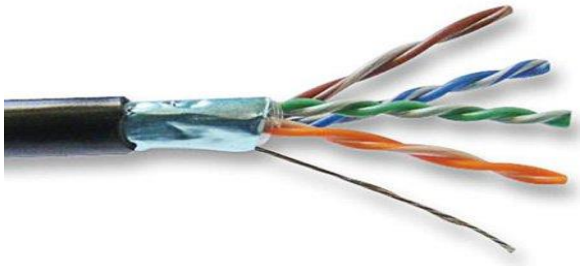


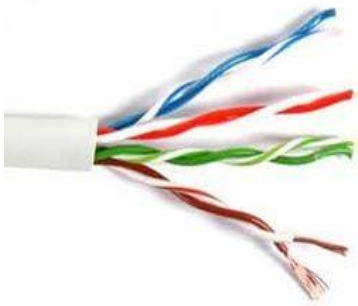
PHYSICAL TRANSMISSION MEDIA

Physical transmission media use wire, cable, and other tangible materials to send communications signals. These wires and cables typically are used underground or within or between buildings. Ethernet and token ring LANs often use physical transmission media.

Twisted-Pair Cable

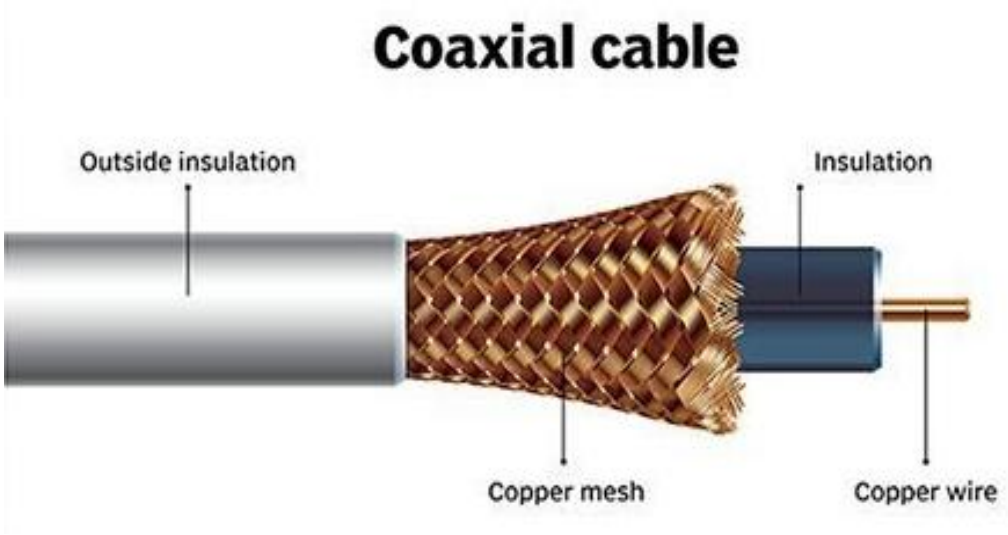
One of the more widely used transmission media for network cabling and landline phone systems is twisted pair cable. **Twisted-pair cable** consists of one or more twisted pair wires bundled together. Each twisted-pair wire consists of two separate insulated copper wires that are twisted together. The wires are twisted together to reduce **noise**, which is an electrical disturbance that can degrade communications. They are two types of twisted pair cables: **Shielded twisted pair** cable and **Unshielded twisted pair** cable





Coaxial Cable

Coaxial cable, often referred to as coax (pronounced KO-ax), consists of a single copper wire surrounded by at least three layers: (1) an insulating material, (2) a woven or braided metal mesh, and (3) a plastic outer coating. CATV network wiring often uses coaxial cable because it can be cabled over longer distances than twisted-pair cable. Most of today's computer networks, however, do not use coaxial cable because other transmission media, such as fibre-optic cable, transmit signals at faster rates.



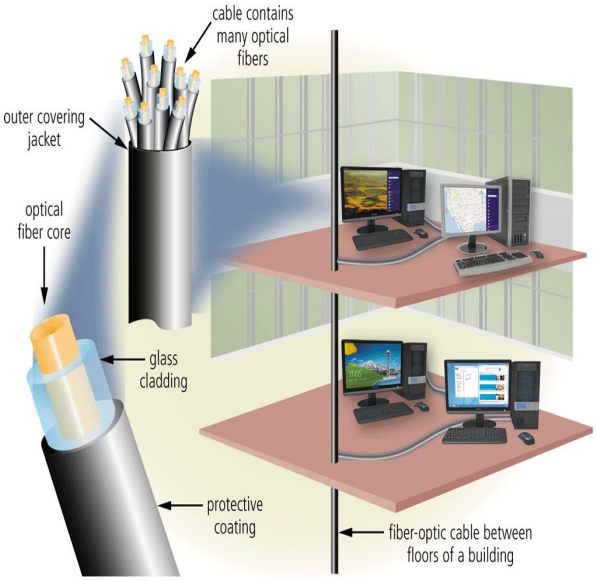
Fibre-Optic Cable

The core of a **fibre-optic cable** consists of dozens or hundreds of thin strands of glass or plastic that use light to transmit signals. Each strand, called an optical fibre, is as thin as a human hair. Inside the fibre-optic cable, an insulating glass cladding and a protective coating surround each optical fibre.

Fibre-optic cables have the following advantages over cables that use wire, such as twisted-pair and coaxial cables:

- Capability of carrying significantly more signals than wire cables
- Faster data transmission
- Less susceptible to noise (interference) from other devices, such as a copy machine
- Better security for signals during transmission because they are less susceptible to noise
- Smaller size (much thinner and lighter weight)

Disadvantages of fibre-optic cable are it costs more than twisted-pair or coaxial cable and can be difficult to install and modify. Despite these limitations, many phone companies replaced original analogue phone lines with fibre-optic cables, enabling them to offer fibre-optic Internet access to home and business users. Businesses also use fibre-optic cables in high-traffic networks or as the backbone in a network.



Wireless Transmission Media

Wireless transmission media send communications signals through the air or space. Many users opt for wireless transmission media because it is more convenient than installing cables. In addition to convenience, businesses use wireless transmission media in locations where it is impossible to install cables.

Types of wireless transmission media used in communications include infrared, broadcast radio, cellular radio, microwaves, and communications satellites.

Infrared

Infrared (IR) is a wireless transmission medium that sends signals using infrared light waves. Mobile computers and devices, such as a mouse, printer, and smartphone, may have an IrDA port that enables the transfer of data from one device to another using infrared light waves.

Broadcast Radio

Broadcast radio is a wireless transmission medium that distributes radio signals through the air over long distances, such as between cities, regions, and countries, and short distances, such as within an office or home. For radio transmissions, you need a transmitter to send the broadcast radio signal and a receiver to accept it. To receive the broadcast radio signal, the receiver has an antenna that is located in the range of the signal.

Some networks use a transceiver, which both sends and receives signals from wireless devices. Broadcast radio is slower and more susceptible to noise than physical transmission media, but it provides flexibility and portability. Bluetooth, UWB, and Wi-Fi communications

technologies discussed earlier in this unit use broadcast radio signals. Bluetooth and UWB are alternatives to infrared communications, with the latter designed for high-bandwidth transmissions. Hot spots use Wi-Fi.

Cellular Radio

Cellular radio is a form of broadcast radio that is in wide use for mobile communications, specifically wireless modems and mobile phones. Telecom Networks such as MTN and Vodafone use cellular Radio to transmit data. A mobile phone uses high-frequency radio waves to transmit voice and digital data messages. Because only a limited number of radio frequencies exist, mobile service providers reuse frequencies so that they can
accommodate the large number of users. Some users install an amplifier or booster to improve the signal strength.

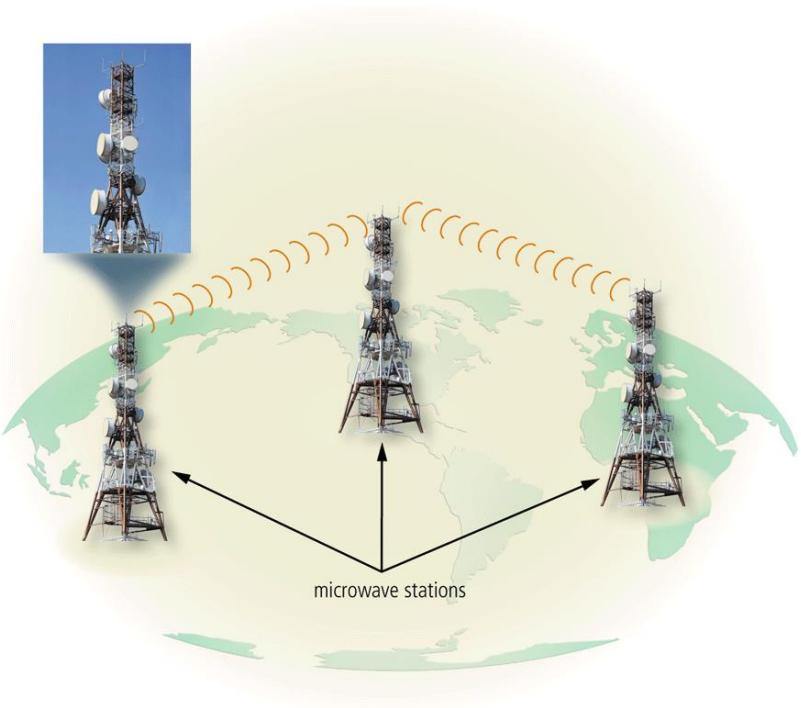
Several categories of cellular radio transmissions exist, defining the development of cellular networks. Although the definitions of these categories may vary by mobile service providers, below are some general guidelines:

- 1G (first generation of cellular transmissions). Analog data transfer at speeds up to 14.4 Kbps
- 2G (second generation of cellular transmissions). Digital data transfer at speeds from 9.6 Kbps to 144 Kbps. Improved voice transmissions, added data communications, and added **SMS (short message service**) or text messaging services. Standards include GSM (Global System for Mobile Communications) and GPRS (General Packet Radio Service)
- 3G (third generation of cellular transmissions). Digital data transfer at speeds from 144 Kbps to 3.84 Mbps. Improved data transmissions, added MMS (multimedia message services). Standards include UMTS (Universal Mobile Telecommunications System), CDMA (Code Division Multiple Access), EDGE (Enhanced Data GSM Environment), and EVDO (Evolution Data Optimized)
- 4G (fourth generation of cellular transmissions). Digital data transfer at speeds up to 100 Mbps. Improved video transmissions. Standards include Long Term Evolution (LTE), Ultra Mobile Broadband (UMB), and IEEE 802.16 (WiMAX)
- 5G (fifth generation of cellular transmissions). Future generation of cellular transmissions. Expected to improve bandwidth. Expected to provide artificial intelligence capabilities on wearable devices

Microwaves

Microwaves are radio waves that provide a high-speed signal transmission. Microwave

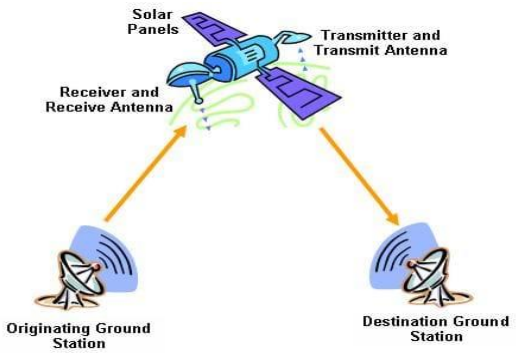
transmission, often called fixed wireless, involves sending signals from one microwave station to another. A microwave station is an earth-based reflective dish that contains the antenna, transceivers, and other equipment necessary for microwave communications. As with infrared, microwaves use line-of-sight transmission. To avoid possible obstructions, such as buildings or mountains, microwave stations often sit on the tops of buildings, towers, or mountains.



Microwave transmission typically is used in environments where installing physical transmission media is difficult or impossible and where line-of-sight transmission is available. For example, microwave transmission is used in wide-open areas, such as deserts or lakes, between buildings in a close geographic area, or to communicate with a satellite. Current users of microwave transmission include universities, hospitals, city governments, CATV providers, and phone companies. Homes and small businesses that do not have other high-speed Internet connections available in their area also opt for lower-cost fixed wireless plans.

Communications Satellite

A **communications satellite** is a space station that receives microwave signals from an earth-based station, amplifies (strengthens) the signals, and broadcasts the signals back over a wide area to any number of earth-based stations. These earth-based stations often are microwave stations. Other devices, such as smartphones and GPS receivers, also can function as earth-based stations. Transmission from an earth-based station to a satellite is an **uplink**. Transmission from a satellite to an earth-based station is a **downlink**.



Applications such as air navigation, television and radio broadcasts, weather forecasting, videoconferencing, GPS, and Internet connections use communications satellites. With the proper satellite dish and a satellite modem, consumers can access the Internet using satellite technology.

GPS

A **GPS** (global positioning system) is a navigation system that consists of one or more earth-based receivers that accept and analyse signals sent by satellites in order to determine the receiver's geographic location.

Many mobile devices, such as smartphones, have GPS capability built into the device or as an add-on feature. Some users carry a handheld GPS receiver; others mount a receiver to an object such as an automobile, a boat, an airplane, farm and construction equipment, or a computer or mobile device. A GPS receiver is a handheld, mountable, or embedded device that contains an antenna, a radio receiver, and a processor. Many include a screen display that shows an individual's location on a map.

UNIT 8: COMPUTER SECURITY, SAFETY, ETHICS AND PRIVACY

8.1 Unit objectives

After reading this unit, you will be able to:

1. Define the term, digital security risks, and briefly describe the types of cybercriminals
2. Describe various types of Internet and network attacks and explain ways to safeguard against these attacks
3. Discuss techniques to prevent unauthorized computer access and use
4. Explain ways that software manufacturers protect against software piracy
5. Discuss how encryption, digital signatures, and digital certificates work
6. Identify safeguards against hardware theft, vandalism, and failure
7. Explain options available for backing up
8. Identify risks and safeguards associated with wireless communications
9. Recognize issues related to information accuracy, intellectual property rights, codes of conduct, and green computing
10. Discuss issues surrounding information privacy, including electronic profiles, cookies, phishing, spyware and adware, social engineering, privacy laws, employee monitoring, and content filtering

8.1 Computer Security Risk

Today, people rely on technology to create, store, and manage their critical information. Thus, it is important that computers and mobile devices, along with the data and programs they store, are accessible and available when needed. It also is crucial that users take measures to protect or safeguard their computers, mobile devices, data, and programs from loss, damage, and misuse. For example, organizations such as banks must ensure that sensitive data and information, such as credit records, employee and customer data, and purchase information, is secure. Home users must ensure that their credit card numbers are secure when they make online purchases.

A **digital security risk** is any event or action that could cause a loss of or damage to computer or mobile device hardware, software, data, information, or processing capability. The more common **digital security risks include Internet and network attacks, unauthorized access and use, hardware theft, software theft, information theft, and system failure**. While some breaches to digital security are accidental, many are intentional. Some intruders do not disrupt a computer or device's functionality; they merely access data, information, or programs on the computer or mobile device before signing out. Other intruders indicate some evidence of their presence either by leaving a message or by deliberately altering or damaging data.

Cybercrime

An intentional breach to digital security often involves a deliberate act that is against the law.

Any illegal act involving the use of a computer or related devices generally is referred to as a **computer crime**. The term **cybercrime** refers to online or Internet-based illegal acts such as distributing malicious software or committing identity theft. Software used by cybercriminals sometimes is called **crimeware**.

Perpetrators of cybercrime typically fall into one of these basic categories: **hacker, cracker, script kiddie, corporate spy, unethical employee, cyberextortionist, and cyberterrorist**.

- The term **hacker**, although originally a complimentary word for a computer enthusiast, now has a derogatory meaning and refers to someone who accesses a computer or network illegally. Some hackers claim the intent of their security breaches is to improve security.
- A **cracker** also is someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious action. Both hackers and crackers have advanced computer and network skills.
- A **script kiddie** has the same intent as a cracker but does not have the technical skills and knowledge. Script kiddies often use prewritten hacking and cracking programs to break into computers and networks.
- Some **corporate spies** have excellent computer and networking skills and are hired to break into a specific computer and steal its proprietary data and information, or to help identify security risks in their own organization. Unscrupulous companies hire corporate spies, a practice known as corporate espionage, to gain a competitive advantage.
- **Unethical employees** may break into their employers' computers for a variety of reasons. Some simply want to exploit a security weakness. Others seek financial gains from selling confidential information. Disgruntled employees may want revenge.
- A **cyberextortionist** is someone who demands payment to stop an attack on an organization's technology infrastructure. These perpetrators threaten to expose confidential information, exploit a security flaw, or launch an attack that will compromise the organization's network —if they are not paid a sum of money.
- A **cyberterrorist** is someone who uses the Internet or network to destroy or damage computers for political reasons. The cyberterrorist might target the nation's air traffic control system, electricity-generating companies, or a telecommunications infrastructure. The term, cyberwarfare, describes an attack whose goal ranges from disabling a government's computer network to crippling a country. Cyberterrorism and cyberwarfare usually require a team of highly skilled individuals, millions of dollars, and several years of planning.

Some organizations hire individuals previously convicted of computer crimes to help identify security risks and implement safeguards because these individuals know how criminals attempt to breach security.

Security Tools

To protect your computers and mobile devices, you can use one or more security tools. Security tools include **personal firewalls, antivirus programs, malware removers, and Internet filters**. Although some of these tools are included with the operating system, you also can purchase stand-alone programs that offer improvements or added functionality.

Personal Firewall

A **personal firewall** is a security tool that detects and protects a personal computer and its data from unauthorized intrusions. Personal firewalls constantly monitor all transmissions to and from a computer or mobile device and may inform a user of attempted intrusions. When connected to the Internet, your computer or mobile device is vulnerable to attacks from hackers who try to access a computer or network illegally. These attacks may destroy your data, steal information, damage your computer, or carry out some other malicious action.

What is a hardware firewall?

A hardware firewall is a device intended to stop network intrusions before they attempt to affect your computer or network maliciously. Many routers also can function as a hardware firewall.

Security Suite: A security suite is a collection of individual security tools available together as a unit. These programs often are called Internet security programs

8.2 Internet and Network attacks

Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises. In an organization, network administrators usually take measures to protect a network from security risks. On the Internet, where no central administrator is present, the security risk is greater.

Internet and network attacks that jeopardize security include **malware, botnets, denial of service attacks, back doors, and spoofing**.

Malware

Malware, short for **malicious software**, consists of programs that act without a user's knowledge and deliberately alter the operations of computers and mobile devices. Some malware contains characteristics in two or more classes. For example, a single threat could contain elements of a **virus, worm, and trojan horse**. Malware can deliver its **payload**, or destructive event or prank, on a computer or mobile device in a variety of ways. These include when a user opens an infected file, runs an infected program, connects an unprotected computer or mobile device to a network, or when a certain condition or event occurs, such as the computer's clock changing to a specific date. A common way that computers and mobile

devices become infected with viruses and other malware is through users opening infected email attachments.

Common types of Malware

Virus: A potentially damaging program that affects, or infects, a computer or mobile device negatively by altering the way the computer or device works without the user's knowledge or permission. A computer **virus** is a potentially damaging program that affects a computer or device negatively by altering the way it works. This occurs without the user's knowledge or permission. Once the virus is in a computer or device, it can spread and may damage your files, programs and apps, and operating system.

Studies show that malware can infect an unprotected computer within minutes after connecting to the Internet. Due to the increasing threat of viruses attacking your computer, it is more important than ever to protect your computer from viruses and other malware.

Viruses do not generate by chance. **The programmer of a virus, known as a virus author**, intentionally writes a virus program. Writing a virus program usually requires significant programming skills. The virus author ensures the virus can replicate itself, conceal itself, monitor for certain events, and then deliver its payload. A payload is the destructive event or prank the virus delivers. Viruses can infect all types of computers and devices.

Most variations of viruses have two phases involved in their execution: infection and delivery. The first step in the infection phase is activation of the virus. The most common way viruses spread is by users running infected programs or apps. During the infection phase, viruses typically perform one or more of the following actions:

a. First, a virus replicates by attaching itself to program files. A macro virus hides in a macro, which is a standard feature of many productivity applications, such as word processing and spreadsheet apps. A boot sector virus targets the computer's start-up files. A file virus attaches itself to program files. The next time an infected program or app is run, the virus executes and infects the computer or device.
b. Viruses conceal themselves to avoid detection. A stealth virus disguises itself by hiding in fake code sections, which it inserts within working code in a file. A polymorphic virus actually changes its code as it delivers the infection.
c. Finally, viruses watch for a certain condition or event and activate when that condition or event occurs. The event might be starting the computer or device, or reaching a date on the system clock. A logic bomb activates when it detects a specific condition. A time bomb is a logic bomb that activates on a particular date or time. If the triggering condition does not exist, the virus simply replicates.

Worm

A program that copies itself repeatedly, for example in memory or on a network, using up resources and possibly shutting down the computer, device, or network. A worm resides in

active memory and replicates itself over a network to infect computers and devices, using up system resources.

Trojan Horse

A program that hides within or looks like a legitimate program. Unlike a virus or worm, a trojan horse does not replicate itself to other computers or devices. A trojan horse is a destructive program disguised as a real program, such as a screen saver. When a user runs a seemingly innocent program, a trojan horse hiding inside can capture information, such as user names and passwords, from your computer or enable someone to control your computer remotely.

Rootkit

A program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device. A rootkit is a program that easily can hide and allow someone to take full control of your computer from a remote location, often for nefarious purposes. For example, a rootkit can hide in a folder on your computer. The folder appears empty because the rootkit has instructed your computer not to display the contents of the folder. Rootkits can be very dangerous and often require special software to detect and remove.

Spyware

A program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online.

Adware

A program that displays an online advertisement in a banner, pop-up window, or pop-under window on webpages, email messages, or other Internet services.

Botnets

A **botnet**, or zombie army, is a group of compromised computers or mobile devices connected to a network, such as the Internet, that are used to attack other networks, usually for nefarious purposes. A compromised computer or device, known as a **zombie**, is one whose owner is unaware the computer or device is being controlled remotely by an outsider. **A bot is a program that performs a repetitive task on a network**. Cybercriminals install malicious bots on unprotected computers and devices to create a botnet. The perpetrator then uses the botnet to send spam via email, spread viruses and other malware, or commit a **Distributed denial of service** attack.

Denial of Service Attacks

A **denial of service attack** (**DoS attack**) is an assault whose purpose is to disrupt computer access to an Internet service, such as the web or email. Perpetrators carry out a DoS attack in a variety of ways. For example, they may use an unsuspecting computer to send an influx of confusing data messages or useless traffic to a computer network. The victim computer network slows down considerably and eventually becomes unresponsive or unavailable, blocking legitimate visitors from accessing the network.

A more devastating type of DoS attack is the **distributed DoS attack (DDoS attack)** in which a zombie army is used to attack computers or computer networks. DDoS attacks have been able to stop operations temporarily at numerous websites, including powerhouses such as Yahoo!, eBay, Amazon.com, and CNN.com.

The damage caused by a DoS or DDoS attack usually is extensive. During the outage, retailers lose sales from customers, news websites and search engines lose revenue from advertisers, and time-sensitive information may be delayed. Repeated attacks could tarnish reputations, causing even greater losses.

Back Doors

A **back door** is a program or set of instructions in a program that allows users to bypass Security controls when accessing a program, computer, or network. Once perpetrators gain access to unsecure computers, they often install a back door or modify an existing program to include a back door, which allows them to continue to access the computer remotely without the user's knowledge. A rootkit can be a back door. Some worms leave back doors, which have been used to spread other worms or to distribute spam from the unsuspecting victim computers. Programmers often build back doors into programs during system development.

These back doors save development time because the programmer can bypass security controls while writing and testing programs. Similarly, a computer repair technician may install a back door while troubleshooting problems on a computer. If a programmer or computer repair technician fails to remove a back door, a perpetrator could use the back door to gain entry to a computer or network.

Spoofing

Spoofing is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network. Two common types of spoofing schemes are IP and email spoofing.

- **IP spoofing** occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source. Perpetrators of IP spoofing trick their victims into interacting with the phony website. For example, the victim may provide confidential information or download files containing viruses, worms, or other malware.

- **Email spoofing** occurs when the sender's address or other components of an email header are altered so that it appears that the email message originated from a different sender. Email spoofing commonly is used in virus hoaxes, spam, and phishing scams

8.2.2 Internet and Network Safeguards.

Safeguards against Internet and Network Attacks
Methods that protect computers, mobile devices, and networks from attacks include the following:

- Use antivirus software.
- Be suspicious of unsolicited email attachments.
- Scan removable media for malware before using it.
- Implement firewall solutions.
- Back up regularly.

Antivirus Programs
To protect a computer from virus attacks, users should install an antivirus program and keep it updated by purchasing revisions or upgrades to the software. An **antivirus program** protects a computer against viruses by identifying and removing any computer viruses found in memory, on storage media, or on incoming files. Antivirus programs scan for programs that attempt to modify a computer's start-up files, the operating system, and other programs that normally are read from but not modified. In addition, many antivirus programs automatically scan files downloaded from the web, email attachments, opened files, and all types of removable media inserted in the computer or mobile device.

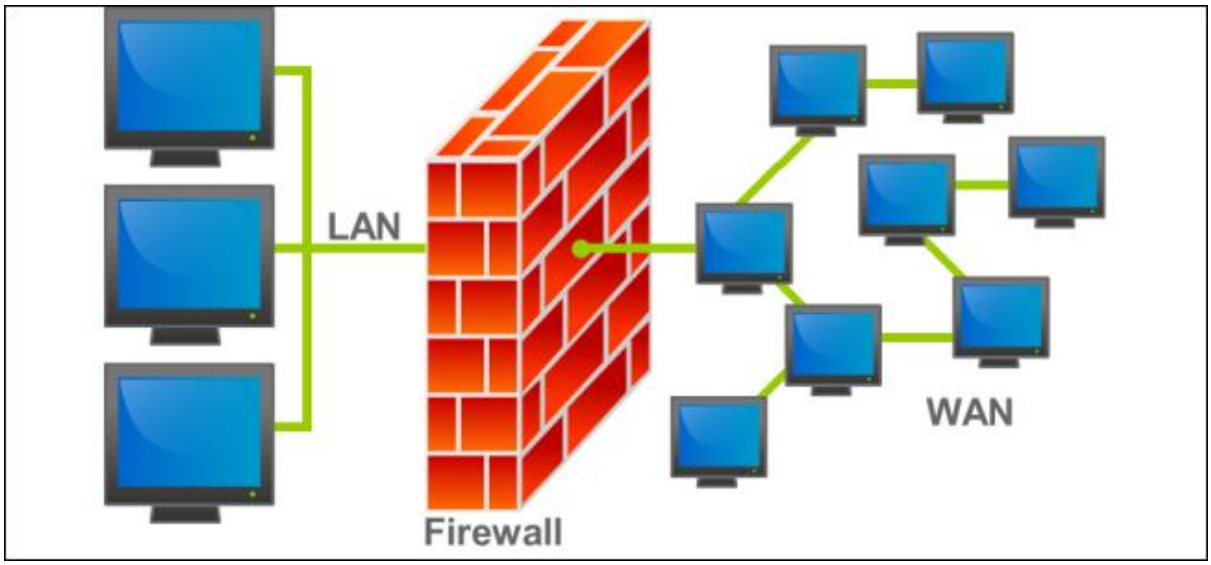
If an antivirus program identifies an infected file, it attempts to remove the malware. If the antivirus program cannot remove the infection, it often quarantines the infected file. A **quarantine** is a separate area of a hard drive that holds the infected file until the infection can be removed. This step ensures other files will not become infected.

Quarantined files remain on your computer or mobile device until you delete them or restore them. Most antivirus programs also include protection against other malware, such as worms, Trojan horses, and spyware. When you purchase a new computer, it may include a trial version of antivirus software. Many email servers also have antivirus programs installed to check incoming and outgoing email messages for viruses and other malware.

Firewalls
A **firewall** is hardware and/or software that protects a network's resources from intrusion by users on another network, such as the Internet. All networked and online users should implement a firewall solution. Organizations use firewalls to protect network resources from outsiders and to restrict employees' access to sensitive data, such as payroll or personnel

records. They can implement a firewall solution themselves or outsource their needs to a company specializing in providing firewall protection.

Large organizations often route all their communications through a **proxy server**, which typically is a component of the firewall. A **proxy server** is a server outside the organization's network that controls which communications pass in and out of the organization's network. That is, a proxy server carefully screens all incoming and outgoing messages. Proxy servers use a variety of screening techniques. Some check the domain name or IP address of the message for legitimacy.



Categories of firewalls

- Hardware Firewall
- Software Firewall
- Packet-Filter Firewall
- Proxy Firewall
- Application Gateways
- Circuit-Level Gateways
- Stateful Packet-Inspection (SPI)

Home and small/home office users often protect their computers with a personal firewall. A **personal firewall** is a software firewall that detects and protects a personal computer and its data from unauthorized intrusions. Personal firewalls constantly monitor all transmissions to and from the computer and may inform a user of any attempted intrusions. Both Windows and Mac operating systems include firewall capabilities, including monitoring Internet traffic to and from installed applications.

Some small/home office users purchase a hardware firewall, such as a router or other device that has a built-in firewall, in addition to or instead of a personal firewall. Hardware firewalls stop malicious intrusions before they attempt to affect your computer or network.

Spyware, Adware, and Other Malware Removers

Spyware is a type of program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online. Some vendors or employers use spyware to collect information about program usage or employees. Internet advertising firms often collect information about users' web browsing habits. Spyware can enter your computer when you install a new program, through a graphic on a webpage or in an email message, or through malware.

Adware is a type of program that displays an online advertisement in a banner or pop-up or pop-under window on webpages, email messages, or other Internet services. Sometimes, Internet advertising firms hide spyware in adware.

A **spyware remover** is a type of program that detects and deletes spyware and similar programs.

An **adware remover** is a program that detects and deletes adware. Malware removers detect and delete spyware, adware, and other malware.

Internet Filters

Filters are programs that remove or block certain items from being displayed. Four widely used Internet filters are anti-spam programs, web filters, phishing filters, and pop-up and pop-under blockers.

Anti-Spam Programs

Spam is an unsolicited email message or posting sent to many recipients or forums at once. Spam is considered Internet junk mail. The content of spam ranges from selling a product or service, to promoting a business opportunity, to advertising offensive material. Spam also may contain links or attachments that contain malware.

An **anti-spam program** is a filtering program that attempts to remove spam before it reaches your inbox or forum. If your email program does not filter spam, many anti-spam programs are available at no cost on the web. ISPs often filter spam as a service for their subscribers. Email services such as gmail, and yahoo mail have anti-spam programs integrated into them.

Web Filters: Web filtering software is a program that restricts access to certain material on the web. Some restrict access to specific websites; others filter websites that use certain words or phrases. Many businesses use web filtering software to limit employee's web access. Some schools, libraries, and parents use this software to restrict access to websites that are not educational.

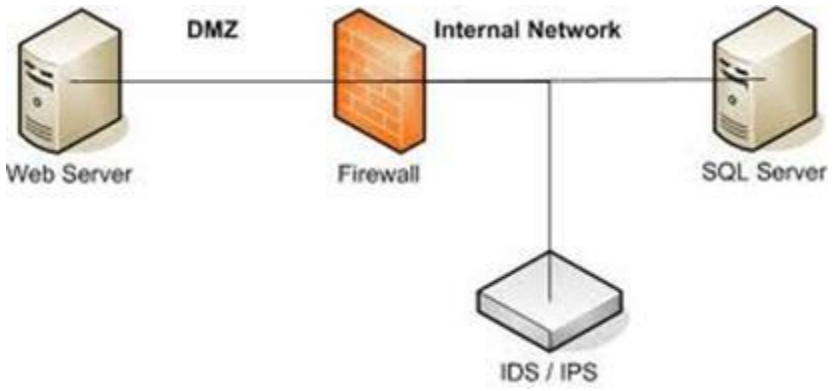
Phishing Filters: **Phishing** is a scam in which a perpetrator sends an official looking email message that attempts to obtain your personal and/or financial information. Some phishing messages ask you to reply with your information; others direct you to a phony website or a pop-up or pop-under window that looks like a legitimate website, which then collects your information. A **phishing filter** is a program that warns or blocks you from potentially fraudulent or suspicious websites. Some browsers include phishing filters.

Pop-Up and Pop-Under Blockers

A pop-up ad is an Internet advertisement that suddenly appears in a new window on top of a webpage. Similarly, a pop-under ad is an Internet advertisement that is hidden behind the browser window so that it will be viewed when users close their browser windows. A **pop-up blocker** or **pop-under blocker** is a filtering program that stops pop-up or pop-under ads from displaying on webpages. Many browsers include these blockers. You also can download pop-up and pop-under blockers from the web at no cost.

Intrusion Detection System (IDS)

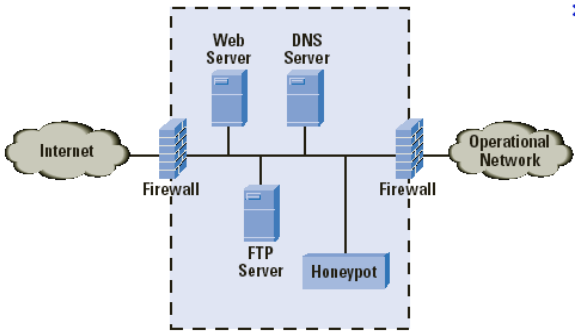
Intrusion Detection (ID) is the process of monitoring for and identifying attempted unauthorized system access or manipulation. An ID system gathers and analyses information from diverse areas within a computer or a network to identify possible security breaches which include both intrusions (attack from outside the organization) and misuse (attack from within the organization).



An Intrusion Detection System (IDS) is yet another tool in the network administrator's computer security arsenal. It inspects all the inbound and outbound network activity. The IDS identifies any suspicious pattern that may indicate an attack the system and acts as a security check on all transactions that take place in and out of the system.

Honeypots

A **honeypot** is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked.



8.3 Unauthorized Access and Use

Unauthorized access is the use of a computer or network without permission. Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities. Home and business users can be a target of unauthorized access and use. Unauthorized use includes a variety of activities: an employee using an organization's computer to send personal email messages, an employee using the organization's word processing software to track his or her child's soccer league scores, or a perpetrator gaining access to a bank computer and performing an unauthorized transfer.

Safeguards against Unauthorized Access and Use

Organizations take several measures to help prevent unauthorized access and use. At a minimum, they should have a **written acceptable use policy (AUP)** that outlines the activities for which the computer and network may and may not be used. An organization's AUP should specify the acceptable use of technology by employees for personal reasons. Some organizations prohibit such use entirely. Others allow personal use on the employee's own time, such as a lunch hour. Whatever the policy, an organization should document and explain it to employees. The AUP also should specify the personal activities, if any, that are allowed on company time. For example, can employees check personal email messages or respond to personal text messages during work hours?

To protect your personal computer from unauthorized intrusions, you should disable file and printer sharing in your operating system. This security measure attempts to ensure that others cannot access your files or your printer. You also should be sure to use a firewall.

The following sections address other techniques for protecting against unauthorized access and use. The technique(s) used should correspond to the degree of risk that is associated with the unauthorized access.

Access Controls

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

mobile device, or network. An access control is a security measure that defines who can access a computer, device, or network; when they can access it; and what actions they can take while accessing it. In addition, the computer, device, or network should maintain an audit trail that records in a file both successful and unsuccessful access attempts. An unsuccessful access attempt could result from a user mistyping his or her password, or it could result from a perpetrator trying thousands of passwords.

Organizations should investigate unsuccessful access attempts immediately to ensure they are not intentional breaches of security. They also should review successful access for irregularities, such as use of the computer after normal working hours or from remote computers. The security program can be configured to alert a security administrator whenever suspicious or irregular activities are suspected. In addition, an organization regularly should review users' access privilege levels to determine whether they still are appropriate.

User Names and Passwords

A **user name** — also called a user ID (identification), log on name, or sign in name — is a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user. A **password** is a private combination of characters associated with the user name that allows access to certain computer resources. Most operating systems that enable multiple users to share computers and devices or that access a home or business network require users to enter a user name and a password correctly before they can access the data, information, and programs stored on a computer, mobile device, or network. Many systems that maintain financial, personal, and other confidential information also require a user name and password as part of their sign-in procedure.

Some systems assign a user name and/or password to each user. For example, a school may use a combination of letters from a student's first and last names as a user name. Some websites use your email address as the user name. Information technology (IT) departments may assign passwords so that they have a record in case the employee leaves or forgets the password. With other systems, users select their own user names and/or passwords. Many users select a combination of their first and last names for their user names. Many online social networks, media sharing sites, and retail and other websites allow you to choose your own user name. You might select a name that is formed from parts of your real name or nickname and possibly some numbers, if the name you want is taken.

If you wish to remain more anonymous, choose a user name that combines common words, or reflects your interests (such as guitarbayor19). Once you select a password, change it frequently. Do not disclose your password to anyone or write it on a slip of paper kept near the computer, especially taped to the monitor or under the keyboard. Email and telemarketing scams often ask unsuspecting users to disclose their credit card numbers, so be wary if you did not initiate the inquiry or phone call.

In addition to a user name and password, some systems ask users to enter one of several pieces of personal information. Such items can include a grandparent's first name, your favorite food, your first pet's name, or the name of the elementary school you attended. These items should be facts that you easily remember but are not easy for others to discover about you when using a search engine or examining your profiles on online social networks. As with a password, if the user's response does not match information on file, the system denies access.

Passphrase

Instead of passwords, some organizations use passphrases to authenticate users.
A passphrase is a private combination of words, often containing mixed capitalization and punctuation, associated with a user name that allows access to certain computer resources. Passphrases, which often can be up to 100 characters in length, are more secure than passwords, yet can be easy to remember because they contain words.

PIN

A **PIN** (personal identification number), sometimes called a passcode, is a numeric password, either assigned by a company or selected by a user. PINs provide an additional level of security. Select PINs carefully and protect them as you do any other password. For example, do not use the same four digits, sequential digits, or dates others could easily determine, such as birth dates.

Possessed Objects

A possessed object is any item that you must possess, or carry with you, in order to gain access to a computer or computer facility. Examples of possessed objects are badges, cards, smart cards, and keys. The card you use in an ATM (automated teller machine), for example, is a possessed object that allows access to your bank account.

Biometric Devices

A **biometric device** authenticates a person's identity by translating a personal characteristic, such as a fingerprint, into a digital code that is compared with a digital code stored in a computer or mobile device verifying a physical or behavioral characteristic. If the digital code in the computer or mobile device does not match the personal characteristic code, the computer or mobile device denies access to the individual. Biometric devices grant access to programs, computers, or rooms using computer analysis of some biometric identifier.

Examples of biometric devices and systems include fingerprint readers, face recognition systems, hand geometry systems, voice verification systems, signature verification systems, iris recognition systems, and retinal scanners. The EC (Electoral Commission) of Ghana uses BVD to verify voters during elections.

Fingerprint Reader

A **fingerprint reader**, or fingerprint scanner, captures curves and indentations of a fingerprint. Organizations use fingerprint readers to secure doors, computers, and software. Some home and small business users install fingerprint readers to authenticate users before they can access a personal computer. The reader also can be set up to perform different functions for different fingers; for example, one finger starts a program and another finger shuts down the computer. External fingerprint readers usually plug into a USB port.

Some laptops, smartphones, and smartwatches have a built fingerprint reader (infinix Hot 4). Using their fingerprint, users can unlock the computer or device, sign in to programs and websites via their fingerprint instead of entering a user name and password, and on some devices, even test their blood pressure and heart rate.

What is a lock screen?

A lock screen is a screen that restricts access to a computer or mobile device until a user performs a certain action. Some simply require a user swipe the screen to unlock the screen. Others verify a user's identity by requiring entry of a password, PIN, or passcode; a fingerprint scan; or a gesture swipe. Gestures are motions users make on a touch screen with the tip of one or more fingers. For example, to unlock the screen on a phone, a user could connect the dots on the screen using a pattern previously defined by the user.

Face Recognition System

A face recognition system captures a live face image and compares it with a stored image to determine if the person is a legitimate user. Some buildings use face recognition systems to secure access to rooms. Law enforcement, surveillance systems, and airports use face recognition to protect the public. Some mobile devices use face recognition systems to unlock the device. Face recognition programs are becoming more sophisticated and can recognize people with or without glasses, makeup, or jewellery, and with new hairstyles.

Hand Geometry System

A hand geometry system measures the shape and size of a person's hand. Because hand geometry systems can be expensive, they often are used in larger companies to track workers' time and attendance.

Voice Verification System

A voice verification system compares a person's live speech with their stored voice pattern. Larger organizations sometimes use voice verification systems as time and attendance devices. Many companies also use this technology for access to sensitive files and networks. Some financial services use voice verification systems to secure phone banking transactions.

Signature Verification System.

A signature verification system recognizes the shape of your handwritten signature, as well as measures the pressure exerted and the motion used to write the signature. Signature verification systems use a specialized pen and tablet. Signature verification systems often are used to reduce fraud in financial institutions.

Iris Recognition System

High security areas use **iris recognition systems**. The camera in an iris recognition system uses iris recognition technology to read patterns in the iris of the eye. These patterns are as unique as a fingerprint. Iris recognition systems are quite expensive and are used by government security organizations, the military, and financial institutions that deal with highly sensitive data. Some organizations use retinal scanners, which work similarly but instead scan patterns of blood vessels in the back of the retina.

Two-Step Verification

In an attempt to further protect personal data and information from online thieves, many organizations such as financial institutions or universities that store sensitive or confidential items use a two-step verification process. With **two-step verification**, also known as two-factor verification, a computer or mobile device uses two separate methods, one after the next, to verify the identity of a user.

ATMs (automated teller machines) usually requires a two-step verification. Users first insert their ATM card into the ATM (Step 1) and then enter a PIN (Step 2) to access their bank account.

Digital Forensics

Digital forensics, also called cyberforensics, is the discovery, collection, and analysis of evidence found on computers and networks. Digital forensics involves the examination of media, programs, data and log files on computers, mobile devices, servers, and networks. Many areas use digital forensics, including law enforcement, criminal prosecutors, military intelligence, insurance agencies, and information security departments in the private sector.

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

Software theft occurs when someone steals software media, intentionally erases programs, illegally registers and/or activates a program, or illegally copies a program.

- **Physically stealing software**: A perpetrator physically steals the media that contains the software, or steals the hardware that contains the media that contains the software. For example, an unscrupulous library patron might steal a game CD/DVD.

- **Intentionally erasing software**: A perpetrator erases the media that contains the software. For example, a software developer who is terminated from a company may retaliate by removing or disabling the programs he or she has written from company computers.
- **Illegal registration/activation**: A perpetrator illegally obtains registration numbers and/or activation codes. A program called a keygen, short for key generator, creates software registration numbers and sometimes activation codes. Some unscrupulous individuals create and post keygens so that users can install software without legally purchasing it.
- **Illegal copying**: A perpetrator copies software from manufacturers.

Software piracy, often referred to simply as **piracy**, is the unauthorized and illegal duplication of copyrighted software. **Piracy is the most common form of software theft**.

Safeguards against Software Theft

To protect software media from being stolen, owners should keep original software boxes and media or the online confirmation of purchased software in a secure location, out of sight of prying eyes. All computer users should back up their files and drives regularly, in the event of theft. When some companies terminate a software developer or if the software developer quits, they escort the employee off the premises immediately. These companies believe that allowing terminated employees to remain on the premises gives them time to sabotage files and other network procedures. Many manufacturers incorporate an activation process into their programs to ensure the software is not installed on more computers than legally licensed.

During the **product activation**, which is conducted either online or by phone, users provide the software product's identification number to associate the software with the computer or mobile device on which the software is installed. Usually, the software can be run a preset number of times, has limited functionality, or does not function until you activate it. To further protect themselves from software piracy, software manufacturers issue users license agreements.

A **license agreement** is the right to use software. That is, you do not own the software. The most common type of license included with software purchased by individual users is a single-user license agreement, also called an **end-user license agreement (EULA)**. The license agreement provides specific conditions for use of the software, which a user must accept before using the software. These terms usually are displayed when you install the software. Use of the software constitutes acceptance of the terms on the user's part.

To support multiple users' access of software, most manufacturers sell network versions or site licenses of their software, which usually costs less than buying individual stand-alone copies of the software for each computer. A network license is a legal agreement that allows multiple users to access the software on the server simultaneously.

The **network license fee** usually is based on the number of users or the number of computers attached to the network.

A **site license** is a legal agreement that permits users to install the software on multiple computers — usually at a volume discount.

Information Theft

Information theft occurs when someone steals personal or confidential information. Both Business and home users can fall victim to information theft. An unethical company executive may steal or buy stolen information to learn about a competitor. A corrupt individual may steal credit card numbers to make fraudulent purchases. Information theft often is linked to other types of cybercrime. For example, an individual first might gain unauthorized access to a computer and then steal credit card numbers stored in a firm's accounting department.

Safeguards against Information Theft

Most organizations will attempt to prevent information theft by implementing the user identification and authentication controls discussed earlier in this unit. These controls are best suited for protecting information on computers located on an organization's premises. To further protect information on the Internet and networks, organizations and individuals use a variety of encryption techniques.

Encryption

Encryption is the process of converting data that is readable by humans into encoded characters to prevent unauthorized access. You treat encrypted data just like any other data. That is, you can store it or send it in an email message. To read the data, the recipient must **decrypt**, or decode it. For example, users may specify that an email application encrypt a message before sending it securely. The recipient's email application would need to decrypt the message in order for the recipient to be able to read it.

In the encryption process, the unencrypted, readable data is called **plaintext**. The encrypted (scrambled) data is called **ciphertext**. An encryption algorithm, or cypher, is a set of steps that can convert readable plaintext into unreadable ciphertext. A simple encryption algorithm might switch the order of characters or replace characters with other characters. Encryption programs typically use more than one encryption algorithm, along with an encryption key. An encryption key is a set of characters that the originator of the data uses to encrypt the plaintext and the recipient of the data uses to decrypt the ciphertext.

Two basic types of encryption are private key and public key. With private key encryption, also called symmetric key encryption, both the originator and the recipient use the same secret key to encrypt and decrypt the data. Public key encryption, also called **asymmetric key** encryption, uses two encryption keys: a **public key and a private key**. Public key encryption software generates both the private key and the public key. A message encrypted with a public key can be decrypted only with the corresponding private key, and vice versa. The public key is made known to message originators and recipients. For example, public keys may be posted

on a secure webpage or a public-key server, or they may be emailed. The private key, by contrast, should be kept confidential.

Some operating systems and email programs allow you to encrypt the contents of files and messages that are stored on your computer. You also can purchase an encryption program to encrypt files. Many browsers use encryption when sending private information, such as credit card numbers, over the Internet. Mobile users today often access their company networks through a **virtual private network**. When a mobile user connects to a main office using a standard Internet connection, a **virtual private network (VPN)** provides the mobile user with a secure connection to the company network server, as if the user has a private line. VPNs help ensure that data is safe from being intercepted by unauthorized people by encrypting data as it transmits from a laptop, smartphone, or other mobile device.

Digital Signatures and Certificates

A **digital signature** is an encrypted code that a person, website, or organization attaches to an electronic message to verify the identity of the message sender. Digital signatures often are used to ensure that an impostor is not participating in an Internet transaction. That is, digital signatures can help to prevent email forgery. A digital signature also can verify that the content of a message has not changed.

A **digital certificate** is a notice that guarantees a user that a website is legitimate. E-commerce applications commonly use digital certificates. Browsers often display a warning message if a website does not have a valid digital certificate. A website that uses encryption techniques to secure its data is known as a **secure site.** Web addresses of secure sites often begin with **https instead of http**. Secure sites typically use digital certificates along with security protocols.

8.4 Hardware Theft and Vandalism

Users rely on computers and mobile devices to create, store, and manage important information. You should take measures to protect computers and devices from theft, vandalism, and failure. Hardware theft is the act of stealing digital equipment. Hardware vandalism involves defacing or destroying digital equipment. Hardware can fail for a variety of reasons: aging hardware, natural or man-made disasters, or random events such as electrical power problems, and even errors in programs or apps.

Safeguards against Hardware Theft and Vandalism

Backing Up — The Ultimate Safeguard

To protect against data loss caused by hardware/software/information theft or system failure, users should back up computer and mobile device files regularly. A **backup** is a duplicate of a file, program, or media that can be used if the original is lost, damaged, or destroyed. To **back up** a file means to make a copy of it. In the case of system failure or the discovery of corrupted

files, you **restore** the files by copying the backed up files to their original location on the computer or mobile device.

If you choose to back up locally, be sure to use high-quality media. A good choice for a home user might be optical discs or an external hard drive. Keep your backup media in a fireproof and heatproof safe or vault, or offsite. Off-site means in a location separate from where you typically store or use your computer or mobile device. Keeping backup copies off-site minimizes the chance that a single disaster, such as a fire, would destroy both the original and the backup media. An off-site location can be a safe deposit box at a bank, a briefcase, or cloud storage or cloud backup.

Cloud storage provides storage to customers, usually along with synchronization services but often on smaller amounts of data. By contrast, cloud backup provides only backup and retrieval services, but generally provides continuous data protection to the cloud. More customers are opting for cloud backup because it saves them the cost of maintaining hardware. Backup programs are available from many sources. Most operating systems include a backup program. Example of cloud storage services include google Drive, Microsoft OneDrive and Dropbox.

Backup devices, such as external disk drives, also include backup programs. Numerous stand-alone backup tools exist. Cloud storage providers may offer backup services. Users of a cloud backup service install software on their computers that backs up files to the cloud as they are modified. Business and home users can perform four types of backup: **full, differential, incremental, or selective**. A fifth type, continuous data protection, often is used only by large enterprises to back up data to an in-house network storage device purchased and maintained by the enterprise. Cloud backup services, a sixth option, are providing continuous data protection capabilities at a lower cost. Some users implement a three-generation backup policy to preserve three copies of important files. The grandparent is the oldest copy of the file. The parent is the second oldest copy of the file. The child is the most recent copy of the file. When a new backup is performed, the child becomes the parent, the parent becomes the grandparent, and the media on which the grandparent copy was stored may be erased and reused for a future backup.

Disaster Recovery

A disaster can be natural or man-made (hackers, viruses, etc.). Each company and each department or division within an organization usually has its own disaster recovery plan. The following scenario illustrates how an organization might implement a disaster recovery plan.

WIRELESS SECURITY

Billions of home and business users have laptops, smartphones, and other mobile devices to access the Internet, send email and Internet messages, chat online, or share network connections — all wirelessly. Home users set up wireless home networks. Mobile users access wireless networks in hot spots at airports, hotels, shopping malls, bookstores, restaurants, and

coffee shops. Schools have wireless networks so that students can access the school network using their mobile computers and devices as they move from building to building.

Although wireless access provides many conveniences to users, it also poses additional security risks. Some perpetrators connect to other's wireless networks to gain free Internet access; others may try to access an organization's confidential data. To access a wireless network, the individual must be in range of the wireless network. Some intruders intercept and monitor communications as they transmit through the air. Others connect to a network through an unsecured **wireless access point (WAP)** or combination router/WAP.

Mobile Security

The consequences of losing a smartphone or mobile device are significant given the amount of storage and the variety of personal and business data stored.

The goal, therefore, for mobile device users is to make their data as secure as possible. Follow these steps to protect sensitive and personal data and to fight mobile cybercrime.

- **Be extra cautious locating and downloading apps.** Any device that connects to the Internet is susceptible to mobile malware. Cyberthieves target apps on widely used phones and tablets. Popular games are likely candidates to house malware, and it often is difficult to distinguish the legitimate apps from the fake apps. Obtain mobile device apps from well-known stores, and before downloading anything, read the descriptions and reviews. Look for misspellings and awkward sentence structure, which could be clues that the app is fake. If something looks awry, do not download. Scrutinize the number and types of permissions the app is requesting. If the list seems unreasonable in length or in the personal information needed, deny permission and uninstall the app.
- **Use a PIN.** Enable the passcode feature on a mobile device as the first step in stopping prying eyes from viewing contents. This four-to-eight-digit code adds a layer of protection. Only emergency functions can be accessed without entering the correct sequence of numbers. This strong code should not be information easily guessed, such as a birthdate.
- **Turn off GPS tracking.** GPS technology can track the mobile device's location as long as it is transmitting and receiving signals to and from satellites. This feature is helpful to obtain directions from your current location, view local news and weather reports, find a lost device, summon emergency personnel, and locate missing children. Serious privacy concerns can arise, however, when the technology is used in malicious ways, such as to stalk individuals or trace their whereabouts. Unless you want to allow others to follow your locations throughout the day, disable the GPS tracking feature until needed.
- **Use mobile security software.** Protection is necessary to stop viruses and spyware and to safeguard personal and business data. Mobile security apps can allow you to lock your mobile device and SIM card remotely, erase the memory, and activate the GPS function. Other apps prevent cyberthieves from hijacking your phone and taking pictures, making recordings, placing calls to fee-imposed businesses, and sending infected messages to all individuals in your contact list.

- **Avoid tapping or clicking unsafe links.** Tapping or clicking an unknown link can lead to malicious websites.

8.5. Ethics, Health and Society

As with any powerful technology, computers and mobile devices can be used for both good and bad intentions. The standards that determine whether an action is good or bad are known as ethics.

Technology ethics are the moral guidelines that govern the use of computers, mobile devices, information systems, and related technologies. Frequently discussed areas of computer ethics are unauthorized use of computers, mobile devices, and networks; software theft (piracy); information accuracy; intellectual property rights; codes of conduct.

Information Accuracy

Information accuracy is a concern today because many users access information maintained by other people or companies, such as on the Internet. Do not assume that because the information is on the web that it is correct. As discussed in Chapter 2, users should evaluate the value of a webpage before relying on its content. Be aware that the organization providing access to the information may not be the creator of the information.

In addition to concerns about the accuracy of computer input, some individuals and organizations raise questions about the ethics of using computers to alter output, primarily graphic output, such as a retouched photo. With graphics equipment and software, users easily can digitize photos and then add, change, or remove images.

Intellectual Property Rights

Intellectual property (IP) refers to unique and original works, such as ideas, inventions, art, writings, processes, company and product names, and logos. Intellectual property rights are the rights to which creators are entitled for their work. Certain issues arise surrounding IP today because many of these works are available digitally and easily can be redistributed or altered without the creator's permission.

A copyright gives authors, artists, and other creators of original work exclusive rights to duplicate, publish, and sell their materials. A copyright protects any tangible form of expression. A common infringement of copyright is piracy, where people illegally copy software, movies, and music. Many areas are not clear-cut with respect to the law, because copyright law gives the public fair use to copyrighted material. The issues surround the phrase, fair use, which allows use for educational and critical purposes. This vague definition is subject to widespread interpretation and raises many questions:

- Should individuals be able to download contents of your website, modify it, and then put it on the web again as their own?
- Should a faculty member have the right to print material from the web and distribute it to all members of the class for teaching purposes only?

- Should someone be able to scan photos or pages from a book, publish them on the web, and allow others to download them?
- Should someone be able to put the lyrics of a song on the web?
- Should students be able to take term papers they have written and post them on the web, making it tempting for other students to download and submit them as their own work?

These issues with copyright law led to the development of **digital rights management (DRM)**, a strategy designed to prevent illegal distribution of movies, music, and other digital content.

Codes of Conduct

A **code of conduct** is a written guideline that helps determine whether a specification is ethical/unethical or allowed/not allowed. An IT code of conduct focuses on acceptable use of technology. Employers and schools often specify standards for the ethical use of technology in an IT code of conduct and then distribute these standards to employees and students. You also may find codes of conduct online that define acceptable forms of communications for websites where users post commentary or other communications, such as blogs, online discussions, and so on.

Information Privacy

Information privacy refers to the right of individuals and companies to deny or restrict the collection, use, and dissemination of information about them. Organizations often use huge databases to store records, such as employee records, medical records, financial records, and more. Much of the data is personal and confidential and should be accessible only to authorized users. Many individuals and organizations, however, question whether this data really is private. That is, some companies and individuals collect and use this information without your authorization. Websites often collect data about you, so that they can customize advertisements and send you personalized email messages. Some employers monitor your computer usage and email messages.

The following sections address techniques companies and employers use to collect your personal data.

Electronic Profiles

When you fill out a printed form, such as a magazine subscription or contest entry, or an online form to sign up for a service, create a profile on an online social network, or register a product warranty, the merchant that receives the form usually stores the information you provide in a database. Likewise, every time you tap or click an advertisement on the web or perform a search online, your information and preferences enter a database. Some merchants may sell or share the contents of their databases with national marketing firms and Internet advertising firms. By combining this data with information from public records, such as driver's licenses and vehicle registrations, these firms can create an electronic profile of individuals. Electronic profiles may include personal details, such as your age, address, phone number, marital status, number and ages of dependents, interests, and spending habits.

Direct marketing supporters claim that using information in this way lowers overall selling costs, which lowers product prices. Critics contend that the information in an electronic profile reveals more about an individual than anyone has a right to know. They argue that companies should inform people if they plan to provide personal information to others, and people should have the right to deny such use. Many websites allow people to specify whether they want their personal information shared or preferences retained

Cookies

A **cookie** is a small text file that a web server stores on your computer. Cookie files typically contain data about you, such as your user name, postal code, or viewing preferences.

Websites use cookies for a variety of purposes:

- Most websites that allow for personalization use cookies to track user preferences. These cookies may obtain their values when a user fills in an online form requesting personal information. Some websites, for example, store user names in cookies in order to display a personalized greeting that welcomes the user, by name, back to the website. Other websites allow users to customize their viewing experience with preferences, such as local news headlines, the local weather forecast, or stock quotes.
- Some websites use cookies to store user names and/or passwords, so that users do not need to enter this information every time they sign in to the website.
- Online shopping sites generally use a session cookie to keep track of items in a user's shopping cart. This way, users can start an order during one web session and finish it on another day in another session. Session cookies usually expire after a certain time, such as a week or a month.
- Some websites use cookies to track how often users visit a site and the webpages they visit while at the website.
- Websites may use cookies to target advertisements. These websites store a user's interests and browsing habits in the cookie.

Many commercial websites send a cookie to your browser; your computer's hard drive then stores the cookie. The next time you visit the website, your browser retrieves the cookie from your hard drive and sends the data in the cookie to the website. A website can read data only from its own cookie file stored on your hard drive. That is, it cannot access or view any other data on your hard drive — including another cookie file.

Phishing

As mentioned earlier, **phishing** is a scam in which a perpetrator sends an official looking email message that attempts to obtain your personal and/or financial information. These messages look legitimate and request that you update credit card numbers, Social Security numbers, bank account numbers, passwords, or other private information.

Clickjacking is yet another scam. With clickjacking, an object that can be tapped or clicked — such as a button, image, or link — on a website, pop-up ad, pop-under ad, or in an email message or text message contains a malicious program. When a user taps or clicks the disguised object, a variety of nefarious events may occur. Browsers typically include clickjacking protection.

Social Engineering

As related to the use of technology, **social engineering** is defined as gaining unauthorized access to or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others. Some social engineers trick their victims into revealing confidential information, such as user names and passwords, on the phone, in person, or on the Internet. Techniques they use include pretending to be an administrator or other authoritative figure, feigning an emergency situation, or impersonating an acquaintance.

Social engineers also obtain information from users who do not destroy or conceal information properly. These perpetrators sift through company dumpsters, watch or film people dialing phone numbers or using ATMs, and snoop around computers or mobile devices looking for openly displayed confidential information.

To protect yourself from social engineering scams, follow these tips:

- Verify the identity of any person or organization requesting personal or confidential information.
- When relaying personal or confidential information, ensure that only authorized people can hear your conversation.
- When personal or confidential information appears on a computer or mobile device, ensure that only authorized people can see your screen.
- Shred all sensitive or confidential documents.
- After using a public computer, clear the cache in its browser.
- Avoid using public computers to conduct banking or other sensitive transactions.

Digital Safety and Security

Green computing involves reducing the electricity consumed and environmental waste generated when using a computer

Strategies include:

- Recycling
- Using energy efficient hardware and energy saving features
- Regulating manufacturing processes
- Extending the life of computers
- Immediately donating or properly disposing of replaced computers