

COMPUTER NETWORKS AND WEB TECHNOLOGIES

3.1 Computer networks

Previous chapters have covered the fundamentals of a single computer system and its peripherals. Now we will look at linking computers together to enhance communication among users, whether in the same office or across the world.

Data communication is the transmission of data and information between two or more computers. Many computer users need to be able to connect their computer to other computers, whether located close by or at a remote site. For example, office workers may want to communicate with data on computers at their workplaces from wherever they may be working in the world, and home computer users may want to access the Internet. Data communication is essential for electronic mail (email), voicemail, facsimile (fax), telecommuting, video conferencing, electronic data interchange (EDI), global positioning systems (GPS), online services, social media and the Internet.

Many schools, businesses and other organisations link computers together to form a network so that they can transmit data and information to share files, resources such as disk drives, CD-ROM drives, modems or printers and programs such as word processors, spreadsheets and databases. There are two ways that data can be transmitted between computers:

- ♦ to **upload** data means to send this data from your computer to another computer on the network or the Internet
- ♦ to **download** data means to receive data to your computer from another computer on the network or the Internet.

Computers can be linked in different ways, or configurations, to transmit data. Two configurations are:

- ♦ **point-to-point:** a direct link between two computers in a network
- ♦ **broadcast:** using one computer to transmit data and information to serve the needs of several terminals or computers connected to it in a network.

A popular way of transmitting data is through microwaves, which are high-frequency radio signals that travel through the atmosphere. They are used for high-volume, long-distance communication. Microwave signals, however, only travel in straight lines. They can be bounced off satellites to cover longer distances. Low-orbit satellites travel closer to earth, so weaker signals can be processed while consuming less power. An example of a system that uses microwaves is a cellular network that supports two-way communication. These networks use interconnected cell sites that communicate with mobile (or cellular) phones.

Network configurations

A computer network connects computers so that peripherals such as printers can be shared among computers. Networks come in different sizes. A few computers, printers and large hard disks – usually on one site – can be linked in a small local area network (LAN). Many small and large computers, located on different sites spread over a large geographical area or in different countries, can be linked in a wide area network (WAN). A good example of a wide area network is the Internet.

A Metropolitan Area Network (MAN) falls between a WAN and LAN. It is large enough to extend to an area like a city or campus. A MAN might therefore be owned and operated by a single organisation (for instance, a university) and accessed by students and other associated organisations. MANs are useful in connecting LANs to WANs like the Internet.

Computers that are not networked are known as **stand-alone** computers. Data that is on a stand-alone system has to be transferred using a secondary storage device if it is to be used on another computer.

Not all networks are connected with cabling; some networks are **wireless networks**. A Wireless Local Area Network (WLAN) is a LAN that is great for allowing laptops or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables. However, they provide poor security and are susceptible to interference from light and electronic devices. They are also slower than LANs even when connected using cabling.

To connect a computer to a LAN using cables, you plug the network cable into the network adapter on the computer. You then have to set up the system software which enables the computer to operate on

the network. The computer is now ready to share files, resources and programs with other computers/users.

To connect computers to a LAN using cables, you need:

- ♦ network cabling
- ♦ a network card in each computer
- ♦ a hub (or hubs)
- ♦ a file server
- ♦ system software.

Hubs

If you have a network in school, it is likely that the computers are connected by cable to a central device called a **hub** (Fig 3.1). One or more hubs (if there are a large number of computers on the network) are then connected to a file server. A **file server** is a high-performance computer containing large capacity hard disk drives that are available to all network users. It is where application programs and data can be shared to all users on the network. A file server is not used as a normal computer terminal, as its job is dedicated only to the task of managing shared files. Some networks also use a printer server that is dedicated to managing all printers on a network. Where one powerful computer controls others, the network is called a hierarchical network.



Fig 3.1 Layout of a typical computer network

Peer-to-peer network

When a network does not have a file server, it is called a **peer-to-peer network**. In a peer-to-peer network, each computer acts as a server to the other computers – its peers – on the network. A peer-to-peer network also allows users to access each other's hard disks and peripherals.

Network layout

Careful planning of a computer network is essential. There are three main types of layout (topology) of computer networks: star, bus and ring.

In a **star network** (Fig 3.2) all the nodes are connected to a central hub. This means that each computer has its own connection to the network and that a break in a cable will not affect the working of other computers. If the hub breaks down, then all the computers on the hub will not work. However, star networks, although more expensive to install than other types, are the quickest.



Fig 3.2 A star network

A **bus network** is the simplest type of topology, where the network nodes (computers) are in a line, as shown in Figure 3.3. Bus networks are cheap and reliable, but if the cable breaks the network is split into two

unconnected parts. Bus networks are slower than star networks, with the speed of network traffic limited to 10 Mb per second.



Fig 3.3 A bus network

Unlike a bus network, a **ring network** (Fig 3.4) has no end to the line. The last node (computer) is connected to the first node, forming a ring or loop. As with a bus network, if the cable breaks it will affect all the computers on the network. Ring networks are also slower than star networks, with the speed of network traffic limited to 10 Mb per second.



Fig 3.4 A ring network

The Internet is a vast collection of computer networks spread throughout the world, which involves all these different ways of linking computers. The most common way to link computers on a network is by cables such as fibre optics or telephone lines. Wireless networks however, are linked by infrared waves, microwaves or radio waves.

WLANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver or antenna to send and receive

the data. Data is relayed between transceivers as if they were physically connected. For longer distances, wireless communication can also take place through mobile telephone technology, microwave transmission or by satellite.

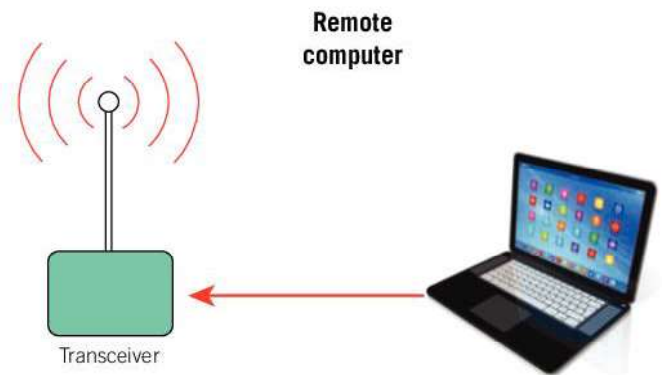
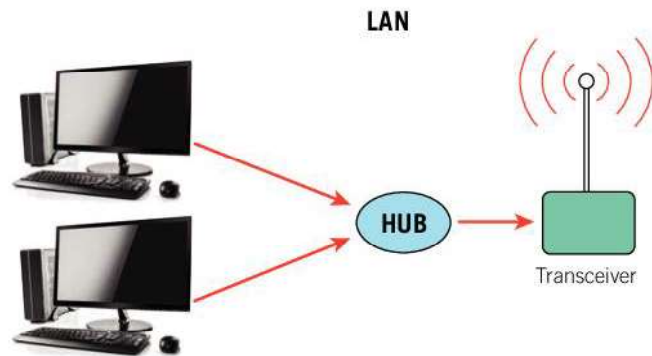


Fig 3.5 Remote computers can connect to the LAN through the transceivers as if they were physically connected. Transceivers are often built into hubs, laptops and portable devices

Bluetooth and **Wi-Fi** (short for wireless fidelity) both provide wireless connectivity using radio waves. The main purpose of Bluetooth is to replace cables, while Wi-Fi provides high-speed wireless access to a network or the Internet. Bluetooth allows for the exchange of data over short distances among wired and wireless devices. WLANs provides easy access to information between wireless devices from different manufacturers. Devices with Wi-Fi, such as computers, mobile phones, games consoles or MP3 players, can

connect to the Internet if a wireless network is within a certain range.

A **hotspot** is a public area as small as a room or as large as many square miles that offers Internet access over a WLAN. Wi-Fi hotspots can be in cafés, airports and hotels. Wi-Fi connections can be made up to about 300 feet away from a hotspot, to keep users connected wirelessly while commuting. Customers may have to pay for this service.

Table 3.1 Advantages and disadvantages of networked systems compared with stand-alone systems

Type of system	Advantages	Disadvantages
Stand-alone computers	<ul style="list-style-type: none"> ♦ Ideal for most home users ♦ No network card needed ♦ Can be dedicated to a specific task, e.g. composing music ♦ No need for network software licences – only single-user licence required ♦ Security from users on other sites 	<ul style="list-style-type: none"> ♦ Cannot easily share data, particularly large amounts of data, with others ♦ Data can be transferred only by disk or by modem. Will need to use an external hard drive or online storage, which can be time consuming and unreliable
Networked computers	<ul style="list-style-type: none"> ♦ Access to network from any workstation ♦ Share files with, and send messages to, other computers ♦ Share resources such as disk drives, CD-ROM drives, modems or printers ♦ Share programs (such as word-processing, spreadsheet or database software) which are stored centrally. Possible for network users to work on the same file rather than each user having their own file. These programs are cheaper per user than one-off software for stand-alone computers ♦ Activities of network users and such things as amount of storage space available to users can be controlled by network manager 	<ul style="list-style-type: none"> ♦ Network cards, cabling, hubs and servers can be costly. Wireless connection to a network may result in reduced data transfer rates and unreliable connectivity ♦ If the file server stops working (known as a 'crash'), it can stop everybody on the network from using a computer ♦ Poor security. With more users there is a greater risk of computer viruses and of unauthorised users (hackers) gaining access to network data ♦ Need for network manager to manage the system. This can be costly

Communication channels

The **communication channel** is the method or medium used for transmitting data. Characteristics of communications channels include transmission mode, direction of data flow, transmission medium and transmission speed.

Transmission modes

Transmission modes or rates determine the number of characters that can be transmitted in one second. Two modes are:

- ♦ **asynchronous:** data is transmitted at irregular intervals, and at a low speed of one character at a time
- ♦ **synchronous:** data is transmitted at regular intervals, with high-speed simultaneous transmission of large blocks of data.

Direction of data flow

Transmission lines and media can also be classified according to the direction in which data can flow.

Simplex

Data in a **simplex** line can flow in only one direction, just like traffic in a one-way street. It is a send-only or receive-only line. Examples are radio, TV, computer to printers, public address systems or any other one-directional transmission.

Half duplex

Data in a **half-duplex** line can flow in both directions, but only one way at a time. In other words, data can be either sent or received at any given time. CB radio and walkie-talkies are half-duplex.

Full duplex

Data in a **full-duplex** line can be both sent and received at the same time, like traffic in a two-way street. Most modem connections today transmit full duplex. This increases efficiency, as data flows on the same pair of wires in both directions simultaneously.

To choose which channel to use, you should first decide how much information you want to transfer at any given time, how important it is to have a fast or slow transmission rate, as well as whether you want a full-duplex, half-duplex or simplex channel.

Transmission media

Data can be transmitted through various types of cabled (wired) or wireless media. Cabled media uses wires to transmit data. Wireless media transmits data through the air. Cabled media include twisted pair, coaxial and fibre optic cables; wireless media include satellite, microwave and infrared methods.

Cabled media

Cabled media include twisted pair, coaxial and fibre optic cables.

Twisted pair or ethernet cable

A **voiceband** channel can transmit data at a rate of 300 bits per second (bps) to 9600 bps. The most popular form of transmitting data is via telephone lines. This is easy to handle and cheap, but relatively slow. You need a modem to do this, since telephone lines are built to handle analogue data and not the digital data found in computers. Twisted pair wires are used for this form of data transmission.

Unshielded twisted pair (UTP) is common in telephone cables (Fig 3.6). These cables have pairs of insulated copper wires twisted round each other to help eliminate interference from adjacent pairs and other electrical devices.

An **ethernet cable** (Fig 3.7) is one of the most popular forms of network cable. It resembles a phone cable but is slightly larger. These cables have different colours which differentiate them from phone cables which are usually grey in colour. Like any cable, an ethernet cable has various lengths, but the longer the cable, the weaker the strength of the signal.

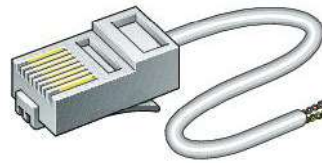


Fig 3.6 Twisted pair cable is used with telephones



Fig 3.7 Ethernet cables are used as network cables

Coaxial cable

A **broadband** channel can transmit data at a rate of thousands of characters per second. Examples of broadband channels are coaxial cables and fibre optic cables.

Coaxial cables (Fig 3.8) are found on televisions, videos and cable TV. They use thickly insulated copper wire and are capable of high-speed transmission but are difficult to install since the cable is somewhat rigid.

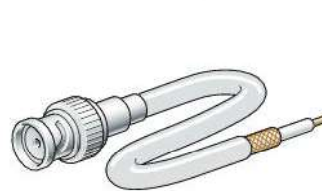


Fig 3.8 Coaxial cable is used for televisions, video and cable TV

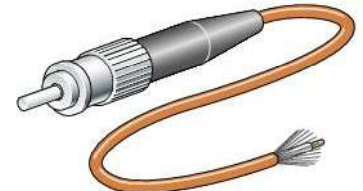


Fig 3.9 Fibre optic cable is used by large telecommunication companies

Fibre optic cable

Fibre optic cables (Fig 3.9) are similar to those used by large telephone and telecommunications companies. These cables consist of clear glass fibres and data is transmitted through them as pulses of light rather than electronic signals. This eliminates the problem of electrical interference. It is the standard for connecting networks between buildings, as it is also not affected by moisture and lightning. Fibre optic cables can transmit signals over much longer distances than coaxial and twisted pair cables. They can also transfer information at vastly greater speeds. This makes it possible to use broadband for services such as video conferencing and interactive services.

Wireless transmission

Remember that wireless media include microwave, satellite and infrared methods. A microwave signal has a very short wavelength, hence the word 'micro'-wave. These powerful signals can be projected over long distances over a direct line-of-sight path between any two points, such as antennae. Satellite transmission is similar to microwave transmission. However, instead of using two microwave dish antennae that are close to each other, it uses a satellite that is located in space.



Fig 3.10 Dish antennae point to satellites located in space

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network.

Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver.

Intranets and extranets

The success of the Internet has led businesses and other organisations to set up intranets. Many schools now have their own intranet.

Intranet

An **intranet** is a private network based on Internet standards but only available within a business or other organisation. No one outside the business or organisation is able to access the intranet. A company can set up an intranet and allow its workers to send messages to each other and use a browser to access company information saved as web pages. It can also be used for staff training. An intranet is not directly connected to the Internet, but some intranets do allow access to the Internet, via so-called gateway computers. For users of an intranet, it looks and functions just like a website.

Intranets may, depending on how they are set up, consist of local area networks (LANs) and wide area networks (WANs). A firewall is used to stop computers on other networks, including the Internet, accessing an intranet. Instead, all communication is through a proxy server that is outside the network. The proxy server acts as a gatekeeper, filtering Internet sites and deciding what files or messages should come in to, or go out from, a computer network.

Intranets are used by many businesses and other organisations to:

- ♦ distribute documents
- ♦ share information
- ♦ distribute software
- ♦ access databases
- ♦ help with staff training
- ♦ facilitate group work
- ♦ enable teleconferencing.

Intranets are popular as they are less expensive to build and manage than other types of private network. Also, users of intranets are familiar with how to use them because they look and behave like websites on the Internet. This saves time and money on staff training.

More and more schools are setting up their own intranets. Internal school information, such as examination timetables, room changes, sports teams and results, can be readily shared with staff and students. Each department in the school can have its own intranet page(s) along with relevant information for students, such as revision guides and homework tasks. Students also have the opportunity to share their work with others.

Extranets

Once intranets were developed, it became clear that businesses and other organisations sometimes wanted to allow others, such as suppliers and customers, to have limited access to their intranet. This would lead to a closer relationship with customers, a better exchange of information and improved efficiency. Therefore, **extranets** were developed. Extranets allow authorised outsiders limited access to an intranet. Not everyone is allowed access to an extranet. Only authorised users are allowed. They must have valid usernames and passwords and an identity that establishes which part of the extranet they can access.

Extranets enable businesses to work closely together. A car manufacturer, for example, might develop an extranet to allow all of its various suppliers (of tyres, lights, windscreens, seats and so on) and car showrooms to keep in very close contact regarding orders and deliveries. An extranet could be used to share information not available to the public, as well as to exchange data and to develop joint training programmes. Data can be exchanged using electronic

data interchange (EDI). Electronic data interchange is a special way to transfer business documents, such as orders and invoices, between computers.

The aim of EDI is to speed up communication between businesses and other organisations, and eventually to do away with paper transactions. EDI often involves putting the data into special computer code to stop other people looking at the data.

Questions

- 1 State the term that describes each of the following:
 - a data that is sent from a user's computer to another computer in the network
 - b data that is received to a user's computer from another computer in the network.
- 2 Give two examples of using microwave signals.
- 3 Name two peripheral devices that are usually connected to a network.
- 4 Explain what the following terms represent:
 - a WAN
 - b LAN
 - c WLAN
 - d MAN.
- 5 What is the name of a network that does not have a file server?
- 6 Name three arrangements of a network.
- 7 What is the term given to an area that offers Internet access over a WLAN?
- 8 State the type of transmission for each of the following descriptions:
 - a data can flow in only one direction
 - b data can flow in both directions, but only one direction at a time
 - c data can be sent and received at the same time.
- 9 State the type of transmission media that describes each of the following:
 - a uses wires to transmit data
 - b transmits data through the air.
- 10 What is the name given to a network that is private to a business?

The Internet has been described as ‘a network of networks’, connecting billions of mobile devices, laptops, microcomputers, minicomputers, mainframes and supercomputers linked in commercial, government and educational networks.

Today businesses set up websites on the Internet so that:

- ♦ they can advertise what they do and what they sell
- ♦ people can email enquiries, orders and requests
- ♦ they can reach an international audience.

The main services provided by the Internet include:

- ♦ **Electronic mail (email):** This is a method of communication between computers on a network. Email means messages that can be sent ‘electronically’ using special software from one computer to another anywhere in the world, via networks such as LANs and WLANs. The mail is then kept in an electronic mailbox. Examples of email software include Microsoft Outlook and Gmail.
- ♦ **Data exchange:** Sending data to another computer (uploading) or receiving data from a computer (downloading).
- ♦ **Instant messaging:** This feature allows users who are connected to the Internet at the same time to exchange text, images, video or audio messages in real time. Different providers have their own brand names for this service, for example Facebook Messenger and WhatsApp.
- ♦ **The World Wide Web (www):** Popularly known as the web. This is the main way of accessing information on the Internet. The web is based on pages of information which are linked and viewed by a web browser. By clicking with the mouse on a link (links are usually underlined words displayed in different colours), you can jump to another location on the web page, or to another web page or website. Millions of web pages are available on virtually every topic imaginable.
- ♦ **File transfer protocol (FTP):** A protocol is a set of rules and procedures that govern transmission between components in a network. Each network has

a set standard for transmitting information, so that computer A in Germany can understand information coming from computer B in Barbados or computer C in France. FTP is the name given to the transfer of files across the Internet. FTP is the Internet equivalent of a file server, with files made available on thousands of the Internet’s computers for downloading onto individual computers. Millions of users use FTP to download updates to popular software, such as Microsoft Word and Excel, although it can also be used to upload (send) files to websites.

Connecting to the Internet

Computers can be connected to the Internet in different ways. Once connected, users are said to be online. To access the Internet, you need:

- ♦ a modem, router and/or switch which is connected to a telephone line
- ♦ a network interface card (NIC) or network adapter, which is usually already installed in your computer
- ♦ software on your computer or mobile device (such as a web browser and email package)
- ♦ Internet service, which is typically a subscription with a company called an Internet service provider (ISP).

A modem (modulator/demodulator) is provided by your ISP, who provides you with access to the Internet. The purpose of the modem is to convert analogue and digital signals between your landline and the Internet. ISPs in the Caribbean include Digicel and Flow. If you are using more than one computer with a modem, then you will need a **router** in addition to the modem.

A router is the ‘traffic cop’ of a network. It directs data from the modem and sends it to the different devices that are connected to it. Devices such as computers, laptops, games consoles, digital televisions and mobile devices can be connected through cables directly to the router or wirelessly.

A switch simply expands the number of devices that can be connected to a router. Some routers, such

as Netgear models, combine the three networking components – modem, router and switch – instead of having separate devices with cables joining them.

A network interface card (NIC) or network adaptor is hardware that is usually already part of a computer or laptop. It provides the computer with a dedicated connection to a network. These cards can be used for wired or wireless connections to the network.

Web browsers and email

The World Wide Web (www) is based on millions of pages of information linked together and viewed by Internet browsers also called web browsers. A web browser is a software application that allows you to access resources and websites on the Internet. Popular browsers include Microsoft Edge, Firefox, Google Chrome and Internet Explorer.

Internet service

There are different types of Internet services, including dial-up, DSL (broadband or cable), and wireless (3G or 4G) for mobile devices.

- ♦ **Dial-up:** This form of connection is the slowest way to connect to the Internet. You need to use your landline telephone to connect to the Internet via dial-up. This means that you cannot use the phone while online.




- ♦ **Broadband:** This method uses a digital subscriber line (DSL) service, which is faster than dial-up. It uses a phone line to connect to the Internet but it is not necessary to have a landline to make the online connection. However, if you do have a landline, broadband allows you to use the phone while connected to the Internet.
- ♦ **Cable:** Many cable television customers can connect to the Internet using a cable modem which sends and receives digital data through a connection to a fibre optic cable television system. Cable television such as Direct TV is a broadband service – a single cable can carry several channels at once – which results in unlimited data being sent and received at very high speeds. Users can also access the Internet at home on a digital television set rather than a computer.
- ♦ **2G, 3G and 4G-LTE:** These services are mostly associated with mobile phones since they are used to connect to the Internet through your provider. However, these connections are slower than broadband and cable. The amount of data sent and received is restricted by your provider, who can charge monthly rates for the data that is used. However, there are companies and universities that offer free Wi-Fi for users who are within the vicinity, to avoid using up personal data allowances.

The 'G' refers to the generations of mobile phone systems. Table 3.3 compares the generations.

Table 3.2 *Methods of connecting to the Internet*

Dial-up	Requires a landline and a modem to connect to the ISP. A point-to-point connection is established to connect to the Internet.
DSL	High speed Asymmetric Digital Subscriber Line (ADSL) that is used with a DSL modem to connect to the Internet. Users can connect to the Internet while using the landline. However, more data can be received from the Internet than is sent.
ISDN	Similar to an ordinary telephone line. The amount you pay depends upon how much you use the line. ISDN is more expensive to use than an ordinary telephone line, but can transmit data digitally at 64 kbps. ISDN lines can be grouped together in pairs to provide even faster data transmission.
Leased line	For a fixed fee per month, a company can rent this dedicated communications line to send and receive large amounts of data. The amount that is charged does not depend on how often the line is used. Speed of a leased line does not change, for example a T1 line has a speed of 1.5 megabits per second.
Cable TV	Uses a cable TV to connect to the Internet. It has fast download speeds, but slower upload speeds
Satellite	Connects to the Internet by using a satellite, an antenna, a coaxial cable and Windows-based software
Wireless	A wireless Internet connection or Wireless Application Protocol (WAP) can be used to connect devices like laptops, mobile phones, remote controls, gaming controls and tablets wirelessly without a physical connection.

Table 3.3 Comparison of 2G, 3G and 4G-LTE

Generation	Features	Problems	Example
2G	Text messaging, multimedia messaging, Internet access, caller ID and the SIM card	Phone calls dropping and slow data transmission rates	
3G	All of 2G, plus web browsing, email, video downloading, picture sharing and other smartphone technology	Major limitation of the 3G network is network coverage	
4G-LTE	All of 3G plus significantly faster speeds and increased network coverage	Still problems with network coverage	

Web technology concepts

In order to access the services on the Internet, the following terms will help you to become familiar with some web technology concepts.

Internet protocol

With so many different computer networks linked together on the Internet, there has to be a standard way in which different networks are linked together. The set of rules, sometimes known as a protocol, for sending and receiving data over the Internet is known as TCP/IP (transmission control protocol/Internet protocol). TCP/IP breaks down the data into little chunks, or packets, which are sent to other computers on the Internet. TCP/IP then ensures that the data is reassembled into its original form.

Getting data sent to the right computer on the Internet is very important, particularly when there are so many. When you address a letter to be sent through the post, you have to be specific about where you want it to go, providing a house number and postcode, or a PO box number. The same principles have to be applied when using the Internet.

A host (server) computer on the Internet is one that provides services such as email, news or data to other computers. Each host computer has its own unique address to identify it. This address is known as an IP address (Internet Protocol address). The IP address is usually four numbers separated by full stops: for example, 194.238.196.100. The first two or three numbers identify the computer network, with the rest identifying the individual computer.

It is much easier to type in and remember a domain name, such as www.cxc.org, than having to remember the IP address. But as far as the computer is concerned, the IP address is crucial. Every time you send an email, or browse a web page, your IP address is sent behind the scenes. This way your Internet usage can be tracked!

Internet address

Every site on the Internet has an address known as a URL (uniform resource locator). To access a site, you enter its address (URL) into the web **browser**. There is a space at the top of the screen (labelled 'address') for you to enter the URL. For example, typing www.nationnews.com would give you access to the *Nation* newspaper for up-to-date news and links to other Caribbean newspapers.

Table 3.4 Understanding Internet addresses

//	A double slash (//) in an address gives you the path to the computer (server) on which the resources are stored
/	A slash (/) in an address shows the path (route) to where resources are stored on the server. In other words, the exact location
http	This tells you that it is a website. Http (hypertext transfer) is the set of rules (protocols) used to show web pages on a computer that have been retrieved from web servers
ftp	File transfer protocol. Ftp sites are not websites, but sites that allow you to transfer files across the Internet
.com	.com in an address indicates a commercial organisation: for example, www.nationnews.com
.uk	.uk in an address indicates that the country is the United Kingdom: for example, www.bbc.co.uk
.edu	.edu in an address indicates a university: for example, www.uwi.edu – The University of the West Indies
.bb	Barbados's country extension. Other country extensions include .tt for Trinidad and Tobago and .lc for St. Lucia
.org	.org in an address indicates a non-profit organisation of some kind: for example, www.rss.org.bb is the Regional Security System located in Barbados (.bb extension)
.gov	.gov in an address indicates a government department or organisation: for example, www.bgis.gov.bb – the Barbados Government Information Service
.net	.net is a network or an Internet service provider: for example, www.sunbeach.net
.html or .htm	.html will often appear at the end of an address and indicates that it is a file which contains hypertext: that is, a web page

You will see addresses that start `http://`. The `http` tells you that it is a **website**. To save you time, most browsers today do not require you to type the '`http://`'. Instead, you just type '`www`' followed by the rest of the address. Sometimes you may also see an address that starts with '`ftp`'. FTP sites are not websites, but sites that allow you to transfer files across the Internet.

The name of the web server is next in the URL. A web server is a computer which uses special software to transmit **web pages** over the Internet. Many web server names are prefixed by `www`, for example `www.caribsurf.com`, `www.sunbeach.net`. If you enter the web server name into the web browser, you will see the **homepage** for the site. This is like the title page in a book from which other related pages may be accessed. You will get a message if there is no homepage available.

After the web server name comes the folder where the file is located then the name of the file being retrieved. Typical file name extensions on web pages are `htm` or `html`.

The web is an information retrieval system which enables users to connect from one website to another

via hypertext links on the page. That is, when you click on a link, you are taken from one website to another, which may be on the same computer or a different computer at a remote location.

**Fig 3.11** The Internet homepage of online Caribbean newspapers

If you do not know the URL of the site you want, you can use a search engine. A **search engine** is a software application that finds websites using keywords. Search engines have their own websites, such as `www.google.com`.

Whenever you find a site that you think you would like to visit again, you can 'bookmark' it, by adding it to your list of favourite sites. By opening your list of favourite sites, you can go straight to any site you have bookmarked without typing the URL or using a search engine.

Search engines index the words on billions of web pages. This indexing is undertaken by software robots (also known as spiders) that continually search the web for new sites or updated web pages. Indexing web pages in this way allows you to search using keywords.

Internet cache

When you are using the Internet, your web browser stores pages and files on your hard disk as you view them. These pages and files are stored in a temporary Internet files folder. This is known as a **cache**.

The caching of 'temporary' pages and files is important, as it speeds up the display of pages of sites that you have already been to. This is because a computer can access files more quickly from hard disk than from the web.

Blogs, vlogs and podcasts

Some Internet users post frequent items of commentary, descriptions of events, graphics, video or audio (**podcasting**) to personal websites. This is also called '**blogging**' for posts of text or picture entries or 'vlogging' for posts of video entries called 'vlogs'. Blogs or vlogs can be posted on any subject, and readers/viewers can reply to the post.



Fig 3.12 Vlogging is a popular way to share information

Creating web pages

Hypertext Markup Language (HTML) is a text-based language used to create web pages for display by a web browser. It is a formatting language, since it consists of codes which instruct the browser how to create, format and display the information on the web page. The data to be displayed on the pages is written

as plain text and the formatting codes are written amongst the data (appearing to 'mark up' the data) in the document.

Email

To send an email message you need to have an email address of your own and know the email address of each intended recipient. An advantage of using email is that files containing pictures, sound, video and text can be attached to the message. Also, more than one file can be attached and sent with one email message. When an email is sent, the recipient does not need to be online. The message is stored in an email list for the recipient to read. One email can be sent to an individual or a group of people simultaneously.

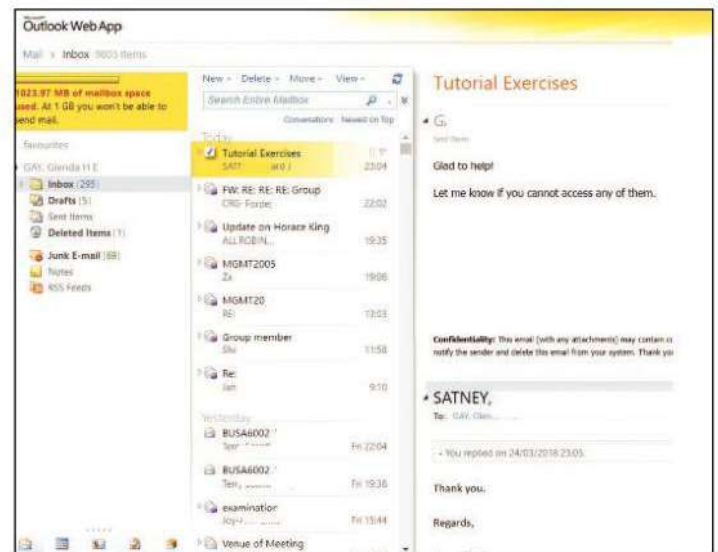


Fig 3.13 There are different web apps for storing email messages

Here are some advantages of email:

- ♦ Ordinary mail takes several days, but email can be sent immediately, and replies received as soon as recipients check their email.
- ♦ Emails do not have to be as formal and structured as typical letters.
- ♦ There is no need to get stamps, envelopes or paper, or go to a post box or the post room in a company.

Disadvantages of email include the following:

- ♦ Not everyone has access to a computer or the software application to use the email facility.
- ♦ Emails are not as private as personal letters.
- ♦ Replies are dependent on the recipient accessing the email and reading the message.

Voice over IP (VoIP) is an Internet protocol used to convert the sound of voice into digital form and transmit it over the Internet. Software applications such as Skype enable users to use the Internet to make telephone calls to others with or without another Internet connection. A major advantage of VoIP is that some users avoid paying international call charges

compared with using an ordinary telephone service. A smartphone (Fig 3.14) is an example of a wireless device that can deliver VoIP, access email and be used for instant messaging and browsing the Internet.



Fig 3.14 Smartphones are an example of a wireless device with VoIP capabilities

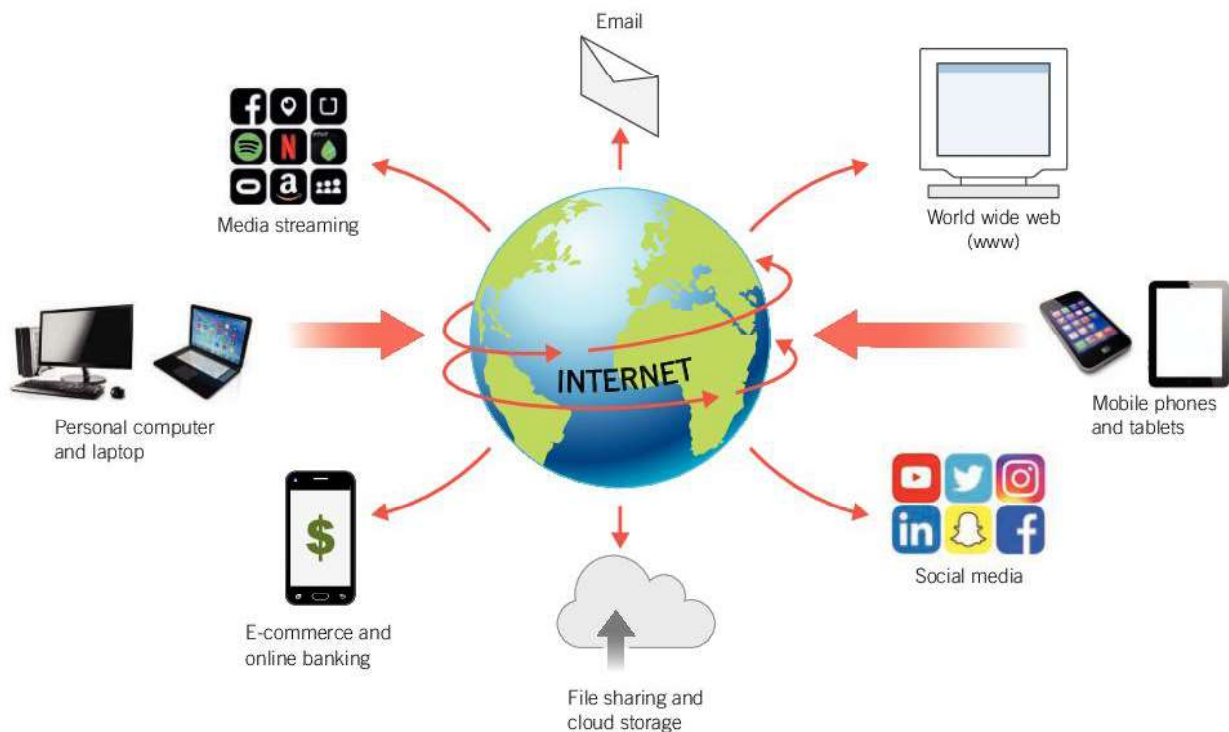


Fig 3.15 The main services provided by the Internet

Table 3.5 *Advantages and disadvantages of the Internet*

Advantages	Disadvantages
<ul style="list-style-type: none">♦ You can find information on the web on virtually any topic you like♦ There is enormous education potential, particularly:<ul style="list-style-type: none">– collaboration between students (and teachers) on projects of interest– simulations, such as dangerous experiments, can be shown on the web– research and finding out more information– gathering of data, such as weather data– access to online experts– to explore and to have fun– information on the web can be multimedia: that is, text, graphics, video, animation and sound♦ With faster access to the Internet, it is possible to have interactive games and TV on demand♦ Some people can now work from home rather than in an office♦ Many commercial organisations advertise, sell goods or provide services on the net: for example, shopping and banking	<ul style="list-style-type: none">♦ The cost of computer equipment, connections and telephone charges can be high♦ There is no control on the quality of information available on the Internet, therefore some information may not be accurate or may be highly offensive, such as racist propaganda. Also, some material is illegal and obscene, such as child pornography♦ Security – many schools, colleges, businesses and other organisations access the Internet via a computer network. It is possible for hackers to gain access, via the Internet, to the network♦ Searching for information can be difficult unless the user knows how to narrow down searches in a search engine♦ It is difficult to protect copyright material: for example, it is easy to download copyright music without paying for it♦ It is possible to download computer viruses that can harm data held on a computer or on a network

Questions

- 1 List any three of the main services provided by the Internet.
- 2 Explain the purpose of the following devices:
 - a modem
 - b router
 - c switch
 - d network interface card (NIC) or network adaptor.
- 3 Name the type of network that is most suitable for each of the following:
 - a allows you to use a landline phone while connected to the Internet
 - b mostly associated with mobile phones.
- 4 What is the difference between a blog and a vlog?
- 5 What is the name of a text-based language used to create web pages for display by a web browser?
- 6 What is the name of the Internet protocol used to convert the sound of voice into digital form and transmit it over the Internet?

Multiple choice questions

- 1 Which of the following devices provides access to the Internet?
 - a adapter
 - b modem
 - c router
 - d switch.
- 2 A network that allows mobile and other devices to connect to it is called a:
 - a LAN
 - b MAN
 - c WAN
 - d WLAN.
- 3 Bluetooth allows for the exchange of data across each of the following, *except*:
 - a long distances
 - b short distances
 - c wired devices
 - d wireless devices.
- 4 The term for sending data from your computer to another computer on a network or the Internet is:
 - a create
 - b download
 - c modify
 - d upload.
- 5 Which of the following connections has the fastest speed to send and receive large amounts of data?
 - a dial-up
 - b satellite
 - c wireless
 - d leased line.
- 6 A type of network where no one outside an organisation is allowed access is called a(n):
 - a telnet
 - b extranet
 - c intranet
 - d Internet.
- 7 Each of the following features are typical of 2G mobile phone systems, *except*:
 - a caller ID
 - b Internet access
 - c multimedia messaging
 - d video streaming.
- 8 A double slash (\\) in an Internet address shows:
 - a that it is a file
 - b the web page on the computer
 - c the path to where the resources are stored
 - d the path to where the computer (server) is located.
- 9 To send an email, you need to have each of the following, *except*:
 - a a file to attach to the email
 - b your own email address
 - c information to type in the email
 - d the email address of each intended recipient.
- 10 Each of the following reasons are issues with using email, *except*:
 - a emails are not private
 - b emails can be sent immediately
 - c not everyone has access to a computer
 - d you don't know if the recipient has read the email.

Short answer questions

- 11 Eli creates videos about his favourite football matches to share with viewers on the Internet.
 - a What input devices would be most suitable when he is creating his videos?
 - b He needs to edit his videos so that they are about five minutes long. What is the general name given to this type of application?
 - c Explain the process that can be used to place his videos on the Internet.
 - d Explain what type of storage is used to keep Eli's videos on the Internet.
 - e What generation of mobile network should his viewers have in order to watch Eli's videos on their mobile phones?

- f** Eli checked the video on his laptop. He can watch it but there is no audio. Give two possible explanations for the lack of audio.
 - g** Within two days, Eli gained around 400 subscribers to his videos, who will be notified as soon he produces another one. Give one characteristic of the information that describes when videos are shared with his subscribers.
- 12** Jarad plays online games using his television, which is connected to the Internet. He then records videos explaining what he likes about the games.
- a** What input device is most suitable when he is playing the games?
 - b** What type of television is most suitable for accessing the Internet?
- c** Jarad is part of an online group that plays computer games. They must all register using their email address to access the games and join the group.
 - i** Describe the other information that might be required during the registration.
 - ii** Explain one type of check that is used to ensure that each member enters the same information each time they log on.
 - d** As members play an online game, the number of points is shown in the top-right corner, along with the names of the players who are joining the game. State the type of output that is displayed on the screen.
 - e** State the name of the protocol that allows Jarad to chat with other players while playing the game.

IMPLICATIONS OF MISUSE AND CYBER SECURITY

4.1 Computer vulnerability

Organisations spend considerable amounts of time and money trying to make sure that their information systems are secure against various hazards, both natural and man-made. The importance of securing computer systems, their data and their network access to the Internet cannot be overstated.

Computer vulnerability is a weakness or flaw in one or more computer systems, or connectivity to computer systems. This weakness can be used to gain access and even damage the system or its data. The fact that the system is exposed to the possibility of theft or damage is its vulnerability. A computer system's vulnerability includes its hardware, software, data communications and users.

Vulnerabilities of systems and their data can be classified as being from external and internal.

External sources:

- ♦ minimal or no protection of computer systems and their data from natural disasters, for example floods and other natural phenomena (hurricanes, earthquakes, volcanoes)
- ♦ lack of protection from electrical power surges and spikes that could damage computer hardware, software and stored data files
- ♦ terrorist activities that target buildings or rooms with computer systems, for example bombings, arson.

Internal sources:

- ♦ errors by employees who overwrite or erase data
- ♦ no backup procedures in place for data files

- ♦ hardware and software not kept in locked rooms or passwords not created to access software
- ♦ internally produced software (known as **proprietary software**) which may be flawed and may as a result damage data
- ♦ lack of anti-virus programs to scan email attachments for viruses
- ♦ former employees whose passwords and security information have not been removed from the system
- ♦ employees who attempt to fraudulently obtain money using the company's name, for example by receiving payments for non-existent orders.



Fig 4.1 Power surges could cause damage to computer hardware

Threats and security

A security threat attempts to take advantage of a vulnerability or weakness in a system or its data. It indicates a possible danger to one or more computer systems, or by extension, a network. **Computer security** refers to the protection of hardware and software resources against their accidental or deliberate

damage, theft or corruption (in the case of software). Data security is the protection of data against intentional or accidental damage.

Computer users can represent the greatest threat to a company's computer system security. Only authorised persons should have access to the computer systems of an organisation. Computer networks are structured so that each user has access only to the various programs and data they need for performing their duties. Each user, for example, is provided with a username and password with which they log in to use network resources.

Deliberate damage

Hacking is the unauthorised access and use of networked or stand-alone computer systems to steal or damage data and programs. Deliberate damage can occur when there is a planned attempt to bypass all legitimate access restrictions. This damage usually occurs when security monitoring is not enforced. Network access logs should be maintained by network administrators to observe the resources being used at any time by users and the time of their logging in and logging out. These software access restrictions are necessary to ensure system security is maintained.

Accidental damage

Accidental damage to computer data occurs through genuine errors by computer users, such as overwriting the most recent data or entering incorrect commands. Damage also occurs as a result of **viruses** transferred from secondary storage devices or via the Internet.

Data communications

Valuable information is transferred via electronic channels to save time. Information is often needed to make vital decisions that depend on the content of the communication. However, all electronic transmissions can be intercepted by persons other than the intended receiver. Such efforts may represent deliberate attempts to access sensitive information.

A cyber threat is an unauthorised attempt to access a system, device and/or network via the Internet. Cyber security focuses on stopping threats that attempt to access a computer or other systems in the network. It protects the network by maintaining logs on attacks and attempted breaches, monitoring sources of attacks and protecting against future ones.



Fig 4.2 Cyber security focuses on stopping threats to systems in a network

Questions

- 1 Name two external and two internal sources that could make computer systems vulnerable.
- 2 Answer the following questions based on the terms security threat, computer security and data security. State the term that describes:
 - a the protection of data against damage
 - b the protection of hardware and software resources against damage
 - c an attempt to take advantage of a weakness in a system.
- 3 Select the appropriate beginning for each of the following statements:
 - a Deliberate/Accidental damage occurs when there is a planned attempt to bypass all computer login requirements.
 - b Deliberate/Accidental damage occurs as a result of viruses erroneously transferred from secondary storage devices.
 - c Cyber threat/Security is an unauthorised attempt to access a system via the Internet.
 - d Cyber threat/Security maintains logs on attacks and attempted breaches.

Organisations gather information from a wide variety of sources, including their employees, customers, suppliers and competitors. When people voluntarily provide information to organisations, it is usually for a specific purpose such as hospitals, clinics and health insurance agencies.

Measures should therefore be in place to ensure that information is not misused. However, security breaches are common. The use of information for purposes other than those for which it was originally intended is also common. Agencies may provide mailing lists to other companies seeking potential clients. For example, the names and addresses of persons between 18 and 25 earning above a given salary level may be sold by a bank to an associated insurance agent as targets for direct advertising. If you subscribe to a computer magazine, you may receive a letter from another company trying to sell you software. You may not mind this, but you should have a choice as to whether your personal information is passed on.

Proprietary data and software

As organisations become increasingly dependent on their information systems, it becomes more important to protect those systems and the data they contain. The data and software developed and used exclusively by the organisation is known as **proprietary data** and must often be used by employees for day-to-day operations. Organisations go to great lengths to protect the integrity and security of this data.

Computer fraud

Developments in computerised systems have contributed to a growth in electronic transaction processing and the use of computers to misuse information. This has led to a rise in computer-based fraud. The following examples show various ways in which information can be misused.

Propaganda

The use of computer systems to distribute information has inevitably resulted in their use for spreading both beneficial and harmful material. The widespread use of the Internet by computer users has created a readily accessible means of transmitting such material. In some countries such **propaganda** may be used to sway public support in favour of one party group or in an attempt to discredit opposing groups.

Identity theft

Criminals use computerised systems to steal people's credit card information, date of birth and other personal details that are typically used by banks to prove who you are online or by telephone. They then use those identities to make expensive purchases or facilitate cash transfers by using your information to make others believe that you are conducting the online transaction.

Identify theft can be prevented by:

- ♦ checking bank and credit card statements for unusual purchases
- ♦ using a secure website when making online purchases
- ♦ not making online purchases using a debit card which is connected to your main source of funds
- ♦ not using public computer systems to enter personal information.

Financial abuse

Another example of computer-based fraud is where individuals have gained unauthorised access to financial accounts and changed the details of those accounts to their advantage. There have also been examples of people setting up websites for companies that do not exist in order to accept people's credit card payments.

Phishing attacks

Phishing attacks involve the use of websites and email messages that try to trick you into entering your personal information. They may appear to look as though they are from an official organisation such as a bank or university in order to trick you into typing personal information such as your credit card number or password in a form or in reply to an email.

Other examples include email messages asking you to send money to help someone who will repay it at a later date. You should ignore these messages, as they are intended to steal money from you. Avoid downloading attachments in email messages from senders that you do not know since the attachment may contain a virus or malware that searches for passwords and other personal information.

Denial-of-service attack

A denial-of-service (DOS) attack occurs when computer systems or networks are overwhelmed with so much data and processing that it makes it difficult or impossible for legitimate users to access their computer systems, devices or other network resources. This type of attack is similar to 20,000 students trying to access the CXC web portal at the same time to see their results online. Signs of an attack include:

- ♦ a decrease in network performance, especially when attempting to open files stored on the network or the cloud
- ♦ difficulty or inability to reach a regularly accessed websites or any website
- ♦ receiving lots of junk email.

This results in an inconvenience to a majority of users on the network although the person who caused the attack usually intended to sabotage only an organisation or individual.

Industrial espionage

Some organisations try to gain an advantage over their competitors by illicitly gaining access to information about their marketing strategy, latest research, expansion plans and so on. In the past they would have done this through break-ins, illegal photographing of documents, and insiders passing out information. Now it can be achieved by hacking into organisational databases and viewing the information they contain.

Electronic eavesdropping

It has been shown that it is possible to gather data from a computer from a distance, by using commercially available equipment which can receive and process the radiation emitted by the monitor. The data being displayed at the time can then be observed without the knowledge of the computer user.

Electronic eavesdropping is the use of electronic devices to monitor electronic communications between two or more groups without the permission of any of the communicating parties. This includes computer data communications, voice, fax, phone and email. Some computers can be modified to intercept information being transferred in any electronic form along a communication channel such as telephone lines, radio waves and so on. In some companies, it is the policy for all electronic communications to be monitored, including the telephone and email messages of their employees.

When this is done by unauthorised persons, however, the threat of invasion of privacy becomes real. It is a good idea to avoid transmitting sensitive information in electronic form unless there is an encryption system in place to ensure that the data is secure.

Most companies ensure that their data is encrypted (often by the communication software) before it is transmitted. If intercepted by the wrong persons, it is useless since the information is unreadable. The intended receiver will have the decryption key with which the data can be decoded and read. However, even this is often not enough to stop the most persistent eavesdropper from intervening.

Software and music piracy

Many software programs and music files can be accessed online by users from anywhere in the world. However, these files are legally owned by individuals or organisations. There are rules or licences for all programs and music specifying the permissions and limitations on how programs or music should be used. Therefore, when you use an online program or listen to a recording of a song, there are some restrictions on what you can do with it.

Software or music piracy occurs when someone does not abide by the rules to obtain permission from an owner. This type of piracy results from illegal use, sharing, selling or distribution of copies of software or music, and prevents the rightful owners from getting money due to them for their creative efforts.

Unauthorised access

This is usually referred to as 'hacking'. Hacking involves trying to electronically 'break into' a system to which the individual does not have authorised access. The purpose behind this infiltration varies; some hackers see their activities as a form of game-playing, where they match their computer skills against those of an adversary and just gaining access is sufficient for them. Others are more destructive in their intentions: they target organisations that they are antagonistic towards and commit acts of 'electronic vandalism' such as changing critical data.

Questions

- 1 Explain the difference between:
 - a computer fraud and propaganda
 - b phishing and identity theft.
- 2 For each of the following state the type of software threat and indicate whether it affects a single computer or multiple systems:
 - a trying to electronically 'break in' without authorised access
 - b hacking and viewing electronic information
 - c using electronic devices to monitor electronic communications
 - d overwhelming a system with so much data and processing that it makes it difficult to access.

Whether a threat is deliberate or accidental, all methods should be taken to prevent it from occurring or to minimise its effects. A countermeasure is a procedure, either physical or logical, that recognises, reduces or eliminates a threat.

Data protection refers to computer users who can protect their data against loss or damage. It also refers to data protection laws, which set down rules about what information can be kept by others about you.

Surveillance

Computer surveillance involves the use of technology to gather information from the user and from the computer, often without the user's knowledge. Monitoring entrances and exits together with methods to identify authorised personnel is a typical method used to identify a threat. This method of security is employed to protect the physical surroundings, that is the building and rooms with computers in them. Common approaches to physical security include:

- ♦ closed-circuit TV monitors
- ♦ electronic alarm systems
- ♦ computer-controlled locks that check employee badges
- ♦ biometric recognition, such as fingerprints, retina scans and voice to authorise entry to different rooms or buildings
- ♦ access codes.

However, there are some negative consequences of computer surveillance, including:

- ♦ loss of privacy for the user
- ♦ lack of security
- ♦ potential misuse of information, possibly for monetary gain
- ♦ difficulty in determining the source and possible scope of surveillance activities in some organisations
- ♦ limited measures to prevent computer surveillance.

Depending on the purpose of the surveillance, it can be used to create or prevent an attack. There are several techniques for surveillance, including monitoring software and hardware devices.

Monitoring with utility software

All data that passes into and out of a network can be monitored. This is also known as '**packet sniffing**', where a packet is the message being checked. Messages can be monitored using utility software or by using a computer on the network which can observe all packets passing through the network.

Monitoring with hardware devices

Physical or hardware devices called '**bugs**' are keystroke loggers implanted in the keyboard. This device can record all keystrokes made by the user over a period of time. The device can then be retrieved and the keyed information can be reproduced. Other more sophisticated devices, which can obtain more information, can be inserted into the computer itself. The disadvantage of hardware devices is that placement and retrieval requires physical entry into the place where the computer is stored. This can be a legal offence and is a violation of privacy without legal authorisation.

Protection from nature

Data should also be protected from natural disasters, including the risk of fire, storm damage, dust and humidity. Organisations use fireproof cabinets and safes to keep critical data stored on media such as optical disks, tapes and microfilm to protect against such hazards. Computer systems should make use of electrical surge protectors to protect computer hardware against electrical surges and spikes. The effect of power outages can be minimised with the use of an **uninterruptible power supply (UPS)**. This device contains a battery which supplies equipment with electricity during a power outage so that data can be

backed up and a normal shutdown of the hardware can be performed (Fig 4.3).



Fig 4.3 Uninterruptible power supply (UPS) provides electricity for a short period after power outage so that computer data can be saved and systems can be safely shut down

Protection from theft

Some schools often lock computers to the desks to prevent theft of the system units and peripherals. However, there is still the theft of memory chips, hard drives, CD and DVD drives, printers, inks and other accessories. Organisations should limit access to authorised persons and maintain records and logs of computer usage.

Computer viruses

A computer **virus** is a program that infects computer files and makes them do something unexpected or damaging. A copy of the virus program is inserted into a computer file, and when the file is used and loaded into memory, other files become infected. Computer users are unaware that a program or a file has become infected. If one of the infected files is sent by email, or given to other users on a device such as a USB memory stick, then other computers are infected and the virus spreads.

Viruses are an increasing threat to computer systems. In 1986, there was only one known computer virus.

Today, hundreds or thousands of new viruses appear every day.

There are three main types of virus:

- ◆ those that infect program files. The virus code is attached to program files and when the program is loaded, the virus is loaded as well.
- ◆ those that infect system or boot files. The boot file is a small program that tells the computer how to load the rest of the operating system. By infecting this boot file, the virus is loaded into memory and is able to run whenever the computer is on.
- ◆ macro viruses. These are written in a language associated with an application such as Microsoft Access. The macro virus is carried by a database file and is executed when it is opened.

A **worm** is another electronic threat. Unlike a virus, it does not require a host program in order to be transmitted. Worms can be transmitted via email and are capable of copying themselves into memory. Mass mailing worms can create infected email messages and send them to the addresses saved on the infected computer.

Preventing viruses

Virus protection programs not only scan a computer's data for harmful viruses but also protect from and intercept viruses attempting to infect data in system or application software.

The best way to protect a computer against viruses is to:

- ◆ Install anti-virus software. **Anti-virus software** protects the operating system, programs and files against viruses. It regularly scans a computer for viruses and then removes any viruses that are found. Anti-virus software can be set up to automatically check storage devices, Internet downloads and emails for any viruses. Because new viruses are being discovered on a daily basis, leading anti-virus software products such as Avast, AVG and

McAfee have anti-virus updates automatically downloaded from their websites to keep protection up-to-date.

- ♦ Turn on program virus protection. Some programs – for example, Microsoft applications – have built-in macro virus protection. When this is the case, make sure that it is turned on (enabled).
- ♦ Try to know the origin of each program or file you use. In the age of the Internet, this is very difficult – hence the need for anti-virus software. As a rule, beware of free software and software downloaded from the Internet.
- ♦ Never open an email attachment that contains an executable file with an extension EXE, COM or VBS, even if you know who sent the email. This is how many viruses are spread.

Protecting files and databases

A database contains the raw data for information. Often the databases in an organisation are its lifeblood. Companies therefore cannot afford to lose records. Maintaining several generations of backups as well as archives of all its critical files are advised. The master and backup files should be stored in fireproof safes, or preferably in separate buildings away from the main computer centre.

Backups and archives

Making **backups** (copies) of files is always important. For businesses and other organisations that depend on databases it is essential. Files can become damaged, corrupted or even lost. Think what would happen to travel agents if they could not use a database for booking flights or to doctors who could not access patients' details. To prevent situations like this happening, the regular backing up of files is essential. If a file does become damaged or corrupted, then the files, and the data they contain, can be restored (or recovered) from the backup copy, and business can continue as normal. How often backups are made depends on how valuable the information is.



Fig 4.4 Files can be restored from backup copies

Most modern networks have software which automatically performs backups of data files to magnetic tape or CD-RW. Backups can be performed after each work day, every other day, or as often as deemed necessary.

Some backups are also stored in a remote location to protect against disasters such as hurricanes, volcanoes, floods or earthquakes that would destroy any backups in the immediate vicinity, along with other equipment. Another alternative, called remote data backup, stores backups in cyberspace. Users and companies buy online storage for easier access to data. However, data stored online is prone to deletion if the online storage company goes out of business.

An archive preserves files that you no longer need on a regular basis. By putting them in an archive, storage space on your hard disk (or network drive) can be released for use by current files. Archives can be extracted if the need arises, usually for reference. For example, an organisation may preserve archives of past ledgers, receipts and tax forms for future reference only.

Network and cyber security

Companies address cyber threats with **encryption** or **decryption** techniques. They encode data before transmission so that it appears unintelligible unless it is decrypted using a software key.

Users on a network can each be given a username with an individual password. This prevents other users accessing an individual's file, changing program

settings, or installing, copying or deleting software. Other techniques include preventing virus attacks through networks, email or by sharing secondary storage devices and media.

Copyright and piracy

Copyright is the name given to the protection in law of the rights of the person(s) responsible for creating such things as text, a piece of music, a painting or a computer program. The illegal copying and stealing of software costs the software industry millions of dollars a year. A copyright law would make it a criminal offence to be caught copying or stealing software. It would also make it an offence to:

- ♦ copy or distribute software without permission
- ♦ run copyright software that has been bought on two or more computers at the same time unless the software agreement (licence) allows it.

The Intellectual Properties Affairs office in a country would be responsible for enforcing the law on copyright and campaigning against software piracy (Fig 4.5).



Fig 4.5 Software piracy is against the law in many countries, but is not outlawed worldwide

Software piracy is the theft of computer programs and the unauthorised distribution and use of these programs. In the Caribbean, countries are enforcing copyright and piracy laws for music, printed material and software.

The main types of piracy are:

- ♦ copying software (and its packaging) to try to make it look like a genuine product
- ♦ copying and selling recordable CD-ROMs that contain pirated software
- ♦ downloading software from the Internet; just because software can be downloaded from certain sites does not mean that it is free or legal for you to download it
- ♦ using software on more computers in a network than the number of computers for which there are software licences.

Because of all of these activities, many countries have enacted laws which make it illegal to misuse computers. People found guilty receive a large fine or a prison sentence. For example, it is illegal to do any of the following:

- ♦ deliberately plant computer viruses that damage program files and data
- ♦ copy computer programs illegally (computer piracy)
- ♦ hack into a computer with the intention of seeing or altering information
- ♦ use a computer to commit crimes (fraud), for example to create a fictitious worker and get money paid into this non-existent person's bank account
- ♦ use your employer's computer to carry out unauthorised work.

Some countries also have legislation that seeks to protect the individual from the potential misuse of personal information. Contents of such legislation include:

- ♦ Information should be used only for the purpose for which it was provided.

4 Implications of misuse and cyber security

- ♦ The individual has the right to examine the contents of any personal record representing the individual.
- ♦ The information must be accurate. Information should be periodically updated to be a true reflection of the individual.
- ♦ Information should not be held for longer than necessary.
- ♦ All measures necessary for ensuring the security of the information against physical and electronic threats should be in place.
- ♦ The privacy of the individual should be protected.

Questions

- 1 Explain why each of the following methods of file storage is important:
 - a making backups
 - b archiving.
- 2 Indicate whether the following statements are true or false:
 - a Virus protection programs only scan a computer's data for harmful viruses.
 - b Software piracy is the authorised distribution and use of computer programs.
 - c An individual has no right to examine the contents of any personal record representing him/her.
 - d Information should not be held for longer than necessary.
 - e The privacy of the individual should be protected.
- 3 State the type of protection for each of the following descriptions:
 - a to keep critical data stored on media such as optical disks protected from risk of fire
 - b to protect computer hardware against electrical surges and spikes
 - c to prevent theft of the system units and peripherals
 - d to monitor suspects, often without their knowledge.

There are numerous examples of how information systems play an increasingly important part in your life – from programmable televisions and remote-

control devices to e-commerce using the Internet. It is important therefore to be aware of, and be able to discuss, the following effects of computers.

Table 4.1 Effects of IT in the workplace

Social impact

- ◆ Less social contact among employees
- ◆ A large increase in the use of computer games (time wasting; no social contact; addictive; some are educational)
- ◆ It may become easier to keep in touch with people (email, social media)
- ◆ Privacy considerations – how secure is personal data?

Work patterns

- ◆ The Internet and WANs have allowed employees to work from home
- ◆ Advantages include flexible hours, a more relaxed atmosphere and no commuting
- ◆ Disadvantages are a lack of social contact and possible disruptions or distractions
- ◆ Advantage to company includes no need to provide office space, heating, refreshments and so on

Cashless society

- ◆ Workers are automatically paid by electronic funds transfer (EFT) into their bank accounts
- ◆ Credit and debit cards are used more for payments
- ◆ Main advantage is no need to carry cash
- ◆ Disadvantage is the possibility of fraud or lost or stolen cards

Employment

- ◆ Practical skilled jobs on the decline
- ◆ Possible redundancies if a more efficient IT-based system replaces workers
- ◆ New jobs created in IT-related fields such as programmers, systems analysts, robot maintenance
- ◆ Workers need to be retrained

Health and safety

- ◆ Attention needs to be paid to posture problems from sitting for long periods at a computer
- ◆ Radiation hazards from monitors and eye strain
- ◆ RSI (repetitive strain injury)

Changes in the workplace

The ICT revolution has brought about widespread changes in the workplace. Most offices now use computer systems, often connected by a LAN or WAN. Most offices will therefore have their networks connected using cables or with wireless technology. Applications such as word processors, databases and email, and mobile telephones are used by millions of people every day. Video conferencing via WAN and the Internet enables meetings to take place without the participants having to leave their offices.

Computers are used in many economic sectors and, as the need for managing information becomes more important in these areas, employees are required to become more skilled in the use of information technology to perform their duties. The skilled use of hardware and software is necessary for most occupations that involve information collection, processing and distribution.

Loss of jobs and retraining

Computers are now being used for jobs that were previously done by people. For example, as more

customers buy products online, staff in stores may be reduced. The use of email may replace the purchase of stamps and delivery of mail, but, on the other hand, there could be an increase in the delivery of products that were purchased online.

Work that has been lost includes:

- ♦ repetitive jobs, such as telephone operators who direct calls to office extensions
- ♦ dangerous jobs, such as defusing bombs or working in areas with extreme heat or cold
- ♦ office jobs that can be automated or take less time using ICT skills, for example typing or re-typing documents that can be saved and edited for future use.

Most jobs now require some ICT skills and so, for some people, retraining is necessary to remain in the workforce. Learning to use a computer and typing quickly are among the more important aspects of retraining. Some people take short courses or learn new on-the-job skills to remain marketable. IT skills help to keep funds in the business since completing jobs in-house using IT saves the money it would cost to **outsource** them.

Telecommuting

Work can now be accessed by employees in their location instead of by the more traditional method of travelling to work. Millions of people, known as telecommuters, teleworkers or remote workers, now work, on a full- or part-time basis, at home or move around the world using a computer or mobile device to communicate with their employers and/or clients.

This has the advantage of reducing office space, with less electricity or air-conditioning usage, but telecommuters must also face higher utility bills if they are working from their homes. Some businesses may compensate their employees for this added expense.

However, telecommuting can be isolating for the employee, as one of the more enjoyable aspects of a job in an office is often socialising with other people. Distractions in the home environment may reduce productivity.

Social concerns

The widespread use of information systems has led to more efficient ways of working and to a decrease in the hours that many people have to work. This allows more time for people to spend on leisure pursuits. Without a second thought, millions of people use personal computers, mobile devices and information system devices such as video recorders. The growth of telecommunications, including the Internet, has led to a situation where people can share information in a '**global village**'. Distance is no longer an issue, with people communicating as if they were living closely together in a small village.

There is disagreement about the effects on young people of spending a long time using computers and playing computer games. Some people argue that prolonged use makes youngsters withdrawn and less likely to socialise with others, whereas others argue that playing games can develop problem-solving skills and encourage collaboration and teamwork.

Health concerns

Millions of people use computers regularly for work, education and leisure. As with any other equipment, computers should be used safely and in a way that doesn't harm users' health. This is important, as there is evidence that using a computer for a long time, and not properly using computer equipment or furniture, can affect your health and result in injury. Some examples of this are given in Figure 4.6.



Fig 4.6 Using a computer for a long time without proper furniture and posture can result in health concerns

Repetitive strain injury

Aches and pains, swelling and difficulty of movement are all symptoms of disorders affecting fingers, wrists, arms and neck that can be caused by lengthy or improper use of computers. The common name for these disorders is **repetitive strain injury (RSI)**. RSI can be extremely painful and is caused by long and regular periods of typing or using the mouse, or even poor workstation setup.



Fig 4.7 Repetitive strain injury (RSI) can be caused by long periods of typing and using the mouse

What can be done to stop RSI?

- ◆ Take regular breaks from the computer or change activity. Short breaks of 5–10 minutes every hour are recommended.
- ◆ Place the mouse immediately to the left or right of the keyboard.

- ◆ Hold the mouse loosely and don't use the mouse continuously for long periods.
- ◆ Use wrist and/or arm rests.
- ◆ Arrange your desk so that your keyboard is easy to use, tilted and separate from the screen.
- ◆ Make sure that there is enough space in front of the keyboard to rest your hands or arms.
- ◆ During regular breaks, stretch and move your hands, wrists and neck as a form of exercise.
- ◆ Relax – RSI can be caused by tension.

Back problems

Back problems can be caused by poor or incorrect posture when using furniture or equipment.

What can be done to stop back problems?

- ◆ Use a chair that is adjustable in height, able to swivel and that has a tilting backrest.
- ◆ Make sure that the chair is at the correct height for you to use the keyboard and screen.
- ◆ Sit in a comfortable position and regularly change the way you sit (consider your posture).
- ◆ Use a desk large enough to take all the computer equipment.
- ◆ Take frequent short breaks and stand up or walk around.

Eye problems

Eye strain is the most common health problem linked to using computer screens for long periods. Eye problems are also linked to poor lighting, glare and being too close to, or too far from, the screen. The size of fonts and colours used in software can affect the eyes.

What can be done to stop eye problems?

Computer screens should:

- ◆ not flicker
- ◆ have brightness and contrast settings that can be easily changed
- ◆ tilt and swivel
- ◆ be positioned to avoid glare and reflections from lights or windows, and be fitted with glare-reduction filters.

Stress

Using computers, or having your work monitored by computers, can be stressful. Also, modern communication technologies, such as email, portable notebook computers and mobile phones, mean that some people cannot take proper breaks as they can always be contacted immediately. This too can be stressful.

Environmental concerns

The widespread adoption of information systems has also had environmental effects. On the one hand, the need to power millions of computers has increased electricity consumption while, on the other hand, the consumption of electricity and other forms of energy has been reduced as computers carefully control air-conditioning and heating systems. Information systems have enabled **teleworking** from home. This can mean less travel to and from work and therefore a reduction in traffic pollution. Although the age of the truly paperless office is some years away, there has already

been some saving on the use of paper (and therefore trees) as data is communicated and stored digitally.

Legal, ethical and moral effects

The legal, ethical and moral effects of information systems will continue to be an area of concern to users. A great deal of personal information is held on computers. The Data Protection Act tries to ensure that personal information is held and processed responsibly. Laws have also been passed to try to stop hacking and the pirating (stealing) of software. All of this raises some important ethical and moral issues, such as the following:

- ◆ How far should the law go in giving government officers, such as the police, access to everyone's personal data or emails in order to fight crime?
- ◆ How far should established and new technologies, such as closed-circuit television (CCTV) and microchip smart cards, be used to monitor people's activities?
- ◆ What will happen to people who cannot afford to buy, or gain access to, a computer system?

Table 4.2 *IT skills required in the workplace*

Category of worker	Skills required
Office employees	<ul style="list-style-type: none"> ◆ Word processing and document preparation ◆ Budgeting – for example, preparing financial statements and invoices ◆ Communications – via fax, email, forum/newsgroups ◆ Basic troubleshooting of hardware and software
Teachers	<ul style="list-style-type: none"> ◆ Word processing, spreadsheet manipulation ◆ Database management – creating and searching databases ◆ Preparing presentations ◆ Network use – accessing and using school LAN resources ◆ Operating hardware – computer systems and peripherals (for example, printers, scanners, multimedia projectors) ◆ Installation and basic troubleshooting of hardware and software
Engineers	<ul style="list-style-type: none"> ◆ Software programming – the ability to design, test and implement new software ◆ Installing hardware and software ◆ Manipulating peripherals such as sensors, controllers and graphics tablets (design) ◆ Using communications systems – LAN, WAN, Internet

(continued)

Table 4.2 IT skills required in the workplace (continued)

Category of worker	Skills required
Medical personnel	<ul style="list-style-type: none"> ◆ Word processing and document processing ◆ Expert system consultation, examining references for surgical procedures, maintain inventory of medical supplies ◆ Prepare budgets, medical bills, insurance claims using financial software for – example, QuickBooks ◆ Manipulate hardware, patient monitoring and imaging systems – for example, ultrasound, MRI and CAT scan technology ◆ Conducting teleconferencing meetings among doctors in different locations
Musicians	<ul style="list-style-type: none"> ◆ Using music notation software for composing music and preparing lyrics ◆ Using MIDI (musical instrument digital interface) hardware to produce music and interfacing with computer systems to add instrument sounds, special effects ◆ storing and retrieving music tracks from optical storage media
Mass media personnel	<ul style="list-style-type: none"> ◆ Word processing – used for preparing articles, news scripts ◆ Database searches and information retrieval – searching for past articles, news articles from other countries ◆ Communications using email, fax, forums/newsgroups ◆ Using hardware and software for film and sound editing before going to the final press
Law enforcement personnel	<ul style="list-style-type: none"> ◆ Word processing and document preparation – used for preparing case reports, letters and so on ◆ Database searches – accessing records kept on known offenders
Movie industry personnel	<ul style="list-style-type: none"> ◆ Word processing and document preparation – used for preparing movie scripts ◆ Animation – some movies are made with the use of computer graphics and animation for some scenes ◆ Accounting and budgeting software – used to create cost and income estimates for movies

Questions

- 1 Name two changes in employment if computers replace workers.
- 2 With increased use of computers, explain what causes each of the following health problems:
 - a back problems
 - b eye problems.

This topic lists the jobs of some personnel working in computer-related fields.

Computer support specialist: provides technical assistance directly to computer users who need assistance with a specific application.

Computer programmer: translates analyst-prepared specifications for software into algorithms and converts the algorithms into applications programs. The programmer will write, test and maintain the application software.

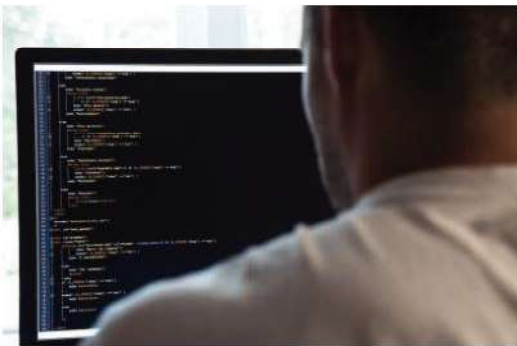


Fig 4.8 A computer programmer

Systems analyst: analyses systems currently in place to assess their suitability for computerisation or recommends upgrades for existing computer systems.

Database administrator (DBA): designs, creates and maintains the integrated database. The integrity and security of the database are also the responsibility of the DBA.

Network administrator: designs, develops and maintains local area networks and wide area networks, and schedules maintenance of the network components. Sets up access and security measures such as user IDs, passwords and firewalls. Also ensures that all shared resources, such as printers and disks, are monitored and working properly.

Network engineer: attends to any hardware faults and malfunctions in the equipment. Installs new systems and services computers.

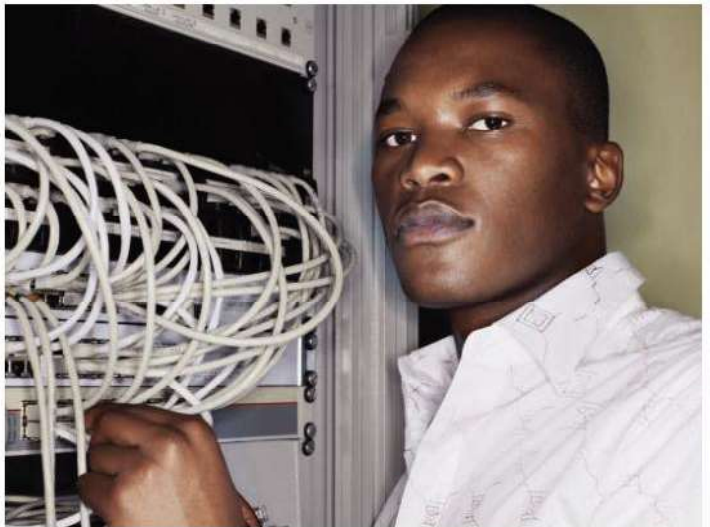


Fig 4.9 Network engineer working with a server

Social media specialist: communicates with the public using social media to create and share content using social media platforms such as Twitter. Manages their employers' social media accounts, working to build the brand's reputation.

Software developer: develops the applications that allow users to complete specific tasks on a computer or another device.

Systems administrator: monitors and maintains the system security. Determines the organisation's system needs and adds users to a network, and assigns and updates security permissions on the network.

Web developer: builds websites, which involves writing the programming code necessary for an efficient and stable website. Web developers oversee and direct the development of the website from idea stage to its final published state, ensuring that loading times are minimised so that users can access information quickly.

Questions

- 1 List three types of administrators that work in computer-related professions.
- 2 Explain the difference between the jobs of a computer support specialist and a social media specialist.

We need systems in almost every aspect of human life to prepare meals, maintain cars, complete our assignments and travel to work or school. An **information system**, however, is responsible for the collection, processing and overall management and distribution of information.

Computers and communication devices can manage large amounts of information at a faster rate than manual systems, such as filing, sorting and mailing.

When choosing a computer information system for a particular situation, you need to consider:

- ♦ what hardware is used, such as input, storage and output devices

- ♦ what software is used, including the choice of custom-written, specialised and general purpose software
- ♦ what processing takes place
- ♦ what human–computer interface is used
- ♦ which people are involved and what work they do
- ♦ what data is required.

The first four points were discussed in Chapter 1. You can now apply this knowledge to decide which systems and applications are appropriate in various computer-related fields. Some examples are illustrated in this chapter, such as commerce, education, law enforcement, medicine and recreation. You should first recognise the advantages and disadvantages of computerised information systems, which are summarised in Table 4.3.

Table 4.3 Advantages and disadvantages of computerised information systems

Advantages	Disadvantages
<ul style="list-style-type: none"> ♦ Save enormous amounts of paper and filing space ♦ Rapidly find, calculate and sort data ♦ Work automatically ♦ Data easily imported (brought in) from another system or program ♦ Data easily exported (moved or copied) from one system or program to another ♦ Data easily entered (by keyboard or scanner) or updated ♦ When computers are linked together in a computer network, more than one person can access the information at the same time 	<ul style="list-style-type: none"> ♦ Some systems can be complicated and/or require a lot of time to be spent on staff training ♦ The computer(s) running the information system may not work due to an electrical failure or a hardware/software fault. If everything is computerised, no work can be done at these times unless backup power or systems are available ♦ Data may be incorrect ♦ Some people may attempt to access confidential information. Therefore, security is extremely important

Business

Commerce

Computer systems are used to help make organisations more efficient, cost-effective and responsive to the needs of their customers. Popular areas are research and development of new products and services, as well as marketing and the monitoring of trends in sales.

Research and development

Computers in this industry analyse existing sales data and the likely market for a new product. Appropriate hardware includes network and personal computers to process images, scanners to input designs, and printers and graph plotters for producing new designs and advertising signs. Specialised software programs are used to create the detailed designs for the product.

Stock management

During product development and manufacturing, each product must be monitored very closely. Keeping an automated stock control system for any raw materials purchased can ensure that there is always an adequate supply for the manufacturing process. The system can also provide early notice to reorder materials before stock levels become critically low.

Marketing and distribution

Marketing departments inform customers of new and existing products. They can use computers to automate the production of advertising material, using word-processing and database software. Computers and scanners also allow vivid product pictures to be included in advertising.

Sales

You may know of small shops where computers are not used, and goods are still priced individually by hand. However, when prices change, the price labels must also be changed. Itemised receipts for the products sold sometimes have to be handwritten. Checking the stock levels in the shop before re-ordering items is done by individually counting the different items in the product lines.

Compare this with a business that uses a computer system. Goods do not need to be individually priced (Fig 4.10). This is because each item has a barcode that is swiped through a barcode reader at the point of sale (POS) computer terminal at the checkout. The

price for each item is maintained by database software. All the items bought by a customer are automatically listed and added up and any discounts due to loyalty cards are given. Payment can be made using credit or debit cards using a reader. The money is automatically transferred through networked computers to the supermarket's account. A bill, listing each item that has been bought, is then printed and given to the customer.



Fig 4.10 A barcode reader can be used to check inventory and prices on products

Each checkout computer may be linked to a warehouse and the main computer system through a wide area network. As the items are swiped through the barcode readers at the checkouts, the stock levels of each product line are automatically updated. When the stock of a product gets too low, the product can be automatically re-ordered from the warehouse. The computer system can give managers instant access to sales figures so that they can see which items are selling well at any branch in the country.

Table 4.4 Hardware and software for commercial applications

Industry	Example of application	Hardware	Software
Marketing and distribution	♦ Automated direct mailing to inform customers of new products	♦ High quality printers for flyers and advertising material	♦ An inventory control system ensures supply to retail agents is efficient
Sales	♦ Monitoring of stock levels and instant payment of goods	♦ Point-of-sale terminals ♦ Use of credit or debit cards	♦ Software for e-commerce, selling direct to customers
Banks	♦ Electronic money transfers	♦ Networked automated teller machines (ATMs)	♦ Specialised ATM software ♦ Banking software

Banking

Banks now depend on computer systems to run their business. Funds are instantly credited and debited from customers' accounts using special banking software. Networked automated teller machines (ATMs) allow customers to withdraw cash and check their account balance. Credit and debit cards enable customers to buy goods and services at most retail outlets, with the purchase cost automatically debited (deducted) from the customers' accounts. Online banking is replacing the need to process millions of cheques. Customers can access online banking via computers or their mobile devices. Some of the services offered with online banking are:

- ♦ checking a bank balance
- ♦ transferring money between accounts and to other customers' accounts
- ♦ paying bills online
- ♦ viewing/printing current and previous bank statements
- ♦ applying for new accounts.

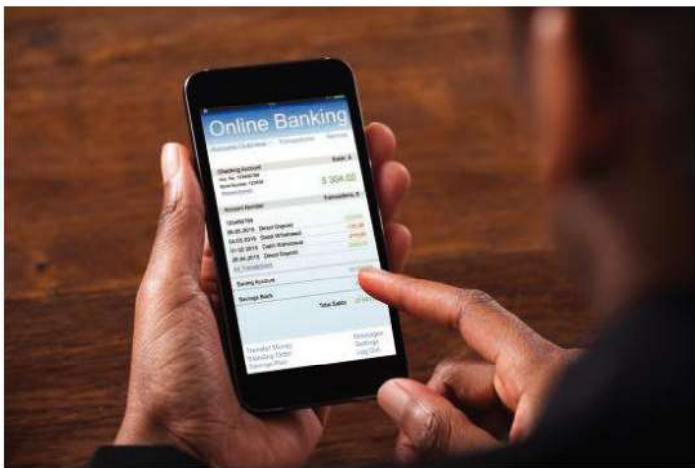


Fig 4.11 Online banking can be done at any time, from anywhere, using a mobile device or computer

Education

Databases

In schools, the collection and organisation of student information is made more efficient by using database management programs. Before widespread

computer use, student information was kept on sheets of paper or index cards, or in folders kept in filing cabinets. With computerised database records, searches are faster, and information is produced when it is wanted.

Teaching and instruction

Software designed specifically for instruction is available for students and teachers alike. Computer Aided Instruction (CAI) and Computer Aided Learning (CAL) software can be purchased for many subjects and cater for students of any age. Students can use them to study topics at their own pace, take practice tests and monitor their progress as they move from one topic to the next. Software such as Moodle® also helps with group work, even if the group members are located in different areas of the country or the world. This form of collaborative learning helps people learn new information together.

Using online software, instructors can also monitor online quizzes and evaluate the results, including how long each student spent completing each question in the quiz (Fig 4.12).

See all course grades		
Name	Attempts	High score
Denise	87.5% Thursday, 29 March 2018, 1:51 PM, (12 mins 50 secs)	87.5%
Claudia	50% Thursday, 29 March 2018, 7:52 PM, (39 mins 47 secs)	50%
Sandy	90% Thursday, 29 March 2018, 6:02 AM, (22 mins 24 secs)	90%
Paul	87.5% Wednesday, 28 March 2018, 10:09 PM, (25 mins 10 secs)	87.5%

Fig 4.12 Using Moodle software to evaluate the results of an online quiz

With so much information available on the Internet, information or even complete essays can be found online or purchased from others. Assignments obtained by these methods and submitted as is or slightly rearranged for grading is illegal. Using someone else's work or ideas and making others believe that it is your own is called plagiarism. Some schools and universities expel students for plagiarising and certificates awarded can be made 'null and void' if students have plagiarised.

Hardware devices used in classrooms include multimedia-ready computers, networks, multimedia projectors, printers, earphones and microphones for independent work.

Medicine

This area covers a wide range of applications. However, the most important ones are found in medical research, which includes access to online medical information and online health services.

Medical research involves using medical models and information systems which study the human body as well as storing details of patients and their illnesses.

Medical information systems

Most doctors today use a medical information program to keep details about their patients and their illnesses. Patient information can be brought up on computer screen while you are seeing the doctor. The medical information program, apart from having your name, age and address, will also have a record of your illnesses and of any drugs given to you. Once the doctor has found out the cause of your illness, and has entered the prescribed medication, the computer can print a prescription that can be taken to a pharmacist. Sometimes, the prescription can be sent electronically from the doctor's database to the pharmacy's database if the two are connected via an extranet.

Other medical health services, such as imaging and ultrasound services, can be connected to a network along with those of medical professionals and pharmacists. Patients' information, together with test results, can then be shared via the network. Medical personnel across the world can be given access to the network for consultations and faster diagnoses.

Expert systems

The **expert system** is one example of artificial intelligence that is designed to store a vast amount of data (known as a knowledge base) related to past aspects of the application area. It draws on this data,

along with certain rules for processing, to come up with a 'prediction' for the outcome of a current situation. In the medical field, the expert system may provide a diagnosis when given a set of symptoms or image scans of the body.

Medical models

Modern medical whole-body scanners can collect a large amount of data about a person's internal systems. The data collected can then be processed on a special computer using customised software to produce a three-dimensional model of the whole body or a part of it. This information is usually collected as a series of 'slices' and the program 'glues' the slices back together to make the three-dimensional model. This model allows doctors to locate precisely, for example, a tumour, and helps them to decide what to do next (Fig 4.13).

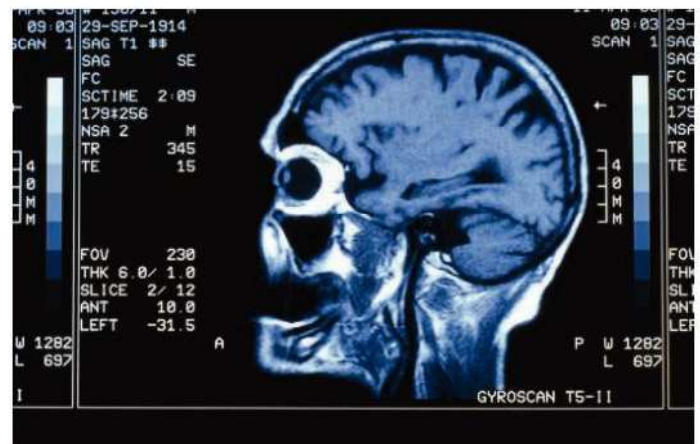


Fig 4.13 A slice image through the brain can be obtained by magnetic resonance imaging (MRI)

Virtual-reality simulations

Virtual reality uses software applications to create an artificial environment which gives users the feeling that they are part of that environment or reality. A special headset fits around the user's face, covering the eyes and sometimes the ears to block all sights and sounds from the immediate surroundings. Other images and sounds are then used to make the 'virtual world' seem more realistic. A user's sight and hearing are the two senses mostly used with virtual reality. However, some programs use touch as another

sense for a more realistic experience. As an example, surgeons can now be trained to perform new surgical procedures without endangering life. A virtual-reality human model can be created, and a trainee surgeon can perform the operation.

The sensor and control systems connected to the operator can give feedback to the surgeon to create an illusion of the real thing. The feedback can be visual, through the imaging system, but more important is the feedback which gives the sense of touch. This will help the surgeon to master the safe manipulation of the surgical instruments.

Virtual reality is also used in actual surgery. For example, the 3D image of a brain tumour can be created from a series of slice images produced by scanning the affected brain, using Magnetic Resonance Imaging (MRI). Virtual reality can also be used in other training simulations (for example, pilots or deep-sea divers) and interactive games for all ages.

Law enforcement

Computer systems help security forces around the world in their fight against crime. Millions of criminal records are held on computer database systems throughout the world. Each year computer technology is used to process requests for information from police officers who want to find information about suspects, robberies and stolen vehicles. Searching for crime statistics, storing new criminal records, accessing databases in other countries and communicating with army mobile units are just some of the uses made of computers in law enforcement. This information can then be provided to officers in seconds. Regional security systems also have networks that participating countries in the region use to share surveillance information.

A fingerprint system can provide fast access to databases of convicted criminals' fingerprints as well as marks collected from scenes of crime. This allows the

police to search the records to find matches for crime-scene marks and to confirm the identity of anyone arrested.

Hardware includes fingerprint scanners, portable and handheld computers such as Personal Data Assistants (PDAs), printers and digital cameras for photos of suspects and crime scenes.

Driver licensing databases

By law, all drivers of vehicles on public roads must have a driving licence. A computerised driver licence system can issue driving licences and vehicle registration documents. Details on every driver and every vehicle can be kept on a massive computerised database involving millions of records. Apart from licensing drivers and vehicles, the database can be accessed by the police in their fight against crime.

If these millions of driver and vehicle records were paper-based, it could take minutes or hours to find the information required. By using a computer, the information can be found in seconds. Compared with paper-based systems, computer information systems are particularly impressive when carrying out searches across a number of different categories.

Recreation and entertainment

Game-playing is one of the most common uses of computer systems (Fig 4.14). Computer games have become a multi-million-dollar industry in the United States and software producers are constantly striving for new ideas for themes and concepts for their consumers. Computer hardware can be configured to suit game-playing specifications, with powerful graphics cards, amplified sound systems, high-resolution monitors and powerful CPUs. Game-playing consoles have also been created as dedicated game systems.

Virtual reality can also be used by game players. For example, some programs include a physical device that is attached to the computer, such as a tennis racket,

to play a game with another user in the online world. Both players will be able to see the moving ball in real-time and use the actual racket to swing to 'hit' and feel the impact of the virtual ball on the monitor.



Fig 4.14 Virtual-reality helmets improve the experience in online games

Multimedia computers can play music CDs and DVD movies for entertainment. Many Internet users also download music and movies from the Internet. Software for playing CDs and DVDs is included with most multimedia computers, usually bundled with the latest operating systems. There are special players designed for storing and playing MP3 music files (Fig 4.15).

In the music industry, DJ controllers are used to blend different types of music. Along with music software programs, these devices include sound effects with the music using knobs, backlit buttons, touch strips and other components (Fig 4.16). They provide better control of the software containing the play list of songs than having to use a computer keyboard or laptop touchpad.

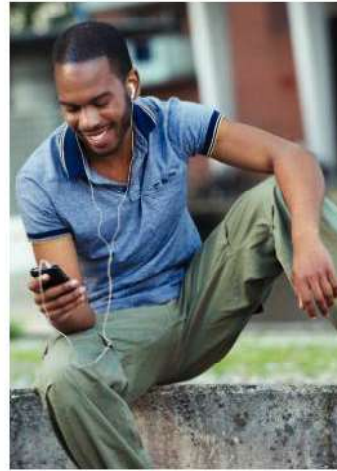


Fig 4.15 MP3 players are very popular for providing access to your downloaded music files while away from your computer



Fig 4.16 DJ Controllers are used to add sound effects to music

In the movie industry, computers have been used to create special effects in some movie scenes. There are also movies that have been made exclusively with computer graphics and animation. This requires the use of graphics workstations with powerful multi-core processors in order to process the data quickly and produce graphics of a high quality.

Questions

- 1 Name a device and explain how it is used to improve the monitoring of stock levels in businesses.
- 2 Name two services that are offered in online banking.
- 3 Name two applications of virtual reality.

Multiple choice questions

- 1 The exposure of a computer system to the possibility of theft or damage is called a(n):
 - a attack
 - b threat
 - c vulnerability
 - d countermeasure.
- 2 The computer-related professional who posts messages using Twitter and Facebook and sends mass emails to clients is a:
 - a computer support specialist
 - b social media specialist
 - c systems administrator
 - d web developer.
- 3 Place the following elements in the correct order to represent the stages in cybersecurity:
 - a attack, countermeasure, vulnerability, threat
 - b countermeasure, vulnerability, threat, attack
 - c threat, attack, countermeasure, vulnerability
 - d vulnerability, threat, attack, countermeasure
- 4 The use of websites or email messages to try to trick you into entering your personal information is known as:
 - a propaganda
 - b identity theft
 - c financial abuse
 - d phishing.
- 5 The use of technology to observe a user's actions, often without the user's knowledge, is known as:
 - a unauthorised access
 - b industrial espionage
 - c computer surveillance
 - d denial-of-service attack.
- 6 Using devices to monitor users' communications without their permission is called:
 - a cyberbullying
 - b computer surveillance
 - c denial-of-service attack
 - d electronic eavesdropping.
- 7 The following statements can be used to describe the three main types of viruses *except* that they:
 - a are carried by a database file
 - b do not require a host program
 - c infect program files
 - d infect system or boot files.
- 8 The use of computer systems to distribute potentially harmful information is called:
 - a propaganda
 - b cyber security
 - c computer fraud
 - d industrial espionage.
- 9 Preventing rightful owners of music from getting money due to them for their creative efforts is known as:
 - a piracy
 - b propaganda
 - c cyberbullying
 - d eavesdropping.
- 10 The best way to protect a computer against viruses is to *never*:
 - a scan for viruses
 - b open email attachments from unknown senders
 - c turn on virus protection
 - d install anti-virus software.

Short answer questions

- 11 Vanessa is working to complete a project on her new laptop to email to her supervisor.
 - a Apart from a keyboard, list one other input device that Vanessa could use to help her complete the project.
 - b Vanessa tried to email the document, but an error occurred each time she tried to attach it. Give one reason to explain a possible cause of the error.
 - c Write an example of a suitable email address that is appropriate for Vanessa to use.
 - d Vanessa decided to upload the document. Explain the term 'upload'.
 - e State the name of the term that enables the project to be uploaded via the Internet.
 - f Explain where the document could be stored once it has been uploaded.

4 Implications of misuse and cyber security

- g** After four hours, Vanessa realised that the document was not uploaded. Explain, giving two possible explanations, why this might have occurred.
- h** Vanessa later realised that she could not access any of her programs that require a password. Discuss whether each of the following elements of cybersecurity occurred to her data:
- i** a threat
 - ii** an attack
 - iii** vulnerable to a threat or attack.
- i** Vanessa thinks she should call a computer professional to help her with the laptop. What is the general name given to this professional?
- 12** Cameron is taking an online course in August, which happens to be during the hurricane season.
- a** Suggest one hardware device that he should have in case of a power outage.
 - b** His lectures are located on a special course page where only students have access to the course notes. Describe the type of network that provides this level of privacy.
- c** On the course page, Cameron clicks on the name of a topic which opens another web page. Describe the special connection that caused this action.
- d** Cameron receives an email stating that the website has been impacted by a 'denial-of-service' attack.
- i** Explain what is meant by this term.
 - ii** Describe two examples which explain that such an attack has occurred.
 - iii** State the computer-related professional who may be able to resolve the problem.
- e** Cameron has been working for over six hours on an assignment. He is relaxing on the floor using his laptop. He has lots of articles around him and types while occasionally glancing at the television.
- i** Explain how Cameron's body can be negatively affected by working in this way.
 - ii** He has quoted information in his assignment from two of the articles but has not included the names of the authors or the articles. Describe the term that explains Cameron's actions, and discuss whether or not it is appropriate for a school assignment.