

Speakers for sound and voice output



Computers can output both music and speech to speakers or headphones. Synthesised speech output, generated from a computer program, can be particularly useful for blind users where passages of text or figures from a spreadsheet are spoken.

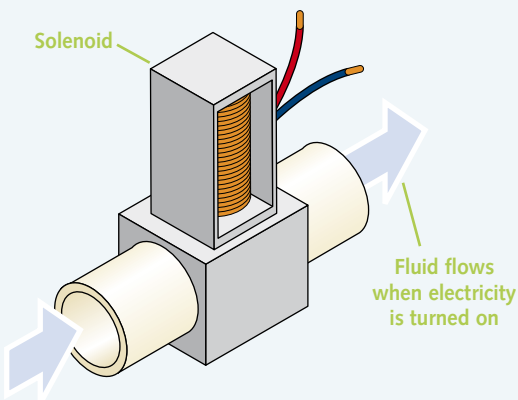
One common example of speech synthesis is used by telephone number enquiry services. When you call them, the operator searches a computer database and locates the number you need. A computer then reads this number out to you by saying, "The number you require is..."

Control devices

When computers are used to control the movement of mechanisms and machines, the output devices are switches and actuators. The tiny output signals from a computer can be electronically amplified to control a broad range of devices, such as the following:

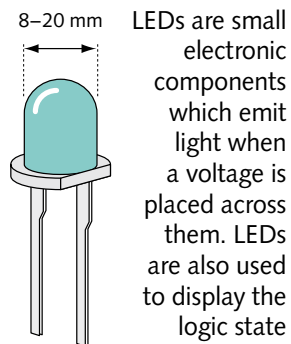
Switches, relays and valves

A computer can be connected to switches and relays to turn electrical appliances on and off. A computer can operate a valve to control fluids, for example, the flow of water into a washing machine, chemical flows in a chemical plant, or the distribution of drinking water.



A control signal from the computer switches the electricity on. The electricity flowing through the coil produces an electromagnet which lifts a valve in the pipe allowing the fluid to flow


Light-emitting diodes (LEDs)

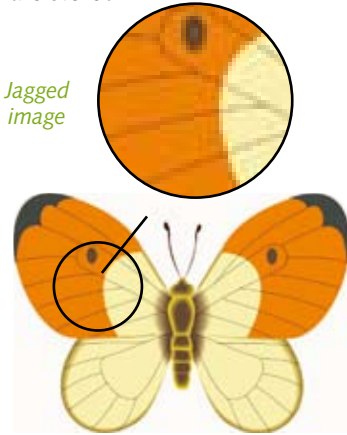


LEDs are small electronic components which emit light when a voltage is placed across them. LEDs are also used to display the logic state (ON and OFF) in control applications.

There are lots of different and important uses for graphics on the computer. Drawing and painting packages are used by illustrators to create images, and games programmers use graphics to produce fast and exciting animations. Many special effects seen on television are generated through computer graphics, and computer aided design (CAD) is vital for many businesses.

Painting programs

Painting programs such as Microsoft® Paint and Adobe® Photoshop are very popular. They are called raster graphics packages because the image is held as a bitmap. The picture is made up of tiny picture elements called pixels . When you zoom into a bitmap image, the edges are often jagged and it is not always easy to rescale the picture. Bitmap images take up a lot of computer memory, as even the blank parts of the picture are stored.

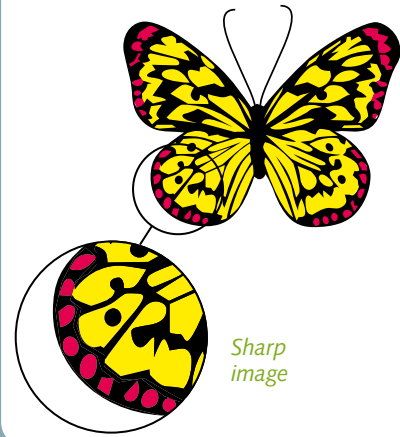




Clip art

Some programs, like the Microsoft® Office collection, come with their own library of professionally-prepared graphics which can be used in documents and publications. You can also buy CDs containing clip art.

Drawing programs

Drawing/illustration programs, like Adobe® Illustrator, use vector graphics. This means that the shapes that are drawn are stored in memory as a series of instructions. This makes them easy to rescale and they take up less memory than bitmap files.



A mouse or a graphics tablet with a stylus  can be used to create freehand drawings on the computer. Packages provide the user with a variety of brush shapes and sizes and spray tools. Colours can be selected from a palette and shapes can be flood filled. All, or part, of a selected drawing can be moved or copied and manipulated on the screen by reflection, rotation, shearing, scaling and cropping .



The data held on a computer is often much more valuable than the computer itself. In business, for example, computers are used to hold data on customers, sales, stock and finances, and to lose this would be very serious.

Network security

When computers are used on a network, the network manager has to ensure that the data on the network is secure. The data should only be accessed by authorised users. Restrictions can be set to limit access (ie which users can read the data, change the data, delete the data and/or add new data). These access rights are associated with a user 'ID' or identifier. A user must enter a valid user ID and password in order to access the network. The computer can then keep track of the transactions performed by each user ID. Passwords should be kept secret and changed regularly. In addition, computers should be kept in locked rooms and laptops secured in lockable cupboards. Data protection laws 57 govern data security.

The most secure passwords are made from a mixture of upper case letters, lower case letters and numbers, for example: **eleNa4Temp**.

Passwords and encrypting data

Many files can be made more secure by adding a password. Take care if you use this feature, as you will not be able to open the file if you forget the password! Some companies use encryption software to prevent stolen data from being read.

Computer viruses

A computer virus is a small program that is transmitted across a network or passed to the computer on disk. There are thousands of different viruses and more are being created by people intent on damaging other people's computer systems. Most viruses are transmitted across the Internet, often as email attachments 44. Some spread rapidly because when they infect a computer they are programmed to transmit themselves to all the users in that person's email address book. Good anti-virus software protects a computer, but new viruses still cause damage costing millions of pounds. In 2007, anti-virus software was checking for over 250 000 specific viruses.

Hackers

A hacker breaks encryption and passwords to gain unauthorised entry to computer systems. Some hackers can do an enormous amount of damage 57. They can change important data or add text and images that might damage a company's reputation. Computers that are accessible over networks are at most risk from hackers. Not all hackers cause harm; ethical hackers help to highlight gaps in security and alert organisations to possible security risks.

Computer fraud

Computer fraud is when someone illegally uses computer data for their own advantage. It is a bigger problem than most people think, because it is sometimes difficult to prove and companies do not always report it, for fear of damaging their reputation. Because it is easy to make a change to data in a computer without people noticing, 'transaction log files' are used to record every change that operators make.

A single computer (or stand-alone computer) is a useful tool for work and leisure activities but when it is joined to other computers in a network, it becomes much more powerful. Users can communicate across a network and share data and peripherals with other users.

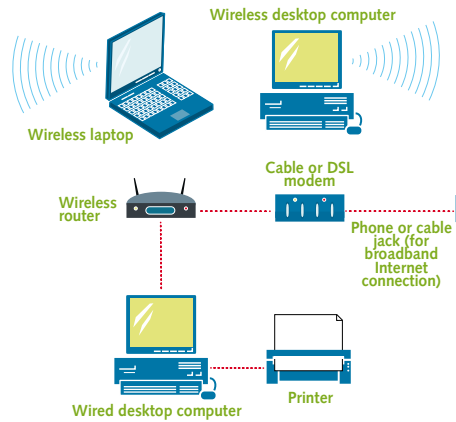
Peer-to-peer network

In homes and small offices, a peer-to-peer network can be set up. In this type of network, the computers communicate directly with each other and every user decides which files they want to allow others to have access to. A peer-to-peer network enables users to share an Internet connection, a printer, files such as music and photos and data such as documents and spreadsheets, and to play multi-player games.

A typical home network

In homes, there may be a mixture of a wired and a wireless network, as shown in the diagram. In this example, the wireless router (also known as an access point) is connected to the broadband Internet connection by a wire.

A fixed desktop computer that is physically close to the router is connected by a wire. The other computers have wireless adapters built into them and use radio signals to transmit and receive data. The fixed desktop computer has a printer connected to it that is shared with the other computers.



Advantages and disadvantages of wireless networks

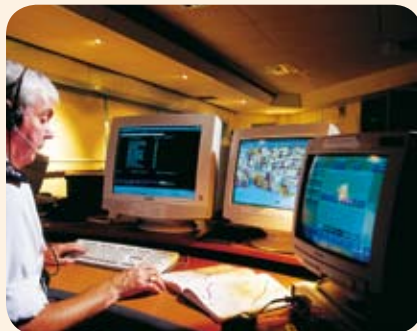
- + **More mobile** – A laptop can access a network anywhere in range.
- + **More flexible** – Computers can be moved without recabling.
- + **Less expensive to install**
- + **Easier to add more computers**
- + **Safer** – There is less risk of tripping over trailing wires.
- **Interference** – Other devices may interfere with the network.
- **Security** – Unauthorised access is more likely.
- **Signal lost** – Something moving into the transmission path can interrupt the signal.
- **Limited by battery power** – Additional power consumption reduces the time a laptop can operate on a battery.

The use of ICT is essential in a modern police force. Every day, police officers require information about stolen goods, criminals and vehicles. They may need to check fingerprints found on a stolen car or check a DNA sample from a murder. This data is all held on computers.

There are 43 police forces in England and Wales, each with their own computer systems. These individual forces are able to share data with other forces across wide area networks (39). A central computer centre – the Police National Computer (PNC) – also makes valuable data available.

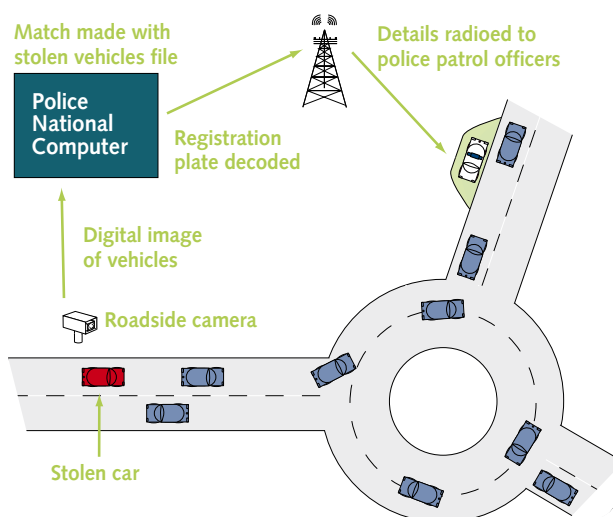
Police communications

With the advances in the technology of mobile telephones, police officers are being equipped with new radios. With these radios, officers can directly access criminal and vehicle databases held on computer, and both the voice and data signals are securely encrypted making them safe from eavesdroppers. The officer's location on patrol can be monitored at the police station and an emergency button on the radio can be used to summon help. The radio network also provides wide national coverage allowing officers to communicate with other forces across the country with a strong, clear signal.



Automatic number plate recognition

If the police wish to check the details of either a vehicle or its owner, then they can look this up in the database of vehicles on the computer. Each record in the database uses the vehicle's registration number as a unique key field (12). Now, with the advances in digital image decoding software, vehicle registration plates can be recognised by the computer as they pass a camera. These cameras are mounted by the roadside and in the back of police patrol vehicles. Full details for every vehicle are returned from the computer in seconds and, if matches are made with stolen or suspect vehicles, details of the vehicle's location are passed directly to police patrol vehicles. More than 100 000 vehicle checks can be processed each day using this system.



Data protection

The 'right to privacy' is a right we all expect. We do not expect personal details such as our age, medical records, personal family details, political and religious beliefs to be freely available to everybody. With the growth of information and communication technology, large databases are able to hold huge quantities of information and global networks are able to share and distribute this information around the world in seconds. In many countries, laws have been introduced to protect people and their personal information. In Europe, these laws are based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data signed by the Council of Europe in 1981. In the UK, the law is the Data Protection Act 1998. Under this Act, if any person, organisation, company or business wishes to hold personal information about people, they must register with the Office of the Information Commissioner.

Personal data

Personal data is data that can identify a living person and allow an opinion to be expressed about that person. For example, just a name and address is not considered personal data. If the data also includes their date of birth and earnings, that is considered personal data.

The data can be further classified as 'sensitive' personal data if it includes details of a person's:

- racial or ethnic origins
- political opinions
- physical or mental health or condition
- religious beliefs
- trade union membership
- sexual life.

Personal data principles

A summary of the basic principles is shown below. Personal data must:

