8 Safety and security

In this chapter you will learn about:
- ★ physical safety issues
- ★ e-safety issues:
  - data protection acts
  - personal and sensitive data
  - e-safety when using the internet
- ★ data security:
  - threats to data
  - protection of data.

This chapter covers safety and security issues when using computers in the office or at home. As the use of computers continues to expand, the health risks and security risks continue to increase. Many of these risks are associated with the internet which, by its very nature, poses a great risk to younger people unless they are vigilant at all times. But large businesses are also at risk from a number of threats, including hackers, pharming attacks and viruses. Many of the precautions people and business can take are common sense, but, equally, it also requires additional knowledge to know how to protect yourself from these external attacks, which can come from anywhere in the world.

8.1 Physical safety

8.1.1 Safety issues

Physical safety is a different issue to health risks (as discussed in Chapter 5.2). While health safety is how to stop people becoming ill, or being affected by daily contact with computers, physical safety is concerned with the dangers that could lead to serious injuries or even loss of life. Some of the more common risks, together with their major causes and possible prevention measures, are listed in Table 8.1.

▼ **Table 8.1** Physical safety hazards and prevention

Safety risk	Cause of safety risk	Prevention measures
Electrocution	» Spilling liquids/drinks on electric equipment » Exposed wires/damaged insulation » Unsafe electrical equipment » Unsafe electrics (for example, wall sockets) in the office	» Do not allow drinks to be taken into the computer room » Check all wires on a regular basis and renew wires if there is any sign of damaged insulation » Ensure all equipment is checked by a qualified electrician on a regular basis » Make use of an RCB (residual current breaker) to prevent electrocution

Safety risk	Cause of safety risk	Prevention measures
Fire hazard	» Overloaded wall sockets (several items plugged into one wall socket) » Overheating of computer equipment (due to poor heat dissipation) » Exposed wires causing a short circuit	» Increase the number of wall sockets and do not use too many extension blocks » Do not cover the cooling vents on computer equipment » Clean out dust accumulation in computers to prevent overheating » Make sure all equipment is fully tested on a regular basis » Ensure there is good room ventilation » Use low-voltage equipment wherever possible » Have a number of fully tested **carbon dioxide/dry powder fire extinguishers**
Tripping hazard	» Trailing wires on the floor » Damaged carpets and other flooring	» Use cable ducts to make the wires safe » Cover exposed wires and hide wires under desks away from general thoroughfare » Use wireless connectivity wherever possible, therefore eliminating the need for trailing cables
Personal injury	» Heavy equipment unstable or falling from desks » Desks collapsing under weight/desks not designed to take the weight	» Use desks strong enough to take the weight of the computer equipment » Use large desks and tables so that hardware is not too close to the edge where it could fall off

8.2 E-Safety

8.2.1 Data protection

Most countries have some form of **data protection act (DPA)**. This is legislation designed to protect individuals and to prevent incorrect or inaccurate data being stored.

Essentially, DPAs are set up to protect the rights of the individual about whom data is obtained, stored and processed – for example, collection, use, disclosure, destruction and holding of data. Any such act applies to both computerised and paper records.

Many data protection acts are based on eight principles, as outlined in Figure 8.1.

In many countries, failure to abide by these simple rules by anyone who holds data about individuals can lead to a heavy fine or even imprisonment.

1 Data must be fairly and lawfully processed.

2 Data can only be processed for the stated purpose.

3 Data must be adequate, relevant and not excessive.

4 Data must be accurate.

5 Data must not be kept longer than necessary.

6 Data must be processed in accordance with the data subject's rights.

7 Data must be kept secure.

8 Data must not be transferred to another country unless they also have adequate protection.

▲ **Figure 8.1** Main principles of data protection acts

There are general guidelines about how to stop data being obtained unlawfully:

- do not leave personal information lying around on a desk when not attended
- lock filing cabinets at the end of the day or when the room is unoccupied
- do not leave data on a computer monitor if it is unattended; log off from the computer if away from your desk for any length of time
- use passwords and user IDs, which should be kept secure; passwords should be difficult to guess/break and should be changed frequently (see earlier notes on passwords)
- make sure that anything sent in an email or fax (including attachments) is not of a sensitive nature.

Link

For more on passwords see Section 4.2.

All of the above are in addition to other security safeguards discussed elsewhere in this book.

8.2.2 Personal data

Personal data refers to any data concerning a living person who can be identified from the data itself or from the data in conjunction with other information. For example, 'Peter Smith has long purple hair and lives at 40 Green Street' would very clearly identify this individual!

Examples of personal data include:

- name
- address or email address (such as myname.lastname@mycompany.com)
- an ID card number/passport number
- an IP address
- cookie ID
- the advertising identifier on a mobile phone
- date of birth
- banking details
- photographs of the individual (for example, in full school uniform).

Some personal data is often referred to as sensitive (personal) data. Examples of sensitive data include:

- ethnicity or race
- political views
- membership of a political party
- membership of a trade union
- religion/philosophical beliefs
- sexual orientation/gender
- criminal record
- medical history
- genetic data/DNA
- biometric data.

Extra special care needs to be taken of sensitive personal data.

Whether data is personal or sensitive, it is imperative that all precautions are taken to keep it confidential, and prevent any inappropriate disclosure. This includes keeping data safe from hackers, for example, but it also means keeping data safe from accidental disclosure. One way to protect data if it is accidentally

disclosed is to encrypt it. You will read many ways of keeping data secure in this chapter and in other chapters throughout this textbook.

8.2.3 E-Safety

E-safety refers to the benefits, risks and responsibilities when using ICT. It is often defined to be the safe and responsible use of technology. However, e-safety is as much about user behaviour as it is about electronic security. In particular:

- when using the internet
- sending and receiving emails
- taking part in social media
- online gaming.

Using the internet

The following is a list of the precautions that can be taken to minimise the potential danger when using the internet:

- When using the internet make sure that the websites being used can be trusted (for example, look out for websites including **https** and/or the green padlock symbol ).
- Only purchase items from websites that offer secure, encrypted connections (see Section 8.3).
- When using search engines, always make sure the device settings are set to 'safe search' and the highest possible level of security is used (also refer to Chapter 10).
- Only use websites recommended by teachers, parents or from trusted sources– refer to Chapter 10.
- Be careful what you download; is the material potentially harmful? Could it be malware? (We will be looking at malware later in this section.) It is essential that anti-virus or anti-malware software is always running in the background and is kept up to date.
- Always remember to log out of sites when you have finished using them; remember that **cookies** are used every time you log into a website (take particular care with websites that store key data such as bank account or credit/debit card details).

Sending and receiving emails

The following list highlights some of the dangers when sending and receiving **emails**. It is important to have an awareness of the risks when opening emails and how to deal with emails from unknown sources.

- Only open emails or attachments from known sources.
- Make sure your internet service provider (ISP) has an effective email filtering feature to ensure emails from unknown sources are put into your spam folder.
- Only reply to an email if you know the person who sent it (or the organisation, if you are 100 per cent certain it is genuine).
- Check that email addresses or website addresses pertaining to come from a genuine company always contain the real company's website address; for example, a web page with the address customer_accounts@gmail.com should

be treated with caution, whereas customer_accounts@amazon.com is more likely to be genuine.

- Think carefully before replying to an email and never include the name of your school/college, or any personal data that could identify you.
- Never send photos of yourself (particularly in school uniform, which could be used to identify your school).
- Beware of phishing and pharming scams (see Section 8.3).
- Protect your email account by using passwords which are difficult to guess, and change them on a regular basis (see Section 8.3).
- Take care when forwarding emails (see Chapter 10 for more details).
- Manually type in email addresses (do not copy and paste an email address from a recipient) because you may not spot typing errors or other clues that it is not genuine.
- Avoid clicking on hyperlinks within emails because it could be part of a phishing scam.
- Remember, the **unsubscribe** link at the bottom of an email could itself be fraudulent.
- Avoid using the Cc or To boxes when sending multiple emails; it is always a good idea to create emailing groups and put the name of the group into the Bcc box; in the To box, send the email to yourself – this will give you and your friends some protection because any unauthorised access will not get to see the email addresses of those in the emailing group (see Chapter 10 for more information).

Link

For more on email see Section 10.1.

Social media

When using social media sites, it is important to be careful and make sure you know how to block undesirable people. The following list shows some of the dangers and some of the ways to protect yourself:

- Do not publicly post or give out personal information to people you do not know, including email addresses or house addresses, because this could be used to find information about you or carry out identity theft.
- Do not send out photos of yourself to people you do not know; again this could lead to identity theft or somebody impersonating you (many of the photos on social media sites are false).
- Always make sure you use the privacy settings when posting photos of yourself on social media sites, so that only people you trust can see them.
- It is important that none of the photos you post can link you to a place or an address (for example, it is not a good idea to show the number plate on a car because it is possible to find your address from this information).
- Particular care should be taken not to post photos of yourself in some form of school uniform; again, this gives somebody information about where they can find you.
- Always maintain privacy settings to stop 'non-friends' from contacting you and also make sure you control who has access to your profile.
- Only make friends with people you know or are very well-known to other friends.
- Avoid using, or forwarding messages containing, inappropriate language.

- It is extremely important to be very vigilant when using social networking sites, instant messaging or chat rooms:
  - Block or report anybody who acts suspiciously or uses inappropriate language.
  - Be very careful with the language used in chat rooms:
    - Always use a nickname and NEVER your real name
    - Keep private and personal data secret.
  - Do not enter private chat rooms – stay in public spaces (the danger signs are if someone wants to enter a private chat room, asks you to instant message or email, requests your telephone number or even suggests that you meet).
  - Never arrange to meet anyone on your own, always tell an adult first and meet the person in a public place.
  - Avoid the misuse of images, including forwarding on other images from other people.
  - Always respect people's confidentiality.

Exercise 8a

Evaluate your own use of the internet, emails and social media/networking sites.

Which of these e-safety strategies do you use every day?

Online gaming

Online gaming has increased over the last few years. There are many reasons for this, such as better internet connections, more sophisticated mobile devices (phones and tablets) and greater realism in recent games. It is important to be careful when using online gaming because is also carries risks. Many users think all the games players are like-minded and, therefore, there are no real risks associated with this type of communication. That is a dangerous assumption. Some of the known risks, associated with online gaming, reported over the years, include:

- predators (people who prey on others who they see as vulnerable)
- cyberbullying (the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature)
- use of webcams (the risks here are obvious!)
- voice-masking technology (to disguise a voice so you cannot tell their sex, age, or even their accent)
- it is often overlooked that online games are also a source of cyber attacks on a user's computer or mobile phone – viruses, phishing or spyware are well-reported examples of problems associated with certain online gaming
- violence in the game itself, which can lead to violent behaviour in reality.

As when using other platforms, you should not reveal any personal information about you or anyone else to anyone while gaming. This includes not using your real name.

Exercise 8b

Find out what safety measures should be taken when playing games on the internet.

Write an article on these safety measures and include ways to minimise or remove these risks.

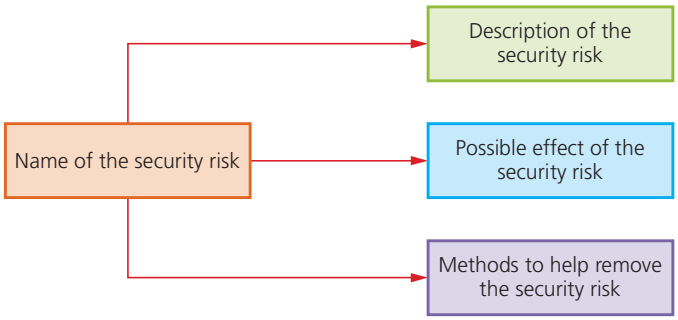
8.3 Security of data

8.3.1 Data threats

There are a number of security risks to data held on a computer/smartphone or data being transferred around networks. This section covers a large number of these risks:

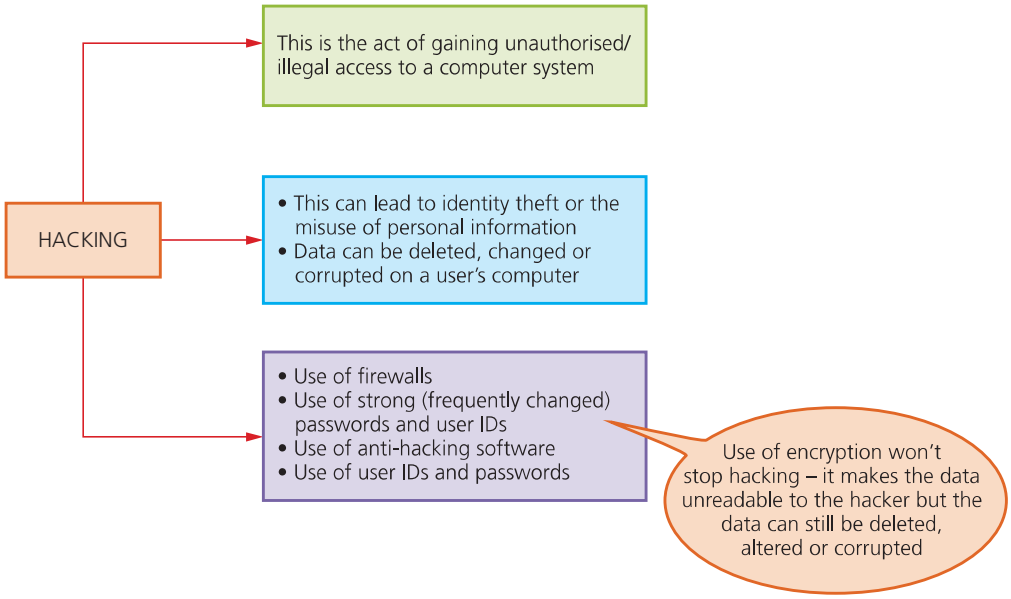
- hacking
- **phishing**
- vishing
- smishing
- **pharming**
- viruses
- malware
- card fraud.

Each security risk together with its description, possible effects and risk mitigation will be set out as shown in Figure 8.2.



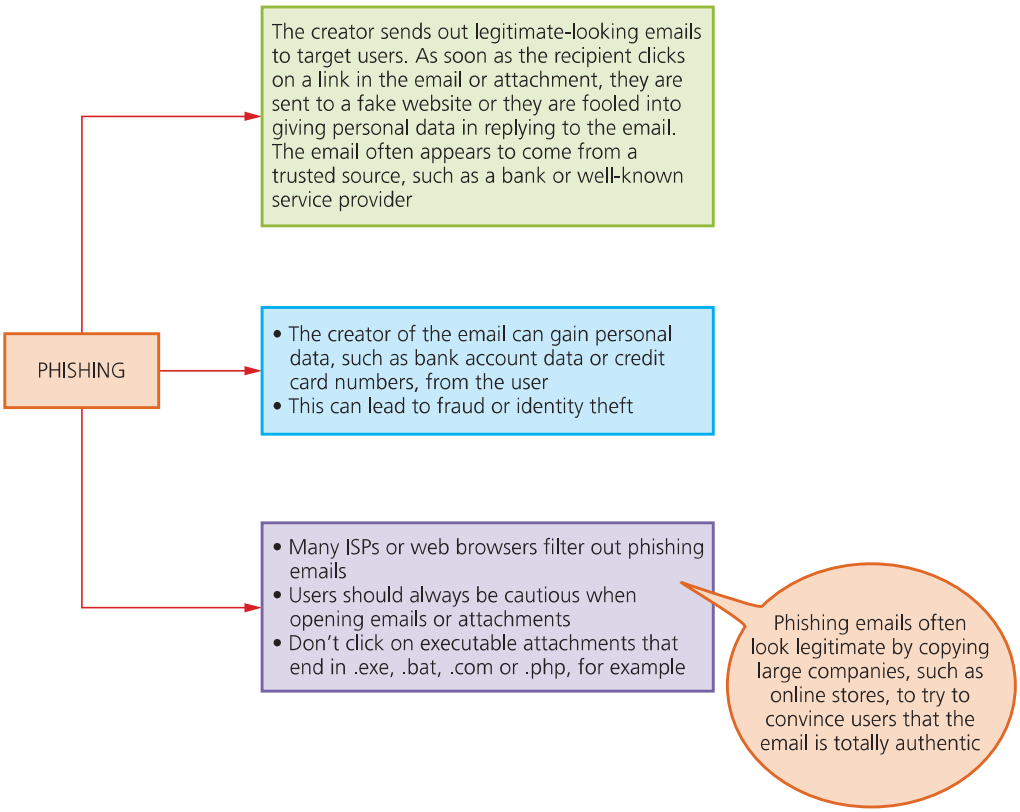
▲ **Figure 8.2** Security risks

Hacking



▲ **Figure 8.3** Risks of hacking

Phishing, smishing, vishing



▲ **Figure 8.4** Risks of phishing

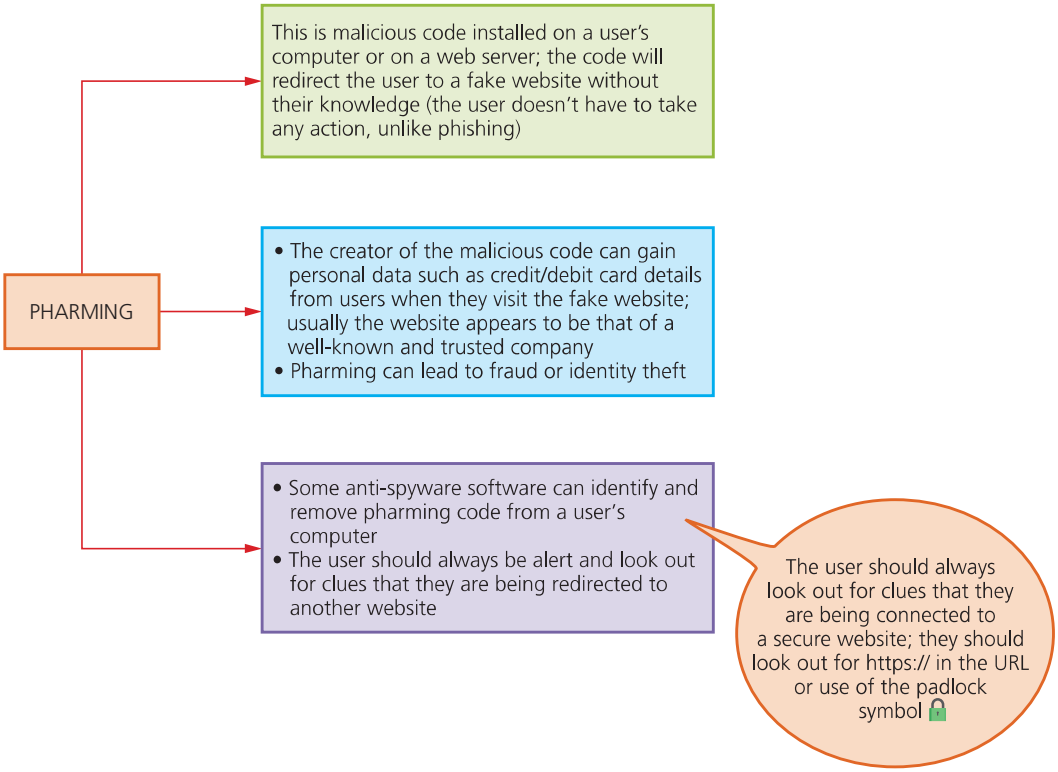
Malicious use refers to, for example, data deletion, fraud, identity theft and selling on personal data. A good example of a phishing attack is when a user is sent an email saying they have ordered an item from an online store. They will be asked to click on a link to see the order details. The link takes the user to a web page that shows a product code that appears to come from a well-known company. A message, such as this will appear: 'if this order wasn't made by you, please fill out the following form to cancel your order in the next 24 hours'.

The form will ask for details such as credit card number, user's address, and so on. Some of the key clues are that links, such as 'how to contact us', do not work.

Smishing – this is short for 'SMS phishing'. It uses the SMS system of mobile phones to send out fake text messages. It is very similar to phishing. These scams often contain a URL or telephone number embedded in the text message. The recipient will be asked to log on to the website or make a telephone call. If they do, they will be asked to supply personal details such as credit/debit card numbers or passwords. As with phishing attacks, the text message will appear to come from a legitimate source and will make a claim, for example, that they have won a prize or that they need to contact their bank urgently. Most people believe that only computers are liable to security threats and that mobile phones are not at risk. This makes smishing a particularly dangerous security threat to many people.

Vishing (voicemail phishing) is another variation of phishing. This uses a voicemail message to trick the user into calling the telephone number contained in the message. As with all phishing attacks, the user will be asked to supply personal data thinking they are talking to somebody who works for a legitimate company.

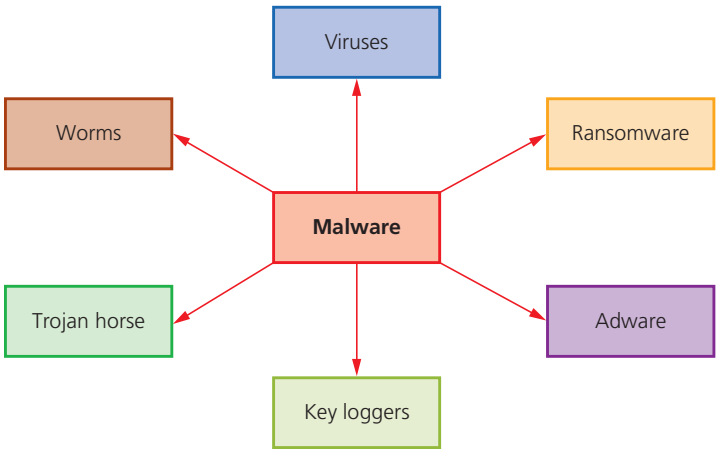
Pharming



▲ **Figure 8.5** Risks of pharming

Viruses and malware

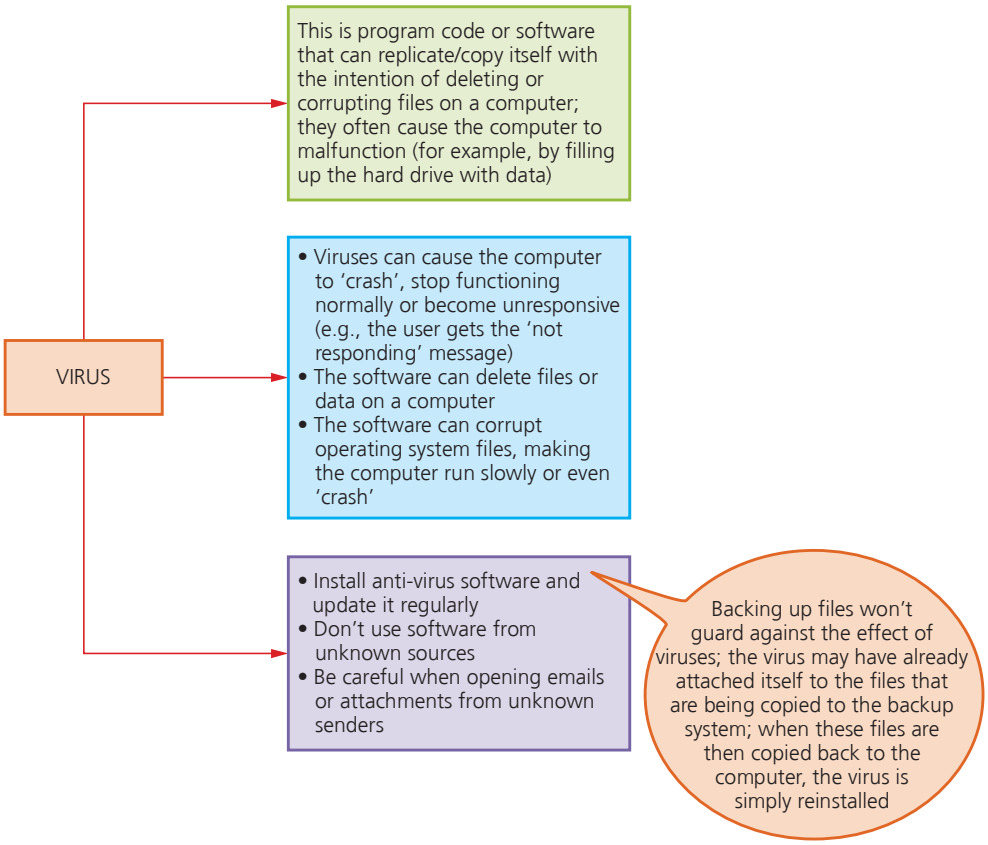
Malware is one of the biggest risks to the integrity and security of data on a computer system. Many software applications, such as anti-virus, are capable of identifying and removing most of the forms of malware. There are many forms of malware; this section details just a selection of those forms.



▲ **Figure 8.6** Malware types

Viruses are programs or program code that replicates (copies itself) with the intention of deleting or corrupting files and causing the computer to malfunction (for example, by deleting .exe files, filling up the hard drive with 'useless' data, and so on).

Viruses need an **active host** program on the target computer or an operating system that has already been infected, before they can actually run and cause harm (that is, they need to be executed by some trigger to start causing any damage).



▲ **Figure 8.7** Risks of viruses

Viruses are often sent as email attachments, and reside on infected websites or on infected software downloaded to the user's computer. Apart from all the usual safety actions (for example, do not open emails from unknown sources, do not install non-original software), always run an up-to-date virus scanner.

Worms

Worms are a type of stand-alone virus that can self-replicate. Their intention is to spread to other computers and corrupt whole networks; unlike viruses, they do not need an active host program to be opened in order to do any damage – they remain inside applications, which allows them to move throughout networks. In fact, worms replicate without targeting and infecting specific files on a computer; they rely on security failures within networks to permit them to spread unhindered.

Worms frequently arrive as message attachments and only one user opening a worm-infested email could end up infecting the whole network. As with viruses, the same safeguards should be employed, together with the running of an up-to-date anti-virus program. Worms tend to be problematic because of their ability to spread throughout a network without any action from an end-user; whereas viruses require each end-user to somehow initiate the virus.

Examples include the 'I love you' worm, which attacked nearly every email user in the world, overloaded phone systems and even brought down television networks. All of this makes them more dangerous than viruses.

Trojan horse

A **Trojan horse** is a malicious program which is often disguised as some legitimate software, but contains malicious instructions embedded within it. A Trojan horse replaces all or part of the legitimate software with the intent of carrying out some harm to the user's computer system.

They need to be executed by the end-user and therefore usually arrive as an email attachment or are downloaded from an infected website. For example, they could be transmitted via a fake anti-virus program that pops up on the user's screen claiming their computer is infected and action needs to be taken. The user will be invited to run fake anti-virus as part of a free trial. Once the user does this, the damage is done.

Once installed on the user's computer, the Trojan horse will give cyber criminals access to personal information on your computers, such as IP addresses, passwords and other personal data. **Spyware** (including key logging software) and ransomware are often installed on a user's computer via Trojan horse malware.

Because they rely on tricking end-users, firewalls and other security systems are often useless because the user can overrule them and initiate the running of the malware.

Key logging software

Key logging software (or **key loggers**) is a form of spyware. It gathers information by monitoring a user's keyboard activities carried out on their computer. The software stores keystrokes in a small file which is automatically emailed to the cybercriminal responsible for the software. It is primarily designed to monitor and capture web browsing and other activities and capture personal data (for example, bank account numbers, passwords and credit/debit card details). Key loggers can be detected and removed by anti-spyware software. Banks try and overcome this risk, by only asking for a different part of the password each time you log on (for example, 'please give the 3rd, 4th and 8th character in your password'). Sometimes drop-down boxes are also used because this involves on-screen selection using a mouse, which is difficult for the key logger to pick up. However, some key loggers work by capturing screen images at random intervals; these are known **screen recorders**.

Exercise 8c

Find out how banks overcome problems such as phishing, key logging software and hacking to ensure online banking is safe for their customers. When doing your research, also check out how risks at ATMs are mitigated by reading the section on card cloning and shoulder surfing (at the end of this section).

Adware

Adware is a type of malware. At its least dangerous, it will attempt to flood an end-user with unwanted advertising. For example, it could redirect a user's browser to a fake website that contains promotional advertising. They can be in the form of pop-ups, or appear in the browser's toolbar thus redirecting the search request.

Although not necessarily harmful, adware can:

- highlight weaknesses in a user's security defences
- be hard to remove – they defeat most anti-malware software because it can be difficult to determine whether or not they are harmful
- hijack a browser and create its own default search requests.

Ransomware

Essentially, **ransomware** are programs that encrypt data on a user's computer and 'hold the data hostage'. The cybercriminal just waits until the ransom money is paid and, sometimes, the decryption key is then sent to the user. It has caused considerable damage to some companies and individuals.

Imagine a situation where you log on to your computer, only to find the screen is locked and you cannot boot up your computer until the demands of the cybercriminal have been met. The malware restricts access to the computer and encrypts all the data until a ransom is paid. It may be installed on a user's computer by way of a Trojan horse or through social engineering.

When ransomware is executed, it either encrypts files straightaway or it waits for a while to determine how much of a ransom the victim can afford. The malware can be prevented by the usual methods (for example, by avoiding phishing emails); but once it is executed, it is almost impossible to reverse the damage caused. The best way to avoid a catastrophe is to ensure regular backups of key files are kept and therfore avoid having to pay a ransom.

Table 8.2 summaries the six types of malware described in this section.

▼ **Table 8.2** Summary of types of malware

Viruses	Programs or program code that can replicate/copy itself with the intention of deleting or corrupting files, or cause the computer to malfunction; they need an active host program on the target computer or an operating system that has already been infected before they can run
Worms	This is a type of stand-alone virus that can replicate itself with the intention of spreading to other computers; often uses networks to search out computers with weak security which are prone to such attacks
Trojan horses	These are malicious programs often disguised as legitimate software; they replace all or part of the legitimate software with the intent of carrying out some harm to the user's computer system
Spyware	Software that gathers information by monitoring, for example, all the activity on a user's computer; the gathered information is then sent back to the person who sent the software (sometimes they monitor key presses, which is referred to as key logging software)
Adware	Software that floods a user's computer with unwanted advertising; usually in the form of pop-ups, but can frequently appear in the browser address window redirecting the browser to a fake website which contains the promotional adverts
Ransomware	Programs that encrypt the data on a user's computer; a decryption key is sent back to the user once they pay a sum of money (a ransom); they are often sent via a Trojan horse or by social engineering

Card fraud

Card fraud is the illegal use of a credit or debit card. This can be due to:

- shoulder surfing when using the card on any device that requires keyboard entries (for example, an ATM or a handheld POS terminal)
- card cloning
- key logging software.

▲ **Figure 8.8** Automatic teller machine (ATM) and handheld point-of-sale (POS) terminal

Shoulder surfing

Shoulder surfing is a form of data theft where criminals steal personal information from a victim when they are using a cash dispensing machine (for example, an automatic teller machine – ATM), when paying for goods/services using a handheld point-of-sale (POS) device or even when paying using a smartphone. Examples of shoulder surfing includes:

- somebody watching you key in data, such as your PIN; this can be something simple like just looking over your shoulder or somebody watching from a distance using binoculars or using a video camera
- somebody listening in when you are giving credit or debit card details over the phone; by simply listening in, a criminal will gain very important data about your card
- some of the more sophisticated examples of shoulder surfing include the use of tiny digital cameras (placed near to the keyboard on the ATM or other device) which take high-quality images of the keys being pressed.

There are ways to overcome this security risk:

- When using ATMs shield the keyboard with your other hand so that no-one can see which keys you are pressing (many ATMs also have a small mirror built into them so you can see if somebody is standing right behind you).
- When using a mobile device (such as a smartphone, tablet or laptop) never key in data in a public place; nor should you speak card details into your smartphone in a public place.
- If you are using a public place, make sure you are nowhere near security cameras which could record passwords or other data about you; it is also a good idea to use biometrics (touch ID or face ID) on your smartphone or tablet, because these cannot be duplicated by simply watching you.

Card cloning

Card cloning is the copying of a credit or debit card which uses a magnetic stripe. Cloning of this type of card employs an electronic device known as a **skimmer**.

This is a data capture device that allows a criminal to record all of the data stored on the magnetic stripe on a card. Skimmers can be placed in ATM slots where they can read all the data from a card; this data is then copied to the magnetic stripe of a fake card. Even the security hologram can be copied. The skimmer is often a false front on the card slot on the ATM. To obtain the PIN to use with the newly cloned car, the criminal would also make use of shoulder surfing.

Smart cards, which contain a microchip, were introduced to combat card cloning and give considerably more security. Therefore, a different device, known as a **shimmer**, is now used to read these smart cards. This uses a paper-thin shim (that contains a chip and a flash drive) that can be put into a card reading slot. It is so thin that it is almost impossible to detect. When a customer puts their card into the reader slot, the shim reads all the data from the credit/debit card, allowing the criminal to create a fake replica credit/debit card. Although the chip itself cannot be cloned, all the data gathered from the cloned card is now stored on a magnetic stripe and a fake card is produced. The fake card can be used to make purchases where a magnetic stripe card is still acceptable; for example, when making purchases online.

Obviously, the best way to check on this type of fraud is to do regular checks of your spending and query any unusual activity.

Key logging
The use of key logging software has been discussed earlier. This is used to detect all key presses, such as when entering a credit or debit card:

- number
- security code (card verification value – CVV)
- PIN.

Because all this data can be obtained by key logging software, illegal use of a credit or debit card to buy things online is a continued risk.

8.3.2 Protection of data

Authentication is used to verify that data comes from a secure and trusted source. Along with **encryption** it strengthens internet security. We will be considering all of the following methods to protect the security of data:

- biometrics
- digital certificates
- secure sockets layer (SSL)
- encryption
- firewalls
- two-factor authentication
- user ID and password.

Biometric authentication

Biometrics relies on certain unique characteristics of human beings. Examples include:

- fingerprint scans
- signature recognition
- retina scans

- iris recognition
- face recognition
- voice recognition.

Biometrics is used in a number of applications as a security device. For example, some of the latest mobile phones require fingerprint matching before it can be operated; some pharmaceutical companies use face recognition or retina scans to allow entry to secure areas. We will now consider two of these biometric techniques in a little more detail.

Fingerprint scans

Images of fingerprints are compared against previously scanned fingerprints stored in a database; if they match then access is allowed. The system compares patterns of 'ridges' and 'valleys' which are unique.

▲ **Figure 8.9** Fingerprint pattern

An example of its use would be as a security method for entering a building. Fingerprint scanning techniques have the following advantages:

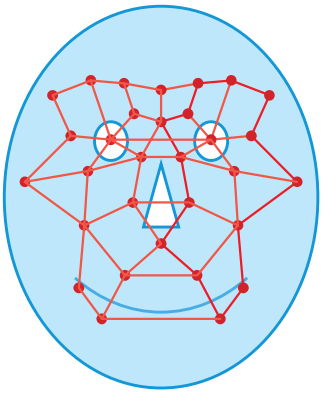
- Fingerprints are unique, therefore this technique would improve security because it would be difficult to replicate a person's fingerprints.
- Other security devices (such as magnetic cards) could be lost or even stolen, which makes them less effective.
- It would be impossible to 'sign in' for somebody else because the fingerprints would match up to one person only on the database.
- Fingerprints cannot be misplaced; a person always has them!

What are the disadvantages?

- It is relatively expensive to install and set up.
- If a person's fingers are damaged through an injury, this can have an effect on the scanning accuracy.
- Some people may regard it as an infringement of civil liberties.

Face recognition

Face recognition is used to identify somebody by their facial features. It is used by many modern smartphones as the method of identifying the owner of the phone, and for authorising purchases using the phone.



▲ **Figure 8.10** Face recognition

Figure 8.10 shows several of the positions used by the face-recognition software. The position of each facial feature is calculated by the software. These values are then compared to values already stored on a database. If the values match, then the face is recognised.

Data such as:

- distance between the eyes
- width of the nose
- shape of the cheek bones
- length of the jawline
- shape of the eyebrows

are all used to uniquely identify a given face.

Face recognition systems can be 'fooled' by wearing spectacles or by people changing their hair style and colour. However, the technology is improving.

One drawback common to all biometric techniques is the need for the systems to store very personal data about users. Some people are uncomfortable with this idea. Table 8.3 shows a comparison of some of the other advantages and disadvantages of the six most common biometric techniques.

▼ **Table 8.3** Comparison of biometric types

Biometric technique	Advantages	Disadvantages
Fingerprint scans	» very high accuracy » one of the most developed biometric techniques » very easy to use » relatively small storage requirements for the biometric data created	» for some people it is very intrusive, because it is still related to criminal identification » it can make mistakes if the skin is dirty or damaged (for example, cuts to the finger)
Signature recognition	» non-intrusive » requires very little time to verify (about five seconds) » relatively low-cost technology	» if individuals do not sign their names in a consistent manner there may be problems with signature verification » high error rate of 1 in 50
Retina scans	» very high accuracy » there is no known way to replicate a person's retina pattern	» it is very intrusive » it can be relatively slow to verify retina scan with stored scans » very expensive to install and set up
Iris recognition	» very high accuracy » verification time is generally less than five seconds	» very intrusive » uses a lot of memory for the data to be stored » very expensive to install and set up
Face recognition	» non-intrusive method » relatively inexpensive technology	» it is affected by changes in lighting, the person's hair, their age, and if the person is wearing spectacles
Voice recognition	» non-intrusive method » verification takes less than five seconds » relatively inexpensive technology	» a person's voice can be easily recorded and used for unauthorised access » low accuracy » an illness, such as a cold, can change a person's voice, making absolute identification difficult or impossible

Digital certificates

A **digital certificate** is a pair of files stored on a user's computer – these are used to ensure the security of data sent over the internet. Each pair of files is divided into:

» a public key (which can be accessed by anyone)
» a private key (known to the computer user only).

For example, when sending an email, the message is made more secure by attaching a digital certificate. When the message is received, the recipient can verify that it comes from a known or trusted source by viewing the public key information (this is usually part of the email attachment). This is an added level of security to protect the recipient from harmful emails. The digital certificate is made up of six parts:

» the sender's email address
» the name of the digital certificate owner
» a serial number
» expiry date (the date range during which the certificate is valid)
» public key (which is used for encrypting the messages and for digital signatures)
» digital signature of certificate authority (CAs) – an example of this is *VeriSign*

Operating systems and web browsers maintain lists of trusted CAs (Figure 8.11).

▲ **Figure 8.11** Digital IDs

Secure sockets layer (SSL)

Secure sockets layer (SSL) is a type of protocol that allows data to be sent and received securely over the internet.

When a user logs onto a website, SSL encrypts the data – only the user's computer and the web server are able to make sense of what is being transmitted. A user will know if SSL is being applied when they see http**s** (as part of the website address) or the small padlock in the status bar at the top of the screen.

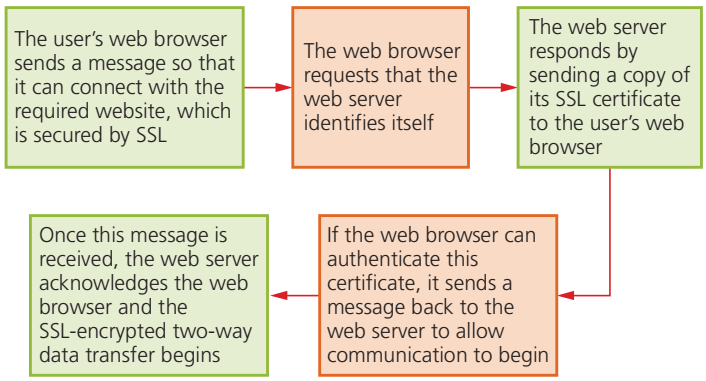
The address window in the browser when https protocol is being applied, rather than just http protocol, is quite different:

Using https: secure https://www.xxxx.org/documents

Using http: http://www.yyyy.co.uk/documents

SSL certificates are small data files that digitally bind an encryption key to an organisation's details. When installed on a web server, it shows as the green padlock and the https protocol ensures secure connections from a web server to a web browser.

Figure 8.12 shows what happens when a user wants to access a secure website and receive and send data to it:



▲ **Figure 8.12** Communicating across a network using SSL

Examples of where SSL would be used:

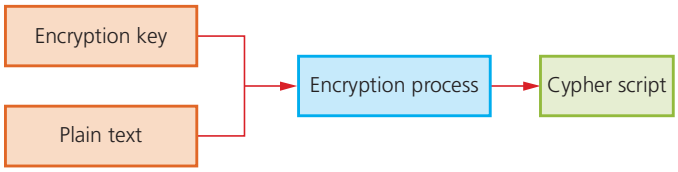
- online banking and all online financial transactions
- online shopping/commerce
- when sending software out to a restricted list of users
- sending and receiving emails
- using cloud storage facilities
- intranets and extranets (as well as the internet)
- Voice over Internet Protocol (VoIP) when carrying out video chatting and/or audio chatting over the internet
- within instant messaging
- when making use of a social networking site.

Encryption

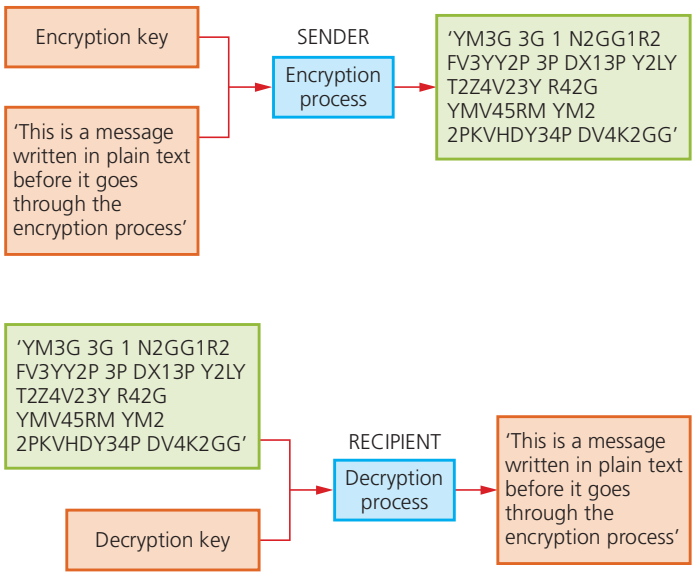
Encryption is used primarily to protect data in case it has been hacked or accessed illegally. While encryption will not prevent hacking, it makes the data meaningless unless the recipient has the necessary decryption tools (as described below).

Encryption uses a secret key that has the capability of altering the characters in a message. If this key is applied to a message, its content is changed, which makes it unreadable unless the recipient also has the same secret key. When this secret key is applied to the encrypted message, it decodes it, allowing it to be read.

The key used to encrypt (or encode) the message is known as the **encryption key**; the key used to decrypt (or decipher) the message is known as the **decryption key**. When a message undergoes encryption it is known as **cypher script**; the original message is known as **plain text**. Figure 8.13 shows how these two are linked together.



▲ **Figure 8.13** Encryption



▲ **Figure 8.14** Example of encryption and decryption

Because the protection of data if it is intercepted or illegally accessed is of paramount importance, encryption has many applications:

- Due to the risks of pharming, hacking or spyware (and other forms of malware) it is important that data stored on HDDs or SSDs is encrypted; if data is then accessed illegally, it will be unreadable to the cybercriminal.
- Encryption of emails is also important (many of the safety aspects of sending and receiving emails was discussed in Section 8.2.3):

- Encryption of email contents protects sensitive information from being read by anyone other than the intended recipients; encrypted messages are meaningless to anyone without the decryption key.
- Hackers who gain unauthorised access to an email account can access attachments, content or even the whole email account.

▼ **Table 8.4** Which part of the email should be encrypted?

Encrypt the connection with your email provider:	Encrypt the actual email messages:	Encrypt stored or archived email messages:
» Encryption of the connection with your email supplier prevents unauthorised users from intercepting and capturing log in details as well as any email messages sent or received » As the emails leave your email supplier's server and travel to their destination server they are at risk; encryption will give the additional protection described above	» Encryption of emails themselves prevents a hacker making sense of any intercepted messages (keeping any sensitive or confidential information safe)	» Any backed-up messages stored on your email supplier's server also need to be encrypted » If a hacker acquires access to this server, they could then gain access to your stored or archived messages

Another important point about emails is that only encrypting sensitive or confidential messages is bad practice – this indicates to a hacker which emails they should target; encrypting all messages means the hacker has to try and decrypt every message to find the ones they want, which certainly will not make life easy for them.

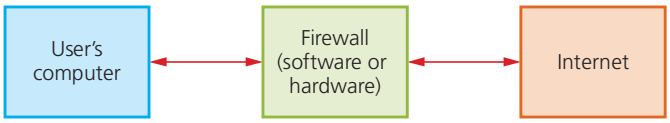
Any data stored on the cloud should also be encrypted (see Chapter 4); it is good practice to encrypt data prior to uploading to the cloud provider – this means that even if the cloud supplier's servers are compromised, your data remains encrypted; here are two recent examples to indicate why encrypting your data on cloud storage is good practice:

» the celebrity photos cloud hacking scandal, in which more than 100 private photos and personal information of some celebrities were leaked; hackers had gained access to a number of cloud accounts, which enabled them to publish photos and other sensitive information on social networks and sell them to publishing companies
» the National Electoral Institute of Mexico suffered a cloud security breach in which 93 million voter registrations, stored on a central database, were compromised and became publicly available to everyone; to make matters worse, much of the information on this database also linked to a cloud server outside Mexico.

As mentioned earlier, https and SSL gives protection when transferring data across the internet.

Firewalls

A **firewall** can be software or hardware. It sits between the user's computer and an external network (for example, the internet). A firewall will help to keep potentially destructive forces away from a user's computer, by filtering incoming and outgoing network traffic. The criteria for allowing or denying access to a computer can be set by the user.



▲ **Figure 8.15** Firewall connection

The following list shows a number of the tasks carried out by a firewall:

- to examine the 'traffic' between user's computer (or internal network) and a public network (for example, the internet)
- checks whether incoming or outgoing data meets a given set of criteria
- if the data fails the criteria, the firewall will block the 'traffic' and give the user (or network manager) a warning that there may be a security issue
- the firewall can be used to log all incoming and outgoing 'traffic' to allow later interrogation by the user (or network manager)
- criteria can be set so that the firewall prevents access to certain undesirable sites; the firewall can keep a list of all undesirable IP addresses
- it is possible for firewalls to help prevent viruses or hackers entering the user's computer (or internal network)
- the user is warned if some software on their system is trying to access an external data source (for example, automatic software upgrade); the user is given the option of allowing it to go ahead or request that such access is denied.

The firewall can be a hardware interface which is located somewhere between the computer and the internet connection. It is often referred to in this case as a **gateway**. Alternatively, the firewall can be software installed on a computer; in some cases, this is part of the operating system.

Two-factor authentication

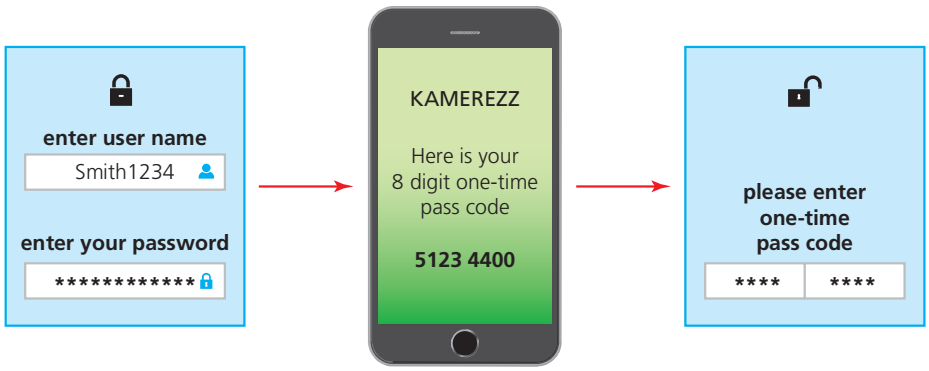
Authentication refers to the ability of a user to prove who they are. There are three common factors used in authentication:

- something you know (for example, a password or PIN code)
- something you have (for example, a mobile phone or tablet)
- something which is unique to you (for example, biometrics).

Two-factor authentication is a form of verification which requires two methods of authentication to verify who a user is. It is used predominantly when a user makes an online purchase, using a credit/debit card as payment method.

For example, suppose Kate wishes to buy a new camera from a website. She logs into the website using her computer. This requires her to enter a user name and a password, which is step one of the authentication process.

To improve security, an eight-digit PIN (called a one-time pass code) is sent back to her either in an email or as a text message to her mobile phone (the mobile phone has already been registered by Kate on the website as the second stage of the authentication process). Kate now enters this eight-digit PIN into her computer and she is now authorised to buy the camera.



▲ **Figure 8.16** Two-factor authentication using a mobile phone

Using the definitions of authentication at the start of this section, the mobile phone is something she has and the password/PIN code is something she knows.

User IDs and passwords

Passwords are used to restrict access to data or systems. They should be hard to break and changed frequently to retain any real level of security. In addition to protecting access levels to computer systems, passwords are frequently used when accessing the internet, for example:

- when accessing email accounts
- when carrying out online banking or shopping
- when accessing social networking sites.

It is important that passwords are protected; some ways of doing this are described below:

- Run anti-spyware software to make sure that your passwords are not being relayed back to anyone who put the spyware on your computer.
- Change passwords on a regular basis in case it has come into the possession of another user illegally or accidentally.
- Passwords should not be easy to break (for example, your favourite colour, name of a pet or favourite music artist); passwords are grouped as either strong (hard to break or guess) or weak (relatively easy to break or guess).
- It is possible to make a password strong but also be easy to remember; suppose we use the phrase: 'The 3rd planet is Earth: the 8th planet is Neptune' could give us an easy-to-remember password: T3piE:t8piN (which is certainly strong and difficult to break).
- Strong passwords should contain:
  - at least one capital letter
  - at least one numerical value
  - at least one other keyboard character (such as @, *, &. etc.)

  An example of a strong password would be: Sy12@#TT90kj=0
  An example of a weak password would be: GREEN

When the password is typed in, it often shows on the screen as ******** so nobody overlooking can see what the user has typed in. If the user's password does not match up with the user name then access will be denied. Many systems ask for the password to be typed in twice when being created, as a verification check (a check on input errors). To help protect the system, users are only

allowed to type in their password a finite number of times – three times is usually the maximum number of attempts allowed before the system locks the user out. After that, the user will be unable to log on until they have re-set their password.

When using an online company, if a user forgets their password or they need to re-set it, they will be sent an email which contains a link to a web page where they can do so. This is done as an added precaution in case an unauthorised person has tried to change the user's password.

Passwords should be changed on a regular basis in case they become known to another user or even a hacker. In particular, it is important to prevent other people gaining access to your password by way of spyware or viruses – many methods to guard against this have been discussed earlier in this chapter.

As mentioned above, it is usually necessary to use a username as well as a password. This gives an additional security level because the username and password must match up to allow a user to gain access to, for example, a bank website.

Exercise 8d

Which of the following are weak passwords and which are strong passwords?

Explain your decision in each case.

i 25-Apr-2005
ii Password1
iii ChapTer@06
iv rX!3&tp%
v 111111"

Exam-style questions

1 **a** Name **three** safety issues when using computer systems. [3]

b For each named safety issue, describe **one** way to remove or militate against the risk. [3]

2 Internet banking can be used by bank customers to check their account balance.
Many ways of logging into such a system involve the use of passwords.
Describe **three** methods of minimising the possibility of passwords being misused or intercepted. [3]

Cambridge IGCSE Information and Communication Technology (0417) Paper 11 Q9 a, May/June 2016

3 There are a number of health and safety issues associated with the use of computers.
Draw arrows from the terms **Health** or **Safety** to the matching issue. Use a maximum of four arrows. [4]

	Tripping over loose wires.
Health	Heavy equipment falling off tables and injuring people.
	Clicking a mouse repetitively causing RSI.
Safety	Overloading sockets causing a fire.

Cambridge IGCSE Information and Communication Technology (0471) Paper 11 Q5, May/June 2017

4 **a** Discuss the e-safety issues when using a social networking site. [7]

b Data can be classified as personal or sensitive.
Give **two** examples of each. [4]

5 Indicate, by ticking (✓) the appropriate box, which of the following are examples of a health risk and which are examples of a safety risk. [7]

Description of risk	Health (✓)	Safety (✓)
Tripping over a loose wire on the floor		
Headaches caused by the glare from a computer screen		
Risk of electrocution caused from damaged insulation on an electric cable		
Broken leg injury caused by falling equipment		
Irritation of the eyes caused by ozone gas coming from a laser printer		
Repetitive strain injury caused by repeated use of a keyboard		
Neck strain from sitting in a prolonged position in front of a computer monitor		

6 Seven ICT descriptions are shown on the left and seven ICT terms on the right.
By drawing arrows, connect each description to the correct term. [6]

Authentication method using, for example, fingerprint scans, retina scans or face recognition	Firewall
Result of putting a message through an encryption algorithm	Pharming
Electronic document that uses a public key and a private key which is used to secure data sent over the internet	Cypher text
Hardware or software that sits between a computer and an external network that filters traffic in and out	Virus
Protocol that allows data to be sent and received securely over the internet	Secure sockets layer (SSL)
Program code that copies itself with the intention of deleting or corrupting files on a computer; needs to be initiated by some event	Biometrics
Malicious code installed on a server or hard disk drive that redirects a web browser to a fake website without the user's knowledge	Digital certificates

7 Complete the following paragraph using words or phrases from the following list. Each word or phrase may be used once, more than once or not at all.

- authenticity
- biometrics
- digital certificate
- encrypted
- e-safety
- hacking
- link
- password protected
- personal data
- pharming
- phishing
- privacy settings
- protocols
- secure sockets layer
- sensitive data
- smishing
- user ID
- vishing

_____ refers to safety when using the internet. Data, such as ethnic origin or political views, are examples of _____ When using online social networks, it is important to maintain _____ to control who has access to your profile. Users have to be aware of _____, which is illegal access to their computer, or to _____ which occurs when legitimate-looking emails are received. In this security threat, as soon as the _____ is clicked on, the user's browser is sent to a fake website. This is similar to _____ where text messages are sent out from a fake company. To prevent intercepted data being understood by a hacker, it is _____. Protocols called _____ are used on the internet to allow data to be sent and received securely. They are often used with _____, which are electronic documents which confirm the _____ of the sender of the data. [11]

8 **a** Explain what is meant by a firewall. [2]

b Describe **four** of the tasks carried out by a typical firewall. [4]

9 Explain each of the following terms and give an example of their use.
- **a** cloning of credit cards
- **b** fingerprint scanning
- **c** digital certificates
- **d** encryption
- **e** vishing [10]

10 a Name **three** biometric authentication techniques. [3]
- **b** For each named technique, describe the advantages and disadvantages of using it as a method of data security. [6]

11 a Explain what is meant by the term authentication. [2]
- **b** Explain what is meant by two-factor authentication. [3]

12 a Explain why it is important to encrypt emails. [3]
- **b** Explain why key logging software poses a security threat when purchasing items on the internet. [3]