Activity 5.2

1 a A blockchain has seven blocks. Draw a diagram to show how they are all connected to form a blockchain network.

b Describe what would happen if block 4 was hacked to change the sum of money in the transaction.

2 What are the main differences between digital currency and cryptocurrency?

5.3 Cyber security

5.3.1 Cyber security threats

Keeping data safe is extremely important for many reasons. It may be personal data that you want to keep within your family or close friends, or it may be commercial data, such as passwords and bank details.

Data can be corrupted or deleted either through accidental damage or malicious acts. There are also many ways data can be intercepted leading to cyber security threats. The following list shows the cyber threats which will be considered in this section:

- brute force attacks
- data interception
- distributed denial of service (DDoS) attacks
- hacking
- malware (viruses, worms, Trojan horse, spyware, adware and ransomware)
- phishing
- pharming
- social engineering.

Brute force attacks

If a hacker wants to 'crack' your password, they can systematically try all the different combinations of letters, numbers and other symbols until eventually they find your password. This is known as a **brute force attack** and there isn't a lot of sophistication in the technique.

One way to reduce the number of attempts needed to crack a password is to first go through a series of logical steps:

1. Check if the password is one of the ***most*** common ones used (the five most common are: 123456, password, qwerty, 111111 and abc123); since these simple passwords are seen so many times it's a good place for the hacker to start.
2. If it isn't in the common password list, the next thing to do is to start with a strong **word list** (this is a text file containing a collection of words that can be used in a brute force attack); some programs will generate a word list containing a million words. Nonetheless this is still a faster way of cracking a password than just total trial and error.

Clearly method (2) would still take several hours until the password was found. The longer a password is and the greater the variation of characters used, the harder it will be to crack (also refer to the notes on the use of passwords in authentication).

Link

For more on data packets refer to Chapter 2.

Data interception

Data interception is a form of stealing data by **tapping** into a wired or wireless communication link. The intent is to compromise privacy or to obtain confidential information.

Interception can be carried out using a **packet sniffer**, which examines data packets being sent over a network. The intercepted data is sent back to the hacker. This is a common method when wired networks are used.

Wi-Fi (wireless) data interception can be carried out using **wardriving** (or sometimes called **Access Point Mapping**). Using this method, data can be intercepted using a laptop or smartphone, antenna and a GPS device (together with some software) outside a building or somebody's house. The intercepted Wi-Fi signal can then reveal personal data to the hacker, often without the user being aware this is happening.

Obviously, encryption of data makes life more difficult for the hacker. While it doesn't stop the data being intercepted or altered in some way, encryption will make the data incomprehensible to the hacker if they don't have access to a decryption key. Therefore, to safeguard against wardriving, the use of a **wired equivalency privacy (WEP)** encryption protocol, together with a firewall, is recommended. It is also a good idea to protect the use of the wireless router by having complex passwords. It is important not to use Wi-Fi (wireless) connectivity in public places (such as an airport) since no data encryption will exist and your data is then open to interception by anyone within the airport.

Distributed Denial of Service (DDoS) attacks

A **denial of service (DoS)** attack is an attempt at preventing users from accessing part of a network, notably an internet server. This is usually temporary but may be a very damaging act or a large breach of security. It doesn't just affect networks; an individual can also be a target for such an attack. The attacker may be able to prevent a user from:

- accessing their emails
- accessing websites/web pages
- accessing online services (such as banking).

One method of attack is to flood the network with useless **spam** traffic. How does this cause a problem?

When a user enters a website's URL in their browser, a request is sent to the web server that contains the website or web page. Obviously, the server can only handle a finite number of requests. So if it becomes overloaded by an attacker sending out thousands of requests, it won't be able to service a user's legitimate request. This is effectively a denial of service. In a **distributed denial of service (DDoS)** the spam traffic originates from many different computers, which makes it hard to block the attack.

This can happen to a user's email account, for example, by an attacker sending out many spam messages to their email account. Internet service providers (ISPs) only allow a specific data quota for each user. Consequently, if the attacker sends out thousands of emails to the user's account, it will quickly become clogged up and the user won't be able to receive legitimate emails. An individual user or a website can guard against these attacks to some degree by:

- using an up-to-date malware checker
- setting up a firewall to restrict traffic to and from the web server or user's computer
- applying email filters to filter out unwanted traffic (for example, spam).

There are certain signs a user can look out for to see if they have become a victim of a DDoS attack:

- slow network performance (opening files or accessing certain websites)
- inability to access certain websites
- large amounts of spam email reaching the user's email account.

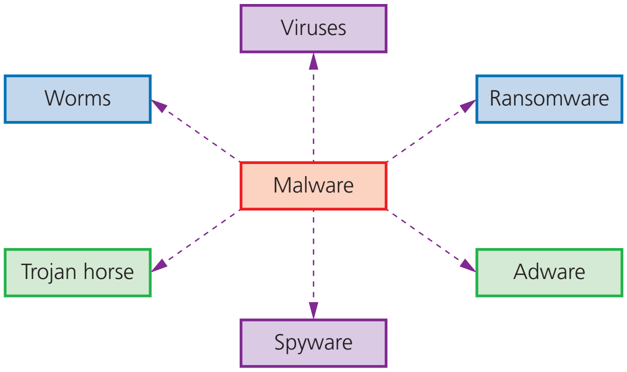
Hacking

Hacking is generally the act of gaining illegal access to a computer system without the user's permission. This can lead to identity theft or the gaining of personal information; data can be deleted, passed on, changed or corrupted. As mentioned earlier, encryption does not stop hacking; it makes the data meaningless to the hacker but it doesn't stop them from deleting, corrupting or passing on the data. Hacking can be prevented through the use of firewalls, user names and frequently changed strong passwords. Anti-hacking software and intrusion-detection software also exists in the fight against hacking.

Malicious hacking, as described above, takes place without the user's permission, and is always an illegal act. However, universities and companies now run courses in **ethical hacking**. This occurs when companies authorise paid hackers to check out their security measures and test how robust their computer systems are to hacking attacks.

Malware

Malware is one of the biggest risks to the integrity and security of data on a computer system. There are many forms of malware; this chapter will only consider the following in any detail:



▲ **Figure 5.10** Malware types

Viruses

Viruses are programs or program code that replicate (copies themselves) with the intention of deleting or corrupting files, or causing a 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 before starting to cause any damage).

Viruses are often sent as email attachments, reside on infected websites or on infected software downloaded to the user's computer. Apart from all the usual safety actions (for example, don't open emails from unknown sources, don't install non-original software), always run an up-to-date virus scanner (refer to Chapter 4 for more details).

Find out more

Reading this chapter and other chapters throughout this book, find out the various ways viruses can be sent. Produce a wall chart showing all of these ways and the various ways to avoid receiving viruses.

Worms

Worms are a type of stand-alone malware that can self-replicate. Their intention is to spread to other computers and corrupt whole networks; unlike viruses, they don't 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 program which is often disguised as legitimate software but with 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 since the user can overrule them and initiate the running of the malware.

Spyware

Spyware is software that gathers information by monitoring a user's activities carried out on their computer. The gathered information is sent back to the cybercriminal who originally sent the spyware. They are 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). Spyware can be detected and removed by anti-spyware software. The big danger of spyware is the method it used to enter a user's system and exploit it; for example, did it come from social engineering? If spyware is found on a computer, it should set off alarm bells since a weakness in the security has been found which could be exploited by other, often more dangerous, malware.

Find out more

Key logging software is often part of spyware.

1 How does this type of malware gather data from the user's computer?
2 Some banks use drop-down menus to overcome key logging software. Explain how using drop-down boxes to enter characters from, for example, a password can help in security.

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 website that contains promotional advertising, it could appear in the form of pop-ups, or it could appear in the browser's toolbar and redirect search requests.

Although not necessarily harmful, adware can:

- highlight weaknesses in a user's security defences
- be hard to remove – it defeats most anti-malware software since it can be difficult to determine whether or not it is 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 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 can't unlock it until the demands of the cybercriminal have been met. This malware restricts access to the computer and encrypts all the data until a ransom is paid. It can 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 back-ups of key files are kept and thus avoid having to pay a ransom.

Summary of malware

Table 5.2 summarises the six types of malware described in Section 5.3.1.

▼ **Table 5.2** Summary of types of malware

Viruses – programs (or program code) that can replicate/copy themselves with the intention of deleting or corrupting files, or causing 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 – these are types of standalone viruses that can replicate themselves with the intention of spreading to other computers; they often networks to search out computers with weak security that 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 spyware monitors key presses and is then 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

Phishing

Phishing occurs when a cybercriminal sends out legitimate-looking emails to users. The emails may contain links or attachments that, when initiated, take the user to a fake website; or they may trick the user into responding with personal data (for example, bank account details or credit/debit card details).

The email usually appears to be genuine coming from a known bank or service provider (also refer to Section 5.3.2). The key point is that the recipient has to initiate some act before the phishing scam can cause any harm. If suspicious emails are deleted or not opened, then phishing attacks won't cause any problems.

There are numerous ways to help prevent phishing attacks:

- users need to be aware of new phishing scams; those people in industry or commerce should undergo frequent security awareness training to become aware of how to identify phishing (and pharming) scams
- it is important not to click on any emails links unless totally certain that it is safe to do so; fake emails can often be identified by 'Dear Customer ......' or 'Dear email person@gmail.com ....' and so on
- it is important to run anti-phishing toolbars on browsers (this includes tablets and mobile phones) since these will alert the user to malicious websites contained in an email
- always look out for https or the green padlock symbol 🔒 in the address bar

- regular checks of online accounts are also advisable as well as maintaining passwords on a regular basis
- ensure an up-to-date browser is running on the computer device (which contains all of the latest security upgrades) and run a good firewall in the background at all times; a combination of a desktop firewall (usually software) and a network firewall (usually hardware) considerably reduces the risk of hacking, pharming and phishing on network computers
- be very wary of pop-ups and use the browser to block them; if pop-ups get through your defences, don't click on 'cancel' since this can ultimately lead to phishing or pharming sites – the best option is to select the small ✖ in the top right-hand corner of the pop-up window which closes it down.

Note: another term connected to phishing is **spear phishing**; this is where the cybercriminal targets **specific** individuals or companies to gain access to sensitive financial information or industrial espionage – regular phishing is not specific regarding who the victims are.

Pharming

Link

See Section 5.1 for more on URLs, IP addresses and DNS (Domain Name Server).

Pharming is malicious code installed on a user's computer or on an infected website. The code redirects the user's browser to a fake website **without** the user's knowledge. Unlike phishing, the user doesn't actually need to take any action for it to be initiated. The creator of the malicious code can gain personal data, such as bank details, from the user. Often the website appears to come from a trusted source and can lead to fraud and identity theft.

Why does pharming pose a threat to data security?

As mentioned above, pharming redirects internet users to a fake or malicious website set up by, for example, a hacker; redirection from a legitimate website to the fake website can be done using **DNS cache poisoning**.

Every time a user types in a URL, their browser contacts the DNS server; the IP address of the website will then be sent back to their browser. However, DNS cache poisoning changes the real IP address values to those of the fake website; consequently, the user's computer will connect to the fake website.

When a user enters a web address (URL) into a browser, the computer is sent the IP address of the website; if the IP address has been modified somehow the user's computer will be redirected to the fake website.

It is possible to mitigate against the risk of pharming:

- Use of anti-virus software can detect unauthorised alterations to a website address and warn the user of the potential risks.
- However, if the DNS server itself has been infected (rather than the user's computer) it is much more difficult to mitigate the risk.
- Many modern browsers can alert users to pharming and phishing attacks.
- It is very important to check the spelling of websites to ensure the web address used is correct.
- As with phishing, use of https or the green padlock symbol 🔒 in the address bar is an additional form of defence.

Activity 5.3

1 A company has offices in four different countries. Communication and data sharing between the offices is done via computers connecting over the internet.

   a Describe **three** data security issues the company might encounter during their day-to-day communications and data sharing.

   b For each issue described, explain why it could be a threat to the security of the company.

   c For each issue described, describe a way to mitigate the threat that has been posed.

2 Explain the following three terms:

   – worm
   – ransomware
   – Trojan horse.

3 John works for a car company. He maintains the database that contains all the personal data of the people working for the car company. John was born on 28th February 1990 and has two pet cats called Felix and Max.

   a John needs to use a password and a user name to log onto the database. Why would the following passwords not be a very good choice:

      i 280290

      ii FiLix1234

      iii John04

   b Describe how John could improve his passwords and also how he should maintain his passwords to maximise database security.

   c When John enters a password on his computer he is presented with the following question on his screen:

      Would you like to save the password on this device?

      Why is it important that John always says **No** to this question?

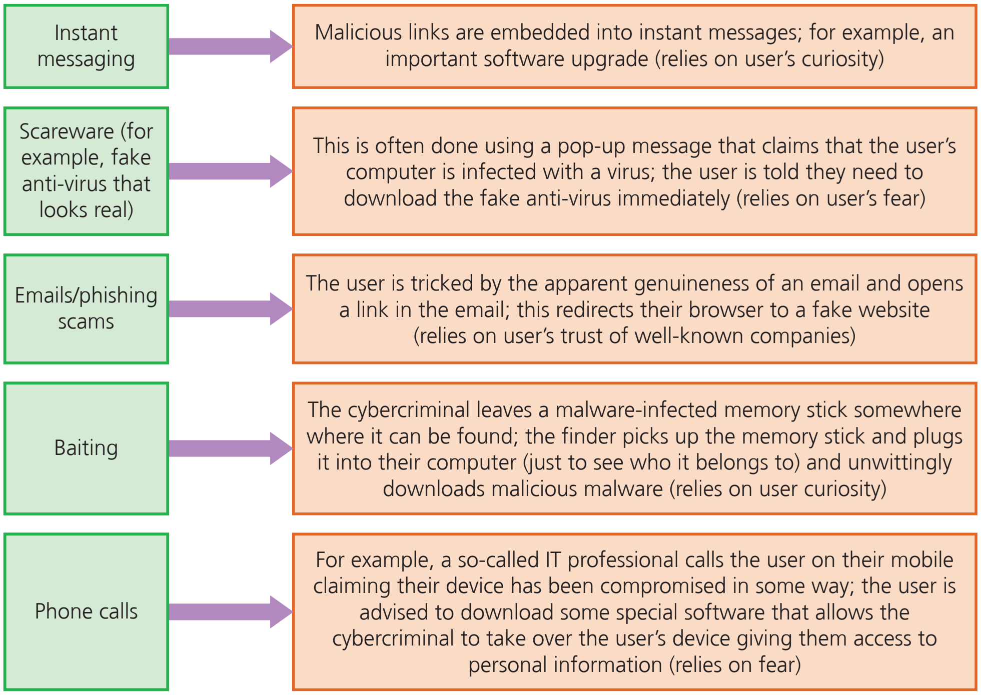
Find out more

Apart from malware, data can be ***accidentally*** lost. Find out ways that data could be recovered and ways to minimise the risk for each of the following situations:

1 Accidental data loss, such as accidental deletion of a file
2 Hardware fault, such as a head crash on a hard disk drive
3 Software fault, due to installation of software incompatible with existing software
4 Incorrect operation of the computer, such as using incorrect procedure for the removal of a memory stick from a computer.

Social engineering

Social engineering occurs when a cybercriminal creates a social situation that can lead to a potential victim dropping their guard. It involves the manipulation of people into breaking their normal security procedures and not following best practice. There are five types of threat that commonly exist:



Instant messaging	Malicious links are embedded into instant messages; for example, an important software upgrade (relies on user's curiosity)
Scareware (for example, fake anti-virus that looks real)	This is often done using a pop-up message that claims that the user's computer is infected with a virus; the user is told they need to download the fake anti-virus immediately (relies on user's fear)
Emails/phishing scams	The user is tricked by the apparent genuineness of an email and opens a link in the email; this redirects their browser to a fake website (relies on user's trust of well-known companies)
Baiting	The cybercriminal leaves a malware-infected memory stick somewhere where it can be found; the finder picks up the memory stick and plugs it into their computer (just to see who it belongs to) and unwittingly downloads malicious malware (relies on user curiosity)
Phone calls	For example, a so-called IT professional calls the user on their mobile claiming their device has been compromised in some way; the user is advised to download some special software that allows the cybercriminal to take over the user's device giving them access to personal information (relies on fear)

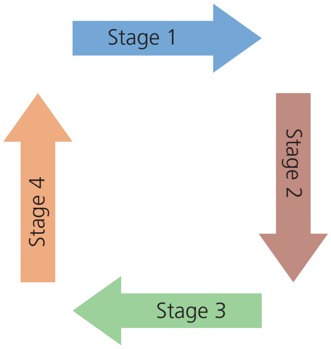
▲ **Figure 5.11** Social engineering

It is clear from the five examples that social engineering links into many other types of malware, and is an effective method of introducing malware. The whole idea is based on the exploitation of certain human emotions; the three most common ones to exploit are:

- fear – the user is panicked into believing their computer is in immediate danger and isn't given time to logically decide if the danger is genuine or not; fear is a very powerful emotion that can easily be exploited by a cybercriminal
- curiosity – the user can be tricked into believing they have won a car or they find an infected memory stick lying around; their curiosity gets the better of them and they give their details willingly to win the car (for example, credit card details to pay for delivery or road tax) or they are curious who the memory stick belongs to; without thinking clearly, their curiosity gets the better of them and the damage is done
- empathy and trust – a real belief that all genuine-sounding companies can be trusted, therefore emails or phone calls coming from such companies must be safe; a dangerous assumption that the cybercriminal can exploit fully.

There is no hacking involved, since the user is willingly allowing the cybercriminal to have access to their computer, to download malicious software or visit fake websites; the user is rushed into making rash decisions.

Figure 5.12 shows the course of action taken by a cybercriminal in targeting their victim:



Stage 1 – The victims are identified; information about victim gathered and method of attack decided

Stage 2 – At this stage the victim is being targeted (either through email, phone call, Trojan horse and so on; it all depends on who the victim is)

Stage 3 – The attack on the victim is now executed allowing the cybercriminal to obtain the information or to cause the disruption decided on at Stage 1

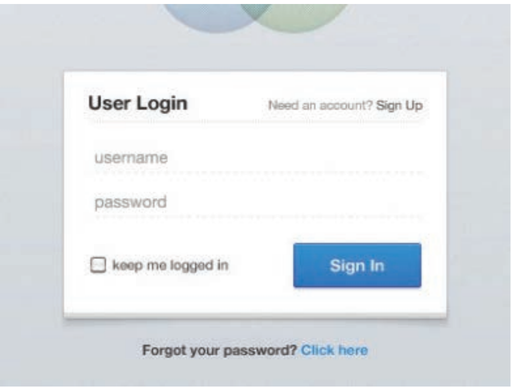
Stage 4 – When the cybercriminal has decided they have what they wanted they try to remove all traces of the malware to cover their tracks

▲ **Figure 5.12** Stages in a typical social engineering scam

5.3.2 Keeping data safe from security threats

Access levels

In many computer systems, user accounts control a user's rights. This often involves having different **levels of access** for different people. For example, in a hospital it would not be appropriate for a cleaner to have access to medical data about a patient. However, a consultant would need access to this vital data. Therefore, most systems have a hierarchy of access levels depending on a person's level of security; this is usually achieved using a user name and password as shown in Figure 5.13.



▲ **Figure 5.13** Access level log in screen

When using databases, levels of access are particularly important; it is essential to determine who has the right to read, write and delete data, for example. By having different views of data tables, it is possible for different users to only have access to certain data.

Link

See Chapter 9 for more details about databases.

Another area where access levels are very important is in social networks (such as Facebook); with this type of application, there are usually four access levels:

1 public access (this refers to the data anyone from the general public can access)
2 friends (only people identified as 'friends' by the owner of the data can see certain data)
3 custom (this allows the user to further refine what data can be seen by 'friends' allowing them to exclude certain content from selected people)
4 data owner (this is data only the owner of the data can see).

In this type of application, users are allowed to use **privacy settings** rather than passwords to decide the level of access (for more on this see later in this section).

Anti-malware

The two most common types of anti-malware are anti-virus and anti-spyware.

Link

For more on anti-virus software see Section 4.1.

Anti-virus

Anti-virus has already been described in great detail in Chapter 4.

Anti-spyware

Anti-spyware software detects and removes spyware programs installed illegally on a user's computer system. The software is based on one of the following methods:

- rules – in this case, the software looks for typical features which are usually associated with spyware thus identifying any potential security issues
- file structures – in this case, there are certain file structures associated with potential spyware which allows them to be identified by the software.

Anti-spyware is now often part of a generic malware bundle that contains an anti-virus, anti-spyware and a personal firewall.

The general features of anti-spyware are:

- detect and remove spyware already installed on a device
- prevent a user from downloading spyware
- encrypt files to make the data more secure in case it is 'spied' on
- encryption of keyboard strokes to help remove the risk posed by the keylogging aspects of some spyware
- blocks access to a user's webcam and microphone (the software stops the spyware taking over the control of a user's webcam and microphone which can be used to collect information without the user's knowledge)
- scans for signs that the user's personal information has been stolen and warns the user if this has happened.

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).

There are a number of ways authentication can be done.

Passwords and user names

Passwords are used to restrict access to data or systems. They should be hard to crack and changed frequently to retain any real level of security. Passwords can also take the form of biometrics (for example, on a mobile phone – see later). 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
- 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 aren't being relayed back to whoever put the spyware on your computer
- change passwords on a regular basis in case they have come into the possession of another user, illegally or accidentally
- passwords should not be easy to crack (for example, your favourite colour, name of a pet or favourite music artist); passwords are grouped as either strong (hard to crack or guess) or weak (relatively easy to crack or guess)
- 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 else can see what the user has typed in. If the user's password doesn't match up with the user name then access will be denied. Many systems ask for a new password to be typed in twice as a verification check (to check for input errors). To help protect the system, users are only allowed to type in their password a finite number of times – usually three times is the maximum number of tries allowed before the system locks the user out. After that, the user will be unable to log on until they have reset their password.

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

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

Activity 5.4

1 Which of the following are weak passwords and which are strong passwords? Explain your decision in each case.
   - a 25-May-2000
   - b Pas5word
   - c ChapTer@06
   - d AbC*N55!
   - e 12345X

2 An airport uses a computer system to control security, flight bookings, passenger lists, administration and customer services.
   - a Describe how it is possible to ensure the safety of the data on the system so that senior staff can see all the data, while customers can only access flight times (arrivals and departures) and duty-free offers.
   - b Describe how the airport can guard against malware attacks from outside and also from customers using the airport services.

Biometrics

Biometrics can be used in much the same way as passwords as a way of identifying a user. Biometrics relies on certain unique characteristics of human beings; examples include:

- fingerprint scans
- retina scans
- face recognition
- voice recognition.

Link

For more on face recognition scans see Section 3.2.1.

Biometrics is used in a number of applications as a security device. For example, some of the latest mobile phones use fingerprint matching before they can be operated; some pharmaceutical companies use face recognition or retina scans to allow entry to secure areas.

We will now consider fingerprint scanning and retina scans in a little more detail.

Fingerprint scans

▲ **Figure 5.14** Fingerprint scan

Images of fingerprints are compared against previously scanned fingerprint images stored in a database; if they match, then a user has been correctly recognised. The system compares patterns of 'ridges' and 'valleys' that are unique. The accuracy of the scan is about around 1 in 5000. Fingerprint scanning techniques have the following benefits as a form of security:

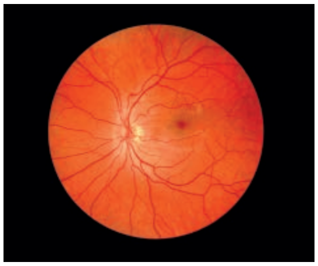
- fingerprints are unique, therefore this technique can improve security since it would be difficult to replicate a person's fingerprints
- other security devices (such as magnetic cards to gain entry to a building) can be lost or even stolen which makes them less effective
- it would be impossible to 'sign in' for somebody else since the fingerprints would match with only one person on the database
- fingerprints can't be misplaced; a person always has them!

What are the drawbacks of fingerprint scanning?

- 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 any biometric device as an infringement of civil liberties.

Retina scans

Retina scans use infrared light to scan the unique pattern of blood vessels in the retina (at the back of the eye); it is a rather unpleasant technique requiring a person to sit totally still for 10 to 15 seconds while the scan takes place; it is very secure since nobody has yet found a way to duplicate the blood vessels patterns. The accuracy is about 1 in 10 million.



▲ **Figure 5.15** Retina scan

Table 5.3 shows a comparison of the benefits and drawbacks of the four common biometric techniques:

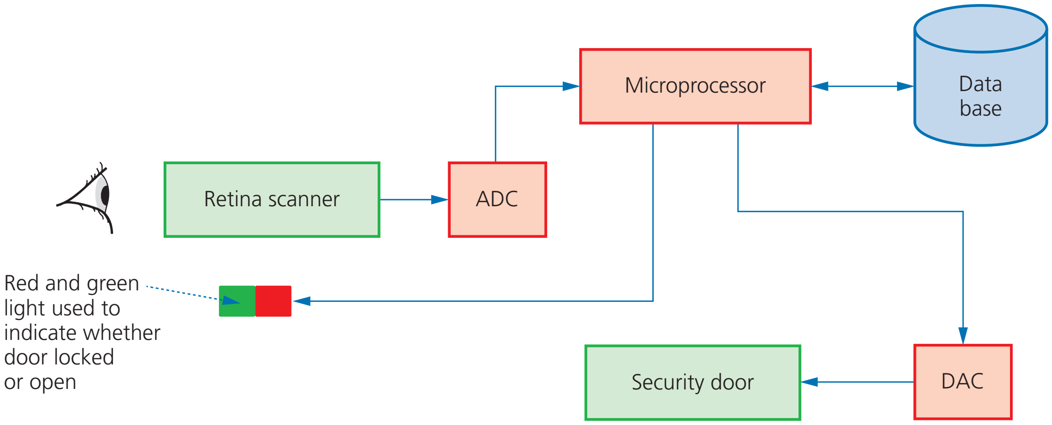
▼ **Table 5.3** Comparison of biometric devices

Biometric technique	Benefits	Drawbacks
fingerprint scans	it is 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, since it is still related to criminal identification it can make mistakes if the skin is dirty or damaged (e.g. cuts)
retina scans	very high accuracy there is no known way to replicate a person's retina	it is very intrusive it can be relatively slow to verify retina scan with stored scans very expensive to install and set up
face recognition	non-intrusive method relatively inexpensive technology	it can be affected by changes in lighting, the person's hair, change in age, and if the person is wearing glasses
voice recognition	non-intrusive method verification takes less than 5 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

Biometric applications

A door security system protected by retina scanner

In this example, a company uses retina scans to permit entry to their secure research laboratories.


Microprocessor
Data base
Retina scanner
ADC
Red and green light used to indicate whether door locked or open
Security door
DAC

▲ **Figure 5.16** Security system controlled by retina scanners

A person stands facing the retina scanner. The scanned data is sent via an ADC (analogue-digital converter) to a microprocessor. The microprocessor compares the data received with retina scan data already stored in a database. If the two sets of data match, a signal is sent to turn a light from red to green and also unlock the security door. The door is controlled by a DAC (digital-analogue converter) and an actuator. If the retina scan data and database data don't match, then entry is denied and the light remains red.

Link

For more on actuators see Chapter 3.

Find out more

One of the most common security systems used on mobile phones is the ***capacitance fingerprint reader***. Describe how this system works.

Activity 5.5

1 In the biometric application example, retina scans were used to control entry to a secure research building.

 a Describe how the system might change if face recognition was used instead of retina scanners. The system is triggered automatically if a motion sensor detects the presence of a person.

 b Name other biometric devices which could be used to control entry to this building.

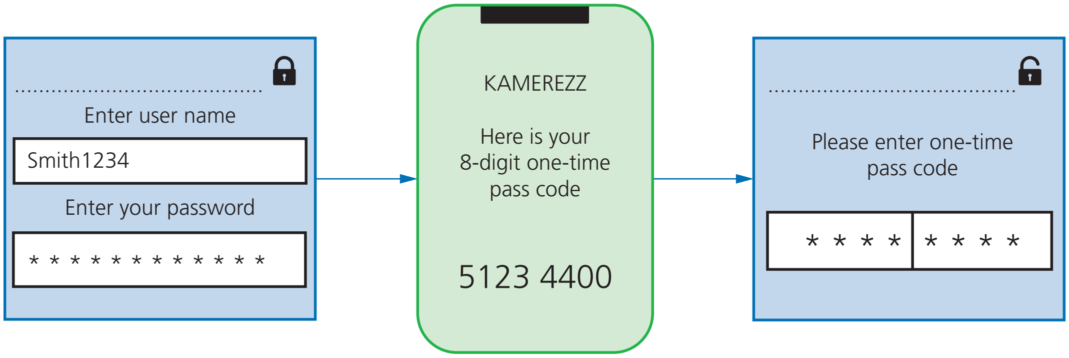
2 Many cars now use voice control as a form of security before a car can be started and it is also used to give some key commands, such as start navigation system. Describe the benefits and drawbacks of such systems in cars.

Two-step verification

Two-step verification 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 1 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. In summary:



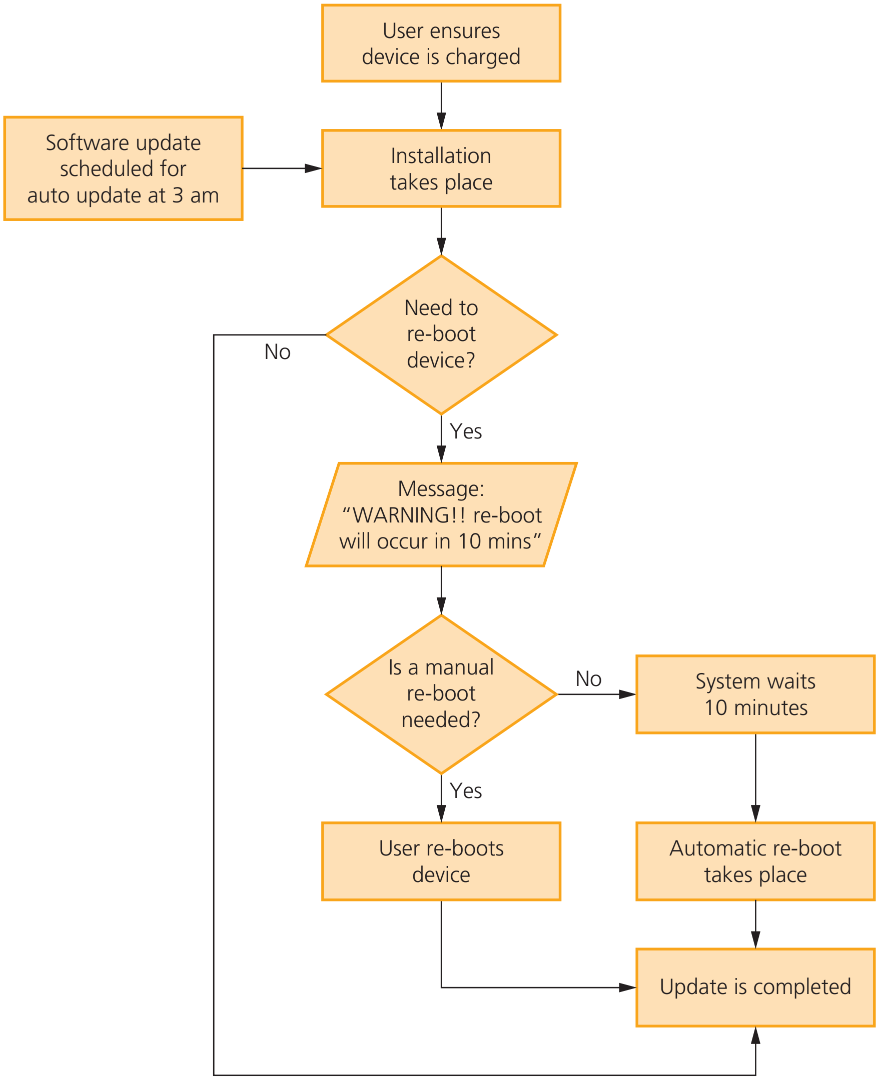
▲ **Figure 5.17** Two-step verification using a mobile phone

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.

Automatic software updates

Automatic software updates mean software on computers and mobile phones/tablets is kept up-to-date. Sometimes this is done overnight or when you log off the device.

These updates are vital since they may contain **patches** that update the software security (to protect against malware) or improve the software performance (for example, removal of bugs and addition of new features). The only downside to this is the potential for updates to disrupt your device following installation. If this happens, the user either has to wait for another patch to put this right, or use the techniques described in Chapter 4 that reverse the clock time to an earlier date before the updates were made.


User ensures device is charged
Software update scheduled for auto update at 3 am
Installation takes place
Need to re-boot device?
No
Yes
Message: “WARNING!! re-boot will occur in 10 mins”
Is a manual re-boot needed?
No
Yes
System waits 10 minutes
User re-boots device
Automatic re-boot takes place
Update is completed

▲ **Figure 5.18** Automatic software update flow chart

Checking the spelling and tone of communication and URL links

When emails are sent to you, there are three actions you always need to take before opening them or activating any links in them.

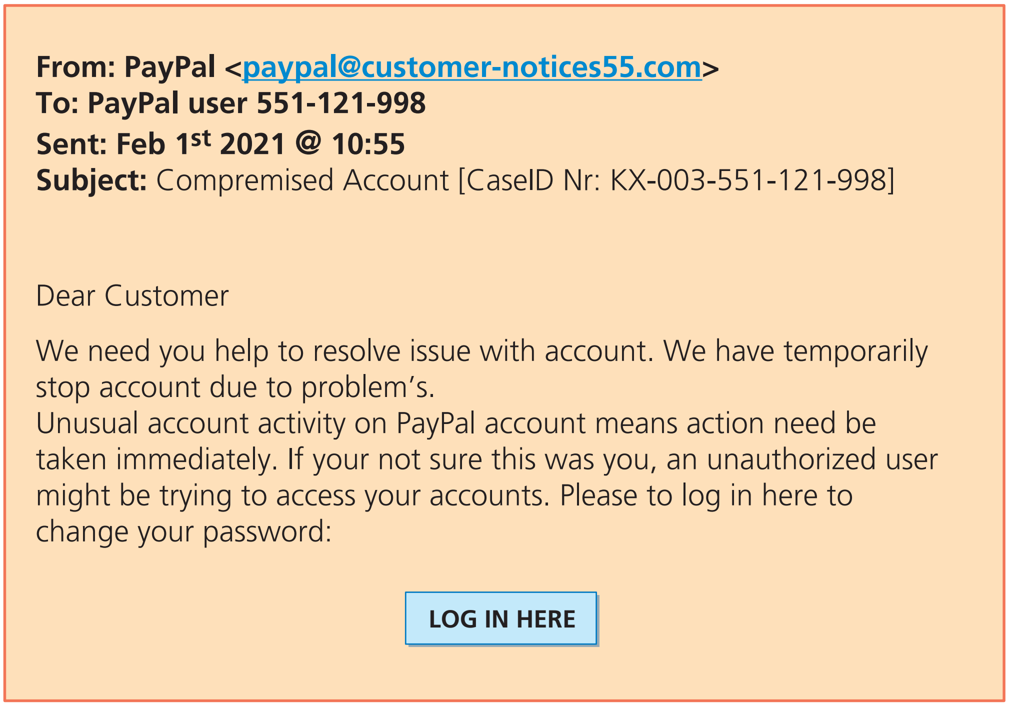
- Check out the spellings in the email and in the links; professional, genuine organisations will not send out emails which contain spelling or major grammatical errors (for example, Amazzon.com)
- Carefully check the tone used in the email message; if it is rushing you into doing something or if the language used seems inappropriate or incorrect, then it could be a phishing email or worse.

There are five things to look out for:

1 The email address itself; no legitimate company will use an email address such as: @gmail.com
Carefully check the part of the address after the '@' symbol which should match the company's name; for example:

account-update@amazon.com

2 The tone of the email and bad spelling of words is a clear indication of a potential scam. Look at this message that claimed it came from PayPal. See if you can find the ten errors in the email that should set off alarm bells.



From: PayPal <paypal@customer-notices55.com>
To: PayPal user 551-121-998
Sent: Feb 1st 2021 @ 10:55
Subject: Compremised Account [CaseID Nr: KX-003-551-121-998]

Dear Customer

We need you help to resolve issue with account. We have temporarily stop account due to problem's.
Unusual account activity on PayPal account means action need be taken immediately. If your not sure this was you, an unauthorized user might be trying to access your accounts. Please to log in here to change your password:

▲ **Figure 5.19** Sample scam email

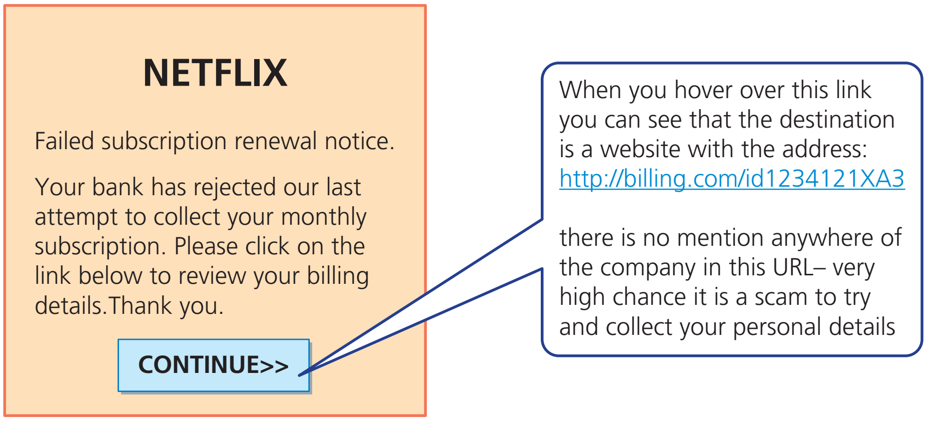
Did you find all the errors? An email like this looks official but there are many clues that it didn't come from a legitimate company; such as, many spelling mistakes, grammatical errors and the domain name in the email address. An email like this should be regarded as phishing; by clicking on the 'LOG IN HERE' box, you will divulge passwords and other key information since you will be sent to a fake 'PayPal' website.

3 Misspelling of domain names in a link are very common errors found in emails sent by scammers and fraudsters. The authors of this book have seen these incorrect spellings:

www.gougle.com
www.amozon.com

This is known as **typo squatting** where names close to the genuine names are used to fool you.

4 Suspicious links; destination addresses should match the rest of the email. Look at this message that claims to be from Netflix:



NETFLIX

Failed subscription renewal notice.

Your bank has rejected our last attempt to collect your monthly subscription. Please click on the link below to review your billing details.Thank you.

CONTINUE>>

When you hover over this link you can see that the destination is a website with the address: http://billing.com/id1234121XA3

there is no mention anywhere of the company in this URL– very high chance it is a scam to try and collect your personal details

▲ **Figure 5.20** Second example of probable scam

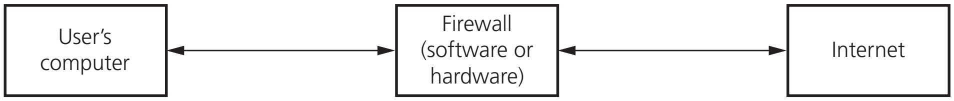
5 Other errors to look out for are just plain spelling mistakes. Look at this address from TKMaxx; find the three errors:

http://www.tkmax.co.ie

- since the company involve online payments, it's very likely to use secure links therefore you would expect to see `https`
- the spelling of the company is incorrect
- it is more likely to see `.com` since they are a large company.

Firewalls

A **firewall** can be either software or hardware. It sits between the user's computer and an external network (for example, the internet) and filters information in and out of the computer. This allows the user to decide whether or not to allow communication with an external source and it also warns a user that an external source is trying to access their computer. Firewalls are the primary defence to any computer system to help protect it from hacking, malware (viruses and spyware), phishing and pharming.



▲ **Figure 5.21** Typical firewall set up

The main tasks carried out by a firewall include:

- 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. Alternatively, the firewall can be software installed on a computer; in some cases, it is part of the operating system.

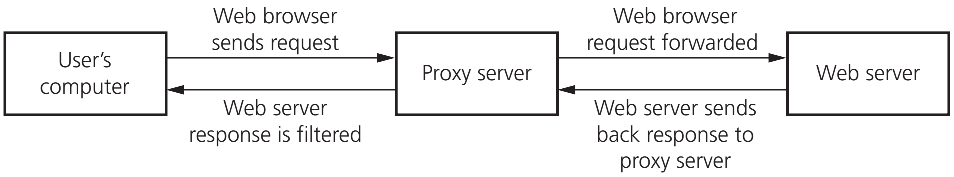
However, there are certain circumstances where the firewall can't prevent potential harmful 'traffic':

- it cannot prevent individuals, on internal networks, using their own hardware devices (e.g. modems, smartphones) to bypass the firewall
- employee misconduct or carelessness cannot be controlled by firewalls (for example, control of passwords or user accounts)
- users on stand-alone computers can choose to disable the firewall, leaving their computer open to harmful 'traffic' from the internet.

All of these issues require management control or personal control (on a single computer) to ensure that the firewall is allowed to do its job effectively.

Proxy servers

Proxy servers act as an intermediate between the user and a web server:



User's computer
Web browser sends request
Web server response is filtered
Proxy server
Web browser request forwarded
Web server sends back response to proxy server
Web server

▲ **Figure 5.22** Proxy server

Features of proxy servers:

- allows internet traffic to be filtered; it is possible to block access to a website if necessary
- keeps users' IP addresses secret which improves security
- if the internet traffic is valid, access to the web server is allowed
- if the internet traffic is invalid, access to the web server is denied
- it is possible to block requests from certain IP addresses
- prevents direct access to a web server by sitting between the user and the web server
- if an attack is launched, it hits the proxy server instead – this helps to prevent hacking, DoS, and so on
- used to direct invalid traffic away from web servers which gives additional protection
- by using the feature known as a cache, it is possible to speed up access to information/data from a website; when the website is first visited, the home page is stored on the proxy server; when the user next visits the website, it now comes from the proxy server cache instead, giving much faster access
- proxy servers can also act as firewalls.

Privacy settings

Privacy settings are the controls available on web browsers, social networks and other websites that are designed to limit who can access and see a user's personal profile. They were discussed earlier in the section on access rights. Privacy settings can refer to:

- a 'do not track' setting; the intention here is to stop websites collecting and using browsing data which leads to improved security
- a check to see if payment methods have been saved on websites; this is a useful safety feature which prevents the need to type in payment details again (every time you have type in financial details, there will be a risk of data interception)
- safer browsing; an alert is given when the browser encounters a potentially dangerous website (the undesirable website will be in a 'blacklist' stored on the user's computer)
- web browser privacy options (e.g. storing browsing history, storing cookies)
- website advertising opt-outs; a website may be tracked by any number of third parties who gather information about your browsing behaviour for advertising purposes
- apps; for instance, the sharing of location data in map apps can be switched off.

Secure sockets layer (SSL)

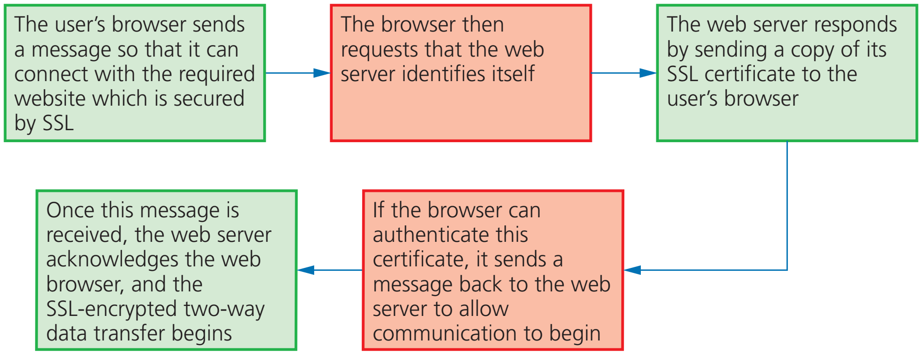
Secure Sockets Layer (SSL) is a type of protocol – a set of rules used by computers to communicate with each other across a network. This allows data to be sent and received securely over the internet.

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 https 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:	ℹ	http://www.yyyy.co.uk/documents

Figure 5.23 shows what happens when a user wants to access a secure website and receive and send data to it:



The user's browser sends a message so that it can connect with the required website which is secured by SSL

The browser then requests that the web server identifies itself

The web server responds by sending a copy of its SSL certificate to the user's browser

If the browser can authenticate this certificate, it sends a message back to the web server to allow communication to begin

Once this message is received, the web server acknowledges the web browser, and the SSL-encrypted two-way data transfer begins

▲ **Figure 5.23** Secure sockets layer (SSL)

The term **SSL certificate** was mentioned in Figure 5.23. An SSL certificate is a form of digital certificate which is used to authenticate a website. This means any communication or data exchange between browser and website is secure provided this certificate can be authenticated.

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 Protocols (VoIP) when carrying out video chatting and/or audio chatting over the internet
- used in instant messaging
- when making use of a social networking site.

Activity 5.6

1 Which computer terms (used in this chapter) are being described below?

a a user is granted access only after successfully presenting two pieces of evidence to verify or identify who they are

b uses a cache to speed up access to web pages from a website

c controls that are used on social networks and other websites to allow users to limit who can access data from their stored profile

d protocol that is used to allow data to be sent securely over a network, such as the internet

e software or hardware that sits between a computer and an external network which monitors and filters out all incoming and outgoing traffic

f supplies domain names for internet hosts and is used to find IP addresses of domain names

g use of unique human characteristics to identify a user as a form of authentication

h made up of three types of identification:
- something you know
- something you have
- something you are

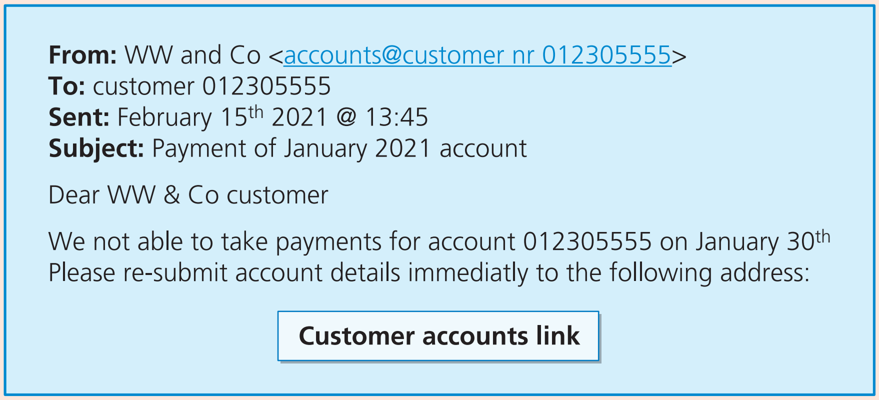
i manipulation of people into breaking normal security procedures and best practices to gain illegal access to a user's computer system

j malicious code stored on a user's hard drive or web server used to redirect a browser to a fake website without their knowledge

2 Describe how SSL and TLS certificates are used to ensure that secure sharing of data between a browser and website takes place.

3 a Describe three things you should look out for when deciding whether or not an email is a potential phishing scam.

b Identify at least three potentials problems with this email from a company called Watson, Williams and Co:



From: WW and Co <accounts@customer nr 012305555>
To: customer 012305555
Sent: February 15th 2021 @ 13:45
Subject: Payment of January 2021 account

Dear WW & Co customer

We not able to take payments for account 012305555 on January 30th
Please re-submit account details immediatly to the following address:

Extension

For those students considering the study of this subject at A Level, the following extension to SSL may be of interest.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a more modern and more secure version of SSL. It is a form of protocol that ensures the security and privacy of data between devices and users when communicating over a network (for example, the internet). It is essentially designed to provide encryption, authentication and data integrity in a more effective way than its predecessor, SSL. When a website and client communicate over the internet, TLS is designed to prevent third party eavesdropping which could cause a breach of security. TLS is comprised of two main layers:

- record protocol – this part of the communication can be used with or without encryption (it contains the data being transmitted over the network/internet)
- handshake protocol – this permits the web server and client to authenticate each other and to make use of encryption algorithms (a secure session between client and server is then established).

Only the most recent web browsers support both SSL and TLS which is why the older, less secure, SSL is still used in many cases (although very soon SSL won't be supported and users will have to adopt the newer TLS protocol if they wish to access the internet using a browser). The main differences between SSL and TLS can be summarised as follows:

- it is possible to extend TLS by adding new authentication methods (unlike SSL)
- TLS can make use of session caching which improves the overall performance of the communication when compared to SSL (see below)
- TLS separates the handshaking process from the record protocol (layer) where all the data is held.

Session caching

When opening a TLS session, it requires considerable computer time (due mainly to complex cryptographic processes taking place). The use of session caching can avoid the need to utilise as much computer time for each connection. TLS can either establish a new session or attempt to resume an existing session; using the latter can considerably boost the system performance.

Summary

As already indicated, two of the main functions of SSL/TLS are:

- encryption of data
- identifying client and server to ensure each knows 'who they are communicating with'.

We will now consider how this is done:

Stage 1

Once the client types the URL into the browser and hits the <enter> key, several steps will occur before any actual encrypted data is sent; this is known as the handshaking stage.

Stage 2

The client's browser now requests secure pages (https) from the web server.

Stage 3

The web server sends back the TLS digital certificate (which also contains the public key) – the certificate is digitally signed by a third party called the Certificate Authority (CA).

Stage 4

Once the client's browser receives the digital certificate it checks:

- the digital signature of the CA (is it one of those in the browser's trusted store – a list of trusted CAs is part of the browser which the client downloads to their computer)
- that the start and end dates shown on the certificate are still valid
- that the domain listed in the certificate is an exact match with the domain requested by the client in the first place

Stage 5

Once the browser trusts the digital certificate, the public key (which forms part of the digital certificate) is used by the browser to generate a temporary session key with the web server; this session key is then sent back to the web server.

Stage 6

The web server uses its private key to decrypt the session key and then sends back an acknowledgement that is encrypted using the same session key).

Stage 7

The browser and web server can now encrypt all the data/traffic sent over the connection using this session key; a secure communication can now take place.