# Cambridge

## OL- IGCSE

# ICT

CODE: (0417)

## Chapter 08

# Safety and security

# 8.1 Physical safety

## 8.1.1 Safety issues

**Physical safety** is a different issue to health risks. 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.

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

| Safety risk | Cause of safety risk | Prevention measures |
|---|---|---|
| Electrocution | » Spilling liquids/drinks on electric equipment<br>» Exposed wires/damaged insulation<br>» Unsafe electrical equipment<br>» Unsafe electrics (for example, wall sockets) in the office | » Do not allow drinks to be taken into the computer room<br>» Check all wires on a regular basis and renew wires if there is any sign of damaged insulation<br>» Ensure all equipment is checked by a qualified electrician on a regular basis<br>» Make use of an RCB (residual current breaker) to prevent electrocution |
| Fire hazard | » Overloaded wall sockets (several items plugged into one wall socket)<br>» Overheating of computer equipment (due to poor heat dissipation)<br>» Exposed wires causing a short circuit | » Increase the number of wall sockets and do not use too many extension blocks<br>» Do not cover the cooling vents on computer equipment<br>» Clean out dust accumulation in computers to prevent overheating<br>» Make sure all equipment is fully tested on a regular basis<br>» Ensure there is good room ventilation<br>» Use low-voltage equipment wherever possible<br>» Have a number of fully tested **carbon dioxide/dry powder fire extinguishers** |
| Tripping hazard | » Trailing wires on the floor<br>» Damaged carpets and other flooring | » Use cable ducts to make the wires safe<br>» Cover exposed wires and hide wires under desks away from general thoroughfare<br>» Use wireless connectivity wherever possible, therefore eliminating the need for trailing cables |
| Personal injury | » Heavy equipment unstable or falling from desks<br>» Desks collapsing under weight/desks not designed to take the weight | » Use desks strong enough to take the weight of the computer equipment<br>» 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.

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.

### 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.

### 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.

### 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

» 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? 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.

## 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.

### Online gaming

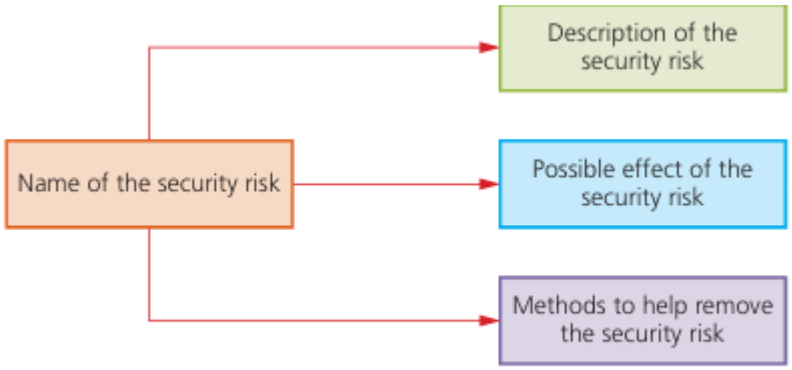
Online gaming has increased over the last few years. There are many reasons for this, such as better internet connections, more sophisticated mobile devices (phones and tablets) and greater realism in recent games. It is important to be careful when using online gaming because is also carries risks.

## 8.3 Security of data

### 8.3.1 Data threats

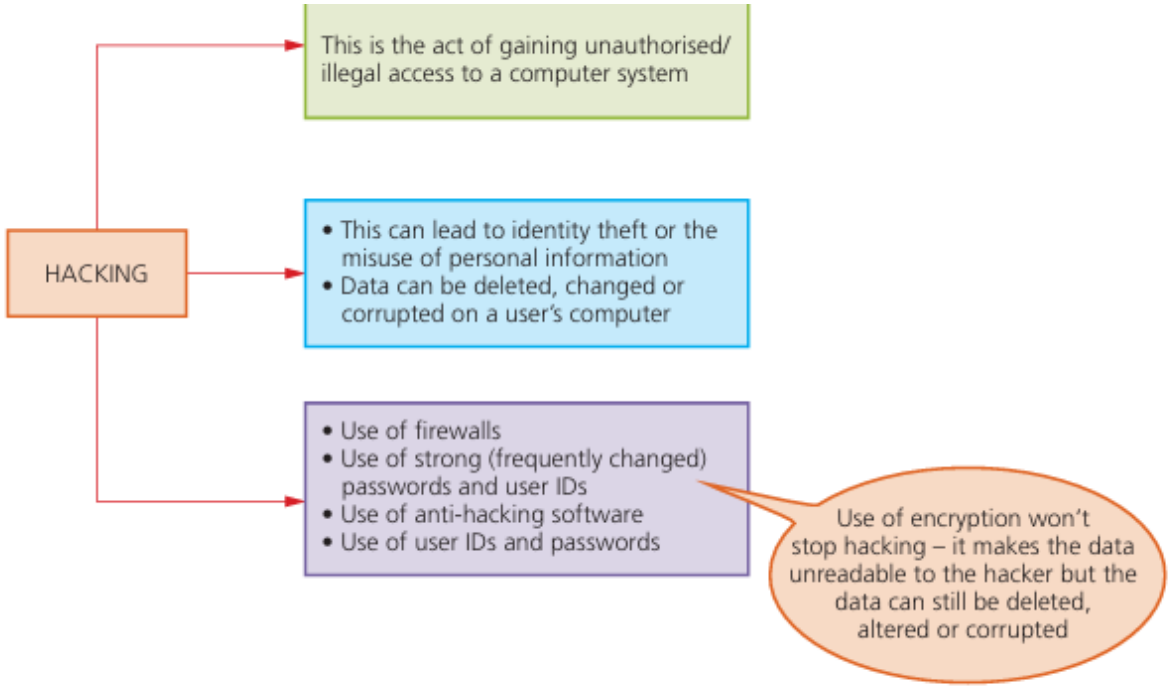
There are a number of security risks to data held on a computer/smartphone or data being transferred around networks. This section covers a large number of these risks:

» Hacking » Phishing » Vishing » Smishing » Pharming » Viruses
» Malware » Card fraud.



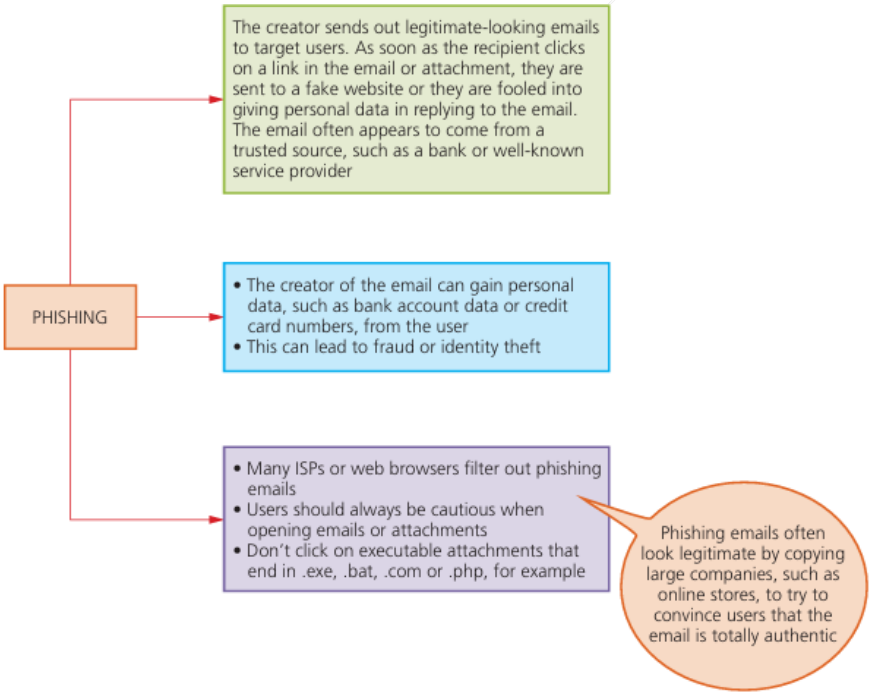

▲ **Figure 8.2** Security risks

## Hacking




▲ **Figure 8.3** Risks of hacking

## Phishing, smishing, vishing



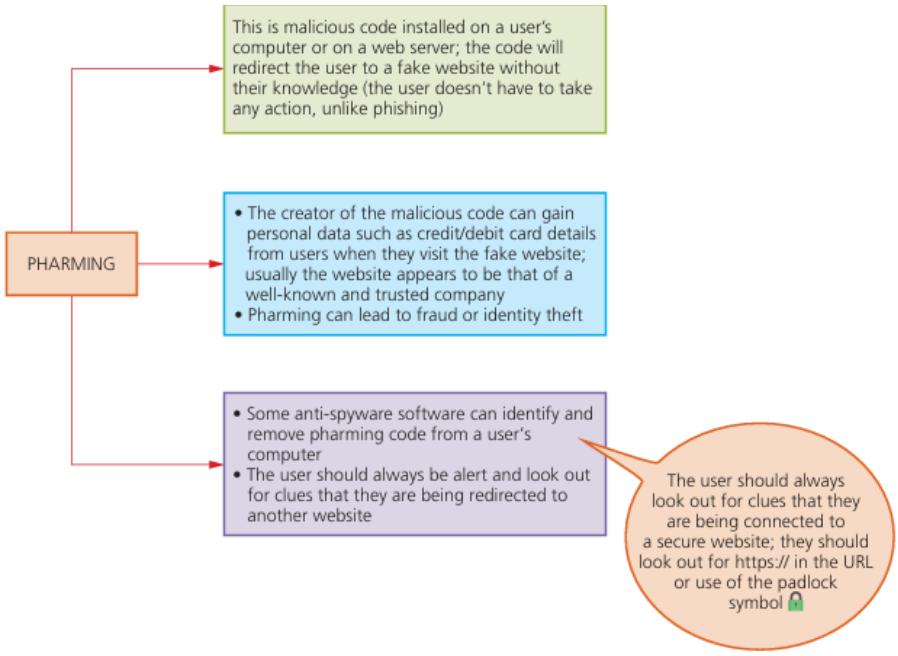

▲ **Figure 8.4** Risks of phishing

**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.

**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.

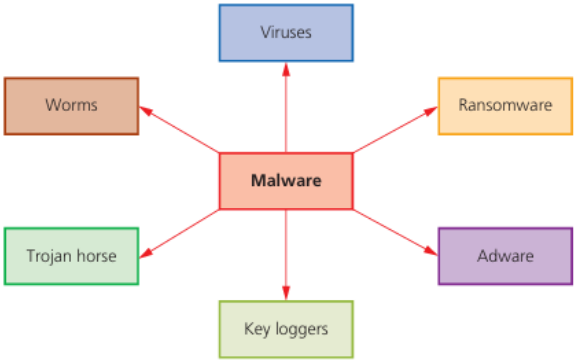
**Pharming**




▲ **Figure 8.5** Risks of pharming

## Viruses and malware

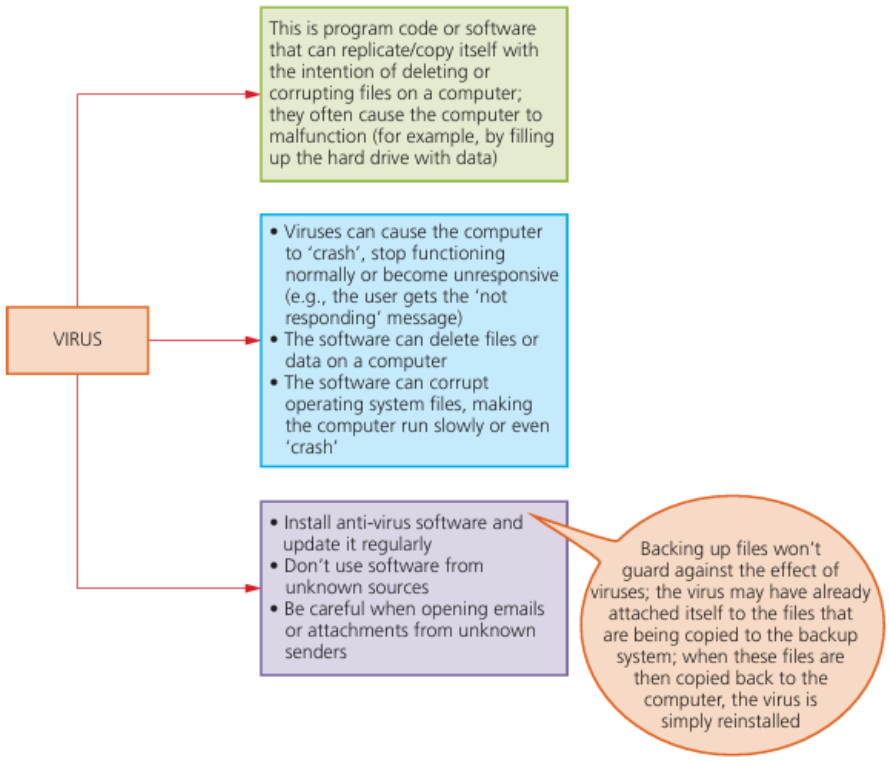
**Malware** is one of the biggest risks to the integrity and security of data on a computer system. Many software applications, such as anti-virus, are capable of identifying and removing most of the forms of malware.




▲ **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

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

**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.

## 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.

Spyware (including key logging software) and ransomware are often installed on a user's computer via Trojan horse 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.

However, some key loggers work by capturing screen images at random intervals; these are known screen recorders.

**Adware**

Adware is a type of malware. At its least dangerous, it will attempt to flood an end-user with unwanted advertising.

**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.

▼ **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.

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.

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.

### 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.

## 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.

### Biometric authentication

Biometrics relies on certain unique characteristics of human beings.

### Fingerprint scans

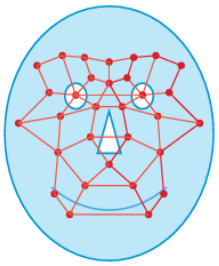
Images of fingerprints are compared against previously scanned fingerprints stored in a database; if they match then access is allowed. The system compares patterns of ‘ridges’ and ‘valleys’ which are unique.

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

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

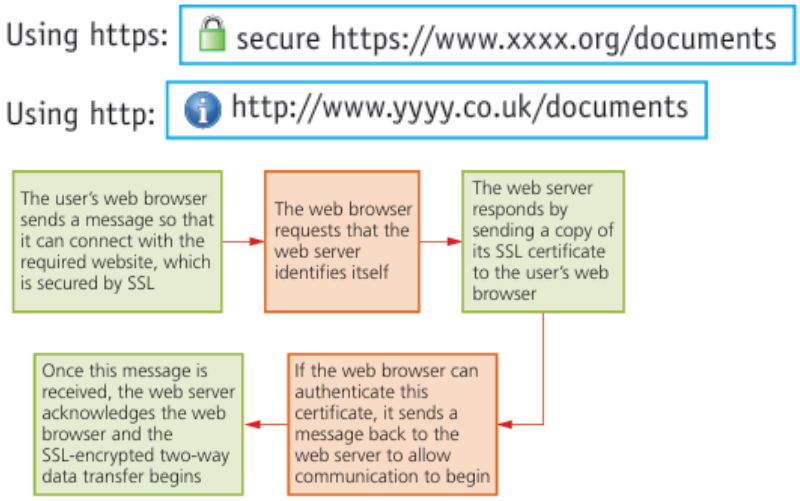
» A private key (known to the computer user only).


▲ **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.

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

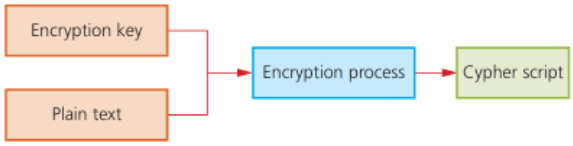



▲ **Figure 8.12** Communicating across a network using SSL

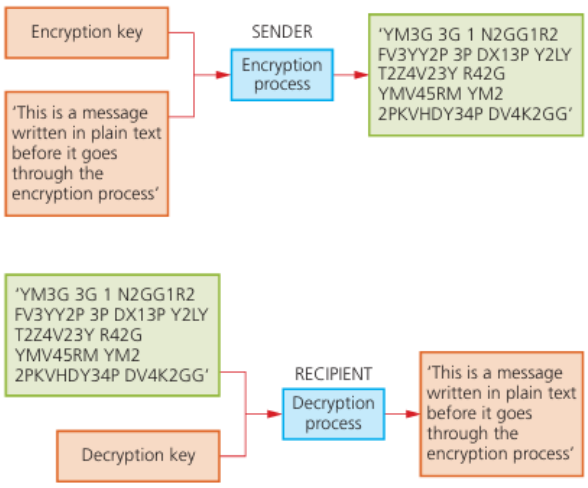
## Encryption

**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

▼ **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<br>» 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<br>» If a hacker acquires access to this server, they could then gain access to your stored or archived messages |

## 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.
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.

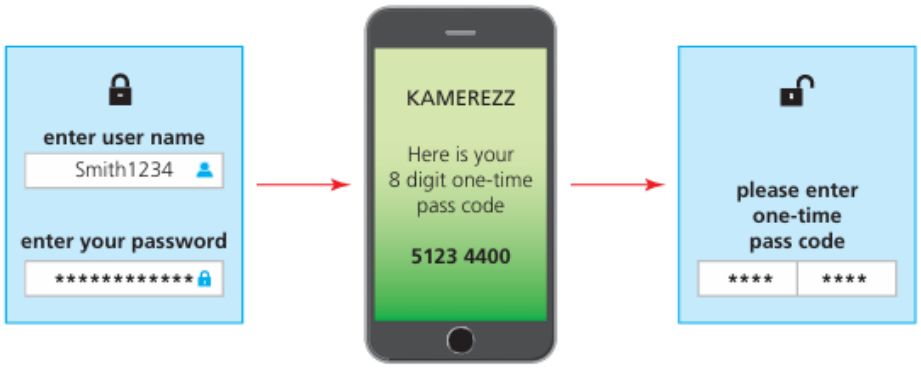

▲ **Figure 8.15** Firewall connection

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.




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

## 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,

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

# Revision questions

1. March/2023/Paper_0417/12/No.4(b)
(b) Social media can be used to communicate with friends.
Give four precautions that young people should take when using social media.

2. March/2023/Paper_0417/12/No.11(a, b, c)
A student has downloaded a file which contains a virus.
(a) Describe the possible effects on his computer system if he opens the file.

(b) Explain how the student could prevent the computer from being infected by viruses.
(c) Some files containing viruses have to be quarantined as they cannot be deleted.
(i) State the type of files that may have to be quarantined rather than deleted.
(ii) Explain how the software detects and quarantines the file.

3. June/2023/Paper_0417/11/No.5
State the safety issue that is most likely to occur for each of these causes.

(a) Spilling drinks on computer equipment
(b) Overloading sockets by plugging in too many devices
(c) Trailing cables across the floor
(d) Placing a laser printer at the edge of a table

4. June/2023/Paper_0417/12/No.5
State which health issue is most likely to occur from each description shown. Your answer must be different in each case.

(a) typing on a keyboard for long periods of time
(b) looking at a computer screen for a long time
(c) sitting with poor posture

5. June/2023/Paper_0417/12/No.6(a, b, c)
A company requires its employees to regularly change their login passwords for the company's computer systems. Passwords must be strong and cannot be reused.

(a) Explain three problems that may occur when the employees change their passwords regularly.

(b) The company has a website which uses a digital certificate.
Explain the purpose of the digital certificate.

(c) A digital certificate is attached to an email.
State three items contained in a digital certificate.

6. June/2023/Paper_0417/13/No.6
Two-factor authentication can use a number of different forms of identification.

(a) One form of identification is to use 'where the user is'.
An example of this would be the user's GPS location.
State two other forms of identification. Give an appropriate example of each.

(b) Explain the purpose of two-factor authentication.

8. Nov/2023/Paper_0417/13/No.4
A company's computer system is protected by both a user ID and a password.

(a) Explain how a user ID and a password are used to increase the security of data.
(b) The company plans to improve the security of its computer system by using biometric methods. Describe what is meant by biometric methods. Give two examples of biometrics. Description

9. March/2024/Paper_0417/12/No.8
solvedpapers.co.uk
A student has been the victim of a vishing scam.
(a) Explain what is meant by the term vishing.
(b) Describe two methods that help to prevent vishing.

10. March/2024/Paper_0417/12/No.16
(a) State four characteristics of spam emails.
(b) Give two ways of reducing spam emails.

11. March/2022/Paper_12/No.9(d)
(d) The office must be a safe working environment.
State two physical safety issues that might exist from the introduction of computers.

12. June/2022/Paper_11/No.12
Many company computer network systems use WiFi as a communication system to help prevent the issue of tripping over trailing cables.
(a) For each of the following physical safety issues describe two ways of helping to prevent them.
(i) Fire
(ii) Electrocution
(b) Describe three eSafety measures which should be taken when playing games on the internet.

13. June/2022/Paper_11/No.13
(a) Explain the need for copyright legislation when data is published on the internet.
(b) Describe methods that software producers use to prevent software copyright being broken.
(c) Emails are used by people to communicate with each other. Copyright and using acceptable language in the email are two of the constraints that affect the use of email.
(i) Describe four other constraints that may affect the use of email.

14. June/2022/Paper_12/No.7
A patient has an injury and the doctor treating him needs to find out information about the patient. Most of the data he needs to collect is personal data.
The data collected is protected by data protection legislation. Most data protection acts include the principle that data should be kept confidential and secure.
(a) List four other principles of a typical data protection act.

(b) Explain what is meant by personal data. Include two examples of personal data in your answer. Explanation
(c) Explain why personal data should be kept confidential and secure.

15. June/2022/Paper_12/No.14
Spam is associated with ICT systems.
(a) Explain what is meant by the term spam.
(b) Describe the ways that a user can recognise spam and methods to help prevent it.
solvedpapers.co.uk

16. June/2022/Paper_12/No.15
(a) Explain what is meant by cloud storage and how it is used.