ICT — CHAPTER 8

SAFETY AND SECURITY

Cambridge IGCSE ICT (0417) | Teaching Presentation

Instructor: Tr. Wai Lin Htet

Learning objectives

- Identify physical safety hazards and prevention
- Explain data protection and personal data
- Apply e-safety rules for internet, email and social media
- Describe security threats, malware and card fraud
- Explain data protection technologies and authentication

Chapter 8 — Visual mind map

8.1 PHYSICAL SAFETY

Electrocution • Fire • Trips • Falling equipment

8.2 E-SAFETY

Data protection • Personal data • Internet • Email • Social media • Gaming

8.3 DATA THREATS

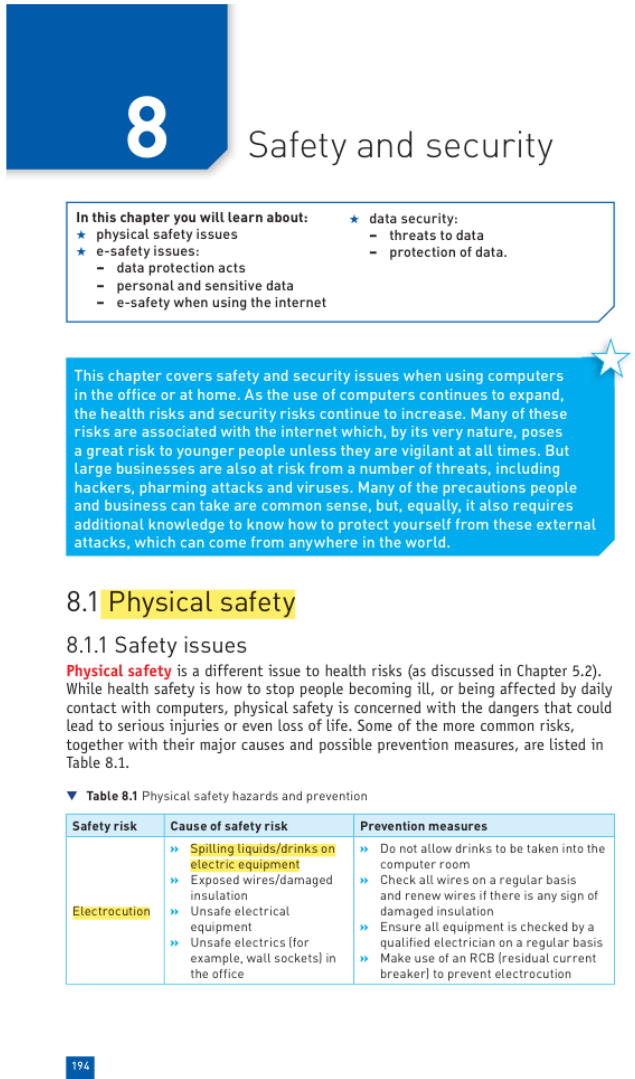
Hacking • Phishing • Pharming • Malware • Card fraud

8.3 PROTECTION

Biometrics • Certificates • SSL • Encryption • Firewalls • 2FA • Passwords

Physical safety vs health

- Physical safety: prevent accidents that cause injury
- Health risks: prevent harm from prolonged computer use
- Examples: electrical shock, fire, trailing cables, falling devices



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

194

Physical safety — hazard → prevention

ELECTROCUTION

Damaged wires / spilled drinks → inspect cables; keep liquids away; use RCB

FIRE

Overloaded sockets / blocked vents → reduce loads; improve ventilation

TRIPPING

Trailing cables → cable ducts; route wires away from walkways

INJURY

Unstable heavy equipment → strong desks; position away from edges

Physical safety — textbook reference

- Review Table 8.1 on textbook pages 194–195
- For each hazard, learn one cause and one matching prevention
- Exam technique: give a specific preventative action

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.



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

Data protection principles

- Data must be processed fairly and lawfully
- Use data only for stated purposes; collect no more than needed
- Keep data accurate and no longer than necessary
- Respect data subject rights and secure the information
- Follow rules for international transfers

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.



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

Personal data vs sensitive data

- Personal: name, address, email, date of birth, photographs, IP address
- Sensitive: medical history, biometric data, religion, political views, genetics
- Both need confidentiality; sensitive data needs extra protection

How to protect personal information

PHYSICAL

Lock filing cabinets; do not leave papers unattended

ACCOUNT

Log off; use strong credentials; restrict access

TRANSFER

Check recipients; encrypt sensitive information

RETENTION

Keep only necessary data; dispose securely

E-safety: using the internet

- Use trusted websites and check addresses carefully
- HTTPS encrypts the connection but does not guarantee a trustworthy seller
- Keep anti-malware software updated
- Avoid suspicious downloads and log out of sensitive accounts

E-safety: email

- Do not open unexpected attachments or suspicious links
- Check sender addresses for impersonation
- Avoid sharing identifying personal information
- Use Bcc to protect recipients in group emails

E-safety: social media

- Use privacy controls and limit personal information
- Do not reveal school, address or real-time location
- Block/report suspicious or abusive users
- Do not arrange to meet strangers alone

E-safety: online gaming

- Risks: cyberbullying, predators, voice disguise, phishing and malware
- Avoid using your real name and never reveal private details
- Report abusive behaviour and protect your account

Online safety — decision flow

RECEIVE

Unknown message, link or attachment

CHECK

Verify sender and URL independently

DECIDE

If suspicious: do not open or share data

REPORT

Block, report and seek trusted help

Data security threats — overview

- Hacking • Phishing • Smishing • Vishing
- Pharming • Viruses • Worms • Trojan horses
- Spyware / keyloggers • Adware • Ransomware
- Card fraud • Shoulder surfing • Card cloning

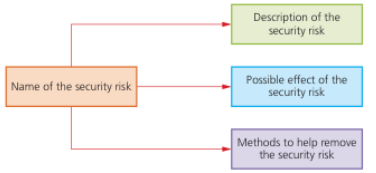
8.3 Security of data

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:

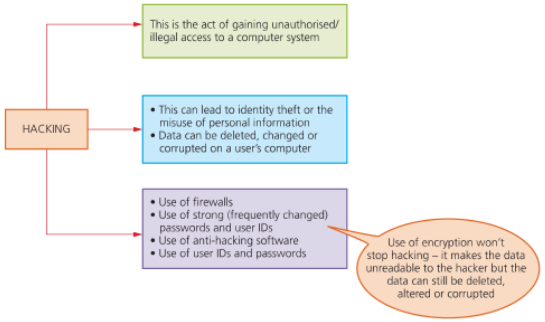
- hacking
- **phishing**
- vishing
- smishing
- **pharming**
- viruses
- malware
- card fraud.

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

200

Hacking

- Unauthorised access to a computer system
- Consequences: identity theft, altered or deleted data
- Protection: firewalls, authentication, updates, access controls

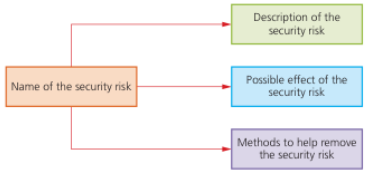
8.3 Security of data

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:

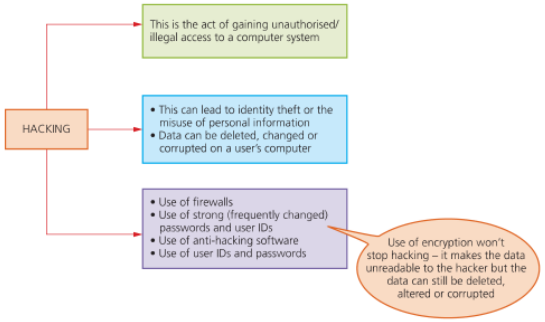
- hacking
- **phishing**
- vishing
- smishing
- **pharming**
- viruses
- malware
- card fraud.

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 vs smishing vs vishing

PHISHING

Fraudulent email asks user to reveal information

SMISHING

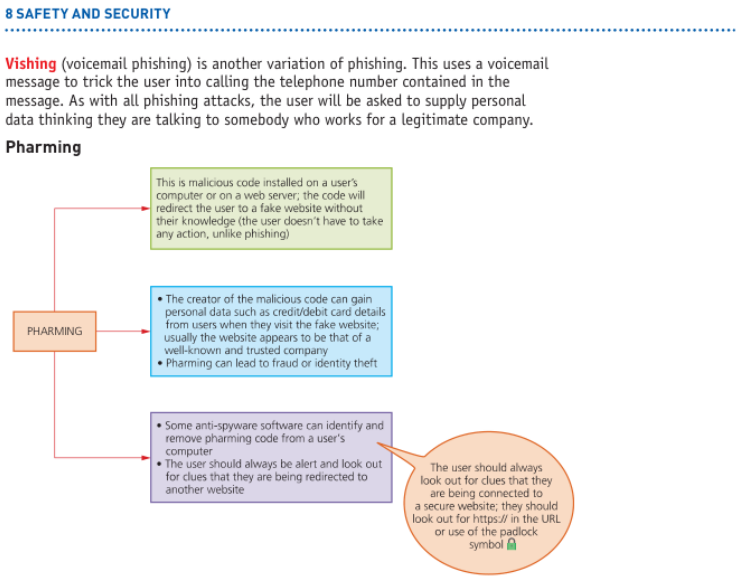
Fraudulent SMS / text message

VISHING

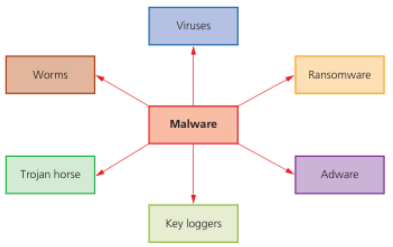
Fraudulent voice or phone message

Phishing — recognise the clues

- Urgent request to click a link or provide payment details
- Unexpected order cancellation or prize claim
- Mismatched sender domain or suspicious destination URL
- Verify using an independently opened official website



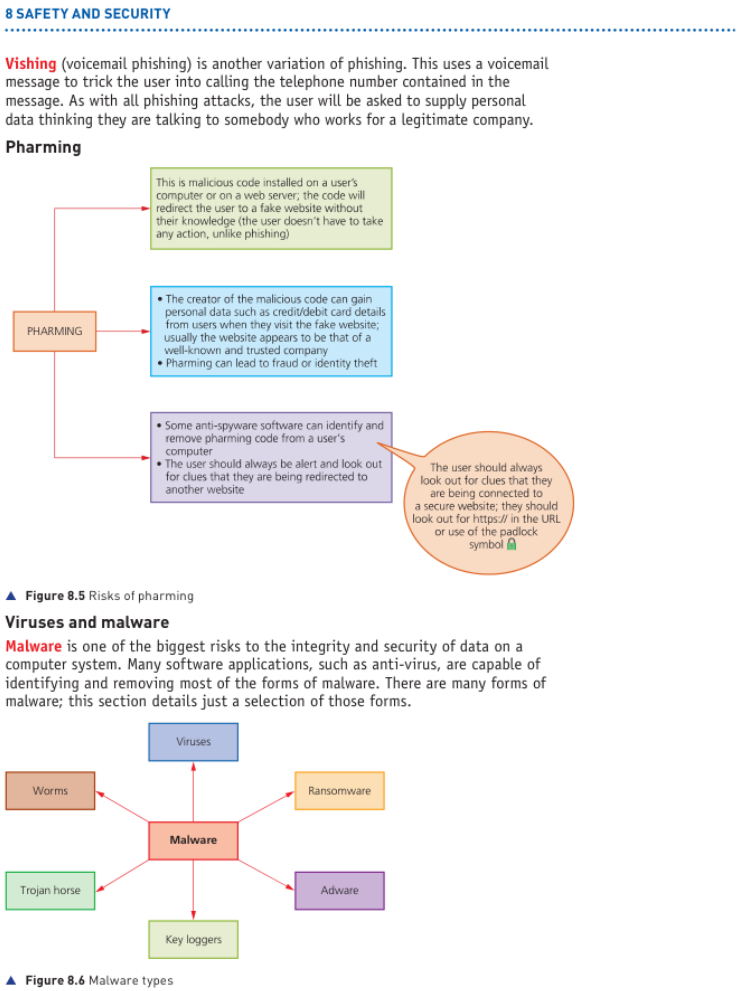
▲ **Figure 8.5** Risks of pharming



▲ **Figure 8.6** Malware types

Pharming

- Redirects a user towards a fake website
- May involve malicious changes to DNS or device settings
- Check unexpected redirects and verify the correct site
- Use updated security software and trusted networks



8 SAFETY AND SECURITY

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

202

Malware — visual mind map

VIRUS

Infects host programs/files

WORM

Self-spreads across networks

TROJAN

Disguised as legitimate software

SPYWARE

Secretly gathers information

ADWARE

Unwanted adverts and redirects

RANSOMWARE

Encrypts files and demands payment

Viruses and worms

- Virus: requires an infected host and execution trigger
- Worm: self-replicates and spreads across networks
- Both may damage systems and disrupt availability
- Keep software patched and antivirus updated

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

Trojan horses and keyloggers

- Trojan: malicious program disguised as legitimate software
- May install spyware or ransomware
- Keylogger records keystrokes such as passwords
- Avoid untrusted downloads and use anti-spyware protection

Adware and ransomware

- Adware floods users with adverts or redirects searches
- Ransomware encrypts data and demands payment

- Prevention: caution with downloads, updates, malware protection
- Maintain offline or otherwise isolated backups

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

Malware — textbook summary

- Study the six malware categories in Table 8.2
- Learn definition, typical effect and suitable prevention
- Practice comparing virus vs worm and Trojan vs ransomware

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 and shoulder surfing

- Shoulder surfing: observing a person entering PIN or card details
- Shield the keypad and stay aware of nearby observers
- Check transaction history for unusual activity

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**.

Card cloning

- Skimmers may copy magnetic stripe data
- Criminals may combine copied data with observed PINs
- Inspect suspicious terminals; use secure payment methods
- Monitor statements and report fraudulent transactions

Protecting data — mind map

AUTHENTICATION

User ID/password • Biometrics • Two-factor

ENCRYPTION

Plaintext → ciphertext → plaintext

NETWORK SECURITY

Firewalls • HTTPS / TLS

TRUST

Digital certificates and certificate authorities

Biometric authentication

- Fingerprint • Signature • Retina • Iris
- Face recognition • Voice recognition
- Advantages: convenient and difficult to share
- Limitations: cost, errors, privacy concerns

» 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.

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.



▲ **Figure 8.9** Fingerprint pattern

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.

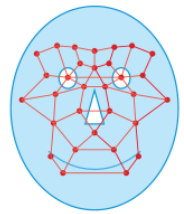
Figure 8.10 shows several of the positions used by the face-recognition software. The position of each facial feature is calculated by the software. These values are then compared to values already stored on a database. If the values match, then the face is recognised.

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.



▲ **Figure 8.10** Face recognition

Fingerprint and face recognition

- Fingerprint systems compare ridge patterns
- Face recognition compares distinctive facial measurements
- Both require stored reference data
- Changes or injuries may affect 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 » 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*

Biometrics — comparison

- Fingerprint: established and easy to use; damaged fingers cause errors
- Face: contactless; lighting and appearance may affect accuracy
- Voice: convenient; illness or recordings may cause problems
- Iris/retina: high accuracy but can be costly or intrusive

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:

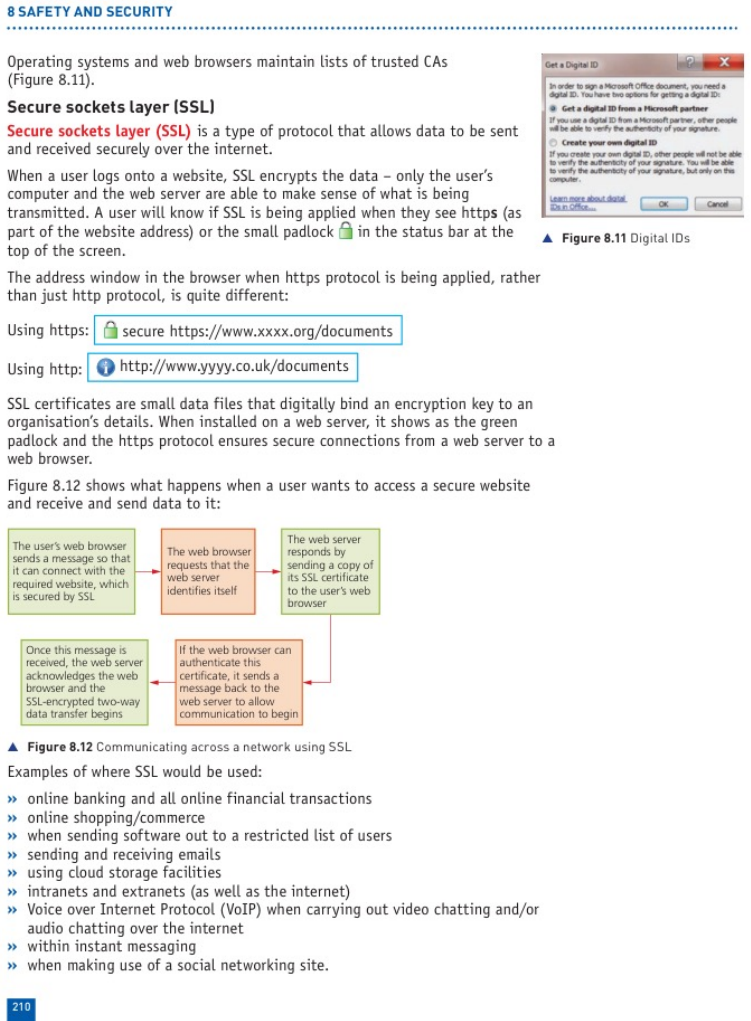
» the sender's email address
» the name of the digital certificate owner
» a serial number
» expiry date (the date range during which the certificate is valid)
» public key (which is used for encrypting the messages and for digital signatures)
» digital signature of certificate authority (CAs) – an example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

Digital certificates

- Help verify identity of a website or sender
- Contain identity information, public key and CA signature
- Certificates support secure communication and trust

SSL / HTTPS

- Textbook describes SSL for secure website connections
- Modern secure websites generally use TLS (successor to SSL)
- HTTPS encrypts data between browser and website
- Padlock indicates an encrypted connection, not guaranteed legitimacy



8 SAFETY AND SECURITY

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

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 https (as part of the website address) or the small padlock in the status bar at the top of the screen.

▲ **Figure 8.11** Digital IDs

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.

210

Encryption — visual process

PLAINTEXT

Readable message

ENCRYPT

Apply encryption algorithm and key

CIPHERTEXT

Unreadable without correct key

DECRYPT

Use the appropriate decryption key

Encryption in practice

- Protects confidentiality of stored or transmitted information
- If intercepted, encrypted data is not readable without the key
- Does not stop unauthorised access, deletion or corruption

Encryption

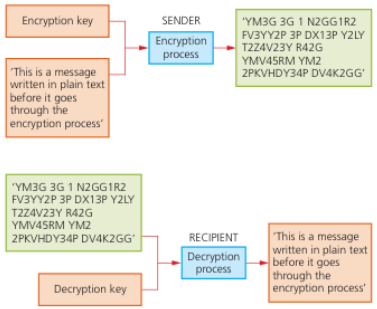
Encryption is used primarily to protect data in case it has been hacked or accessed illegally. While encryption will not prevent hacking, it makes the data meaningless unless the recipient has the necessary decryption tools (as described below).

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):

Firewalls

- Monitor network traffic according to security rules
- Can block unwanted connections and reduce exposure
- Not a substitute for updates or user awareness

Two-factor authentication (2FA)

- Requires two distinct verification factors
- Example: password plus authenticator app code
- Reduces risk from stolen passwords
- Never share one-time codes with unknown callers

Passwords and user IDs

- Use long, unique passwords and avoid predictable details
- Keep credentials private; use account lockout and 2FA
- Change a password if compromised
- A password manager can help manage unique passwords

Security controls — quick comparison

FIREWALL

Filters traffic

ANTIVIRUS

Detects malicious code

ENCRYPTION

Protects data confidentiality

2FA

Verifies login using another factor

BIOMETRICS

Uses a physical or behavioural characteristic

CERTIFICATE

Helps verify a trusted digital identity

Exam technique — how to earn marks

- Define the term accurately
- Explain a consequence or mechanism, not just name it
- Link prevention to the specific threat
- For comparisons, state clear differences
- Use scenario details in longer answers

Exam Practice 1 — Question

State two causes of electrocution in a computer room. (2)

Discuss first • Then reveal the model answer

Exam Practice 1 — Model Answer

State two causes of electrocution in a computer room. (2)

Spilled liquid on electrical equipment; damaged cable insulation. [1 mark each]

Suggested answer — not an official Cambridge mark scheme

Exam Practice 2 — Question

Explain two ways to reduce fire risk in a computer room. (4)

Discuss first • Then reveal the model answer

Exam Practice 2 — Model Answer

Explain two ways to reduce fire risk in a computer room. (4)

Avoid overloaded sockets to reduce overheating; keep vents clear so equipment can dissipate heat. [2 developed points]

Suggested answer — not an official Cambridge mark scheme

Exam Practice 3 — Question

Distinguish personal from sensitive personal data. (4)

Discuss first • Then reveal the model answer

Exam Practice 3 — Model Answer

Distinguish personal from sensitive personal data. (4)

Personal data identifies an individual (e.g., email); sensitive personal data includes especially private attributes (e.g., medical history) requiring additional care.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 4 — Question

Explain why Bcc is preferable to Cc for a group email. (2)

Discuss first • Then reveal the model answer

Exam Practice 4 — Model Answer

Explain why Bcc is preferable to Cc for a group email. (2)

Bcc conceals recipients' email addresses from other recipients, reducing unintended disclosure.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 5 — Question

Compare phishing and pharming. (4)

Discuss first • Then reveal the model answer

Exam Practice 5 — Model Answer

Compare phishing and pharming. (4)

Phishing tricks users via deceptive messages/links; pharming redirects users to a fraudulent website, sometimes without clicking a deceptive email link.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 6 — Question

Explain one difference between a virus and a worm. (2)

Discuss first • Then reveal the model answer

Exam Practice 6 — Model Answer

Explain one difference between a virus and a worm. (2)

A virus typically needs an infected host and execution; a worm can replicate and spread through networks without user execution of each copy.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 7 — Question

Describe how ransomware affects a business and one precaution. (4)

Discuss first • Then reveal the model answer

Exam Practice 7 — Model Answer

Describe how ransomware affects a business and one precaution. (4)

It encrypts or locks business files, disrupting operations; isolated backups enable recovery without relying on the attacker.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 8 — Question

Explain shoulder surfing and one prevention. (3)

Discuss first • Then reveal the model answer

Exam Practice 8 — Model Answer

Explain shoulder surfing and one prevention. (3)

A criminal observes a user entering confidential details such as a PIN; shield the keypad from view.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 9 — Question

Give two advantages and one disadvantage of fingerprint authentication. (3)

Discuss first • Then reveal the model answer

Exam Practice 9 — Model Answer

Give two advantages and one disadvantage of fingerprint authentication. (3)

Unique biometric; cannot be forgotten like a password; injury or dirty fingers may cause false rejection.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 10 — Question

Explain why encryption does not prevent hacking. (3)

Discuss first • Then reveal the model answer

Exam Practice 10 — Model Answer

Explain why encryption does not prevent hacking. (3)

Encryption makes captured data unreadable without a key, but does not itself stop an attacker gaining access or deleting files.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 11 — Question

Describe the purpose of a digital certificate. (3)

Discuss first • Then reveal the model answer

Exam Practice 11 — Model Answer

Describe the purpose of a digital certificate. (3)

A certificate associates an identity with a public key and is signed by a trusted authority, allowing software to verify identity.

Suggested answer — not an official Cambridge mark scheme

Exam Practice 12 — Question

Explain how two-factor authentication improves security. (3)

Discuss first • Then reveal the model answer

Exam Practice 12 — Model Answer

Explain how two-factor authentication improves security. (3)

It requires another independent factor beyond a password, so knowing a stolen password alone is insufficient to log in.

Suggested answer — not an official Cambridge mark scheme

Chapter 8 — final revision

- Physical safety: identify hazard, cause and prevention
- E-safety: protect personal information online
- Security threats: identify how attacks work
- Protection: choose an appropriate control and justify it
- Practice: explain, compare and apply to a scenario