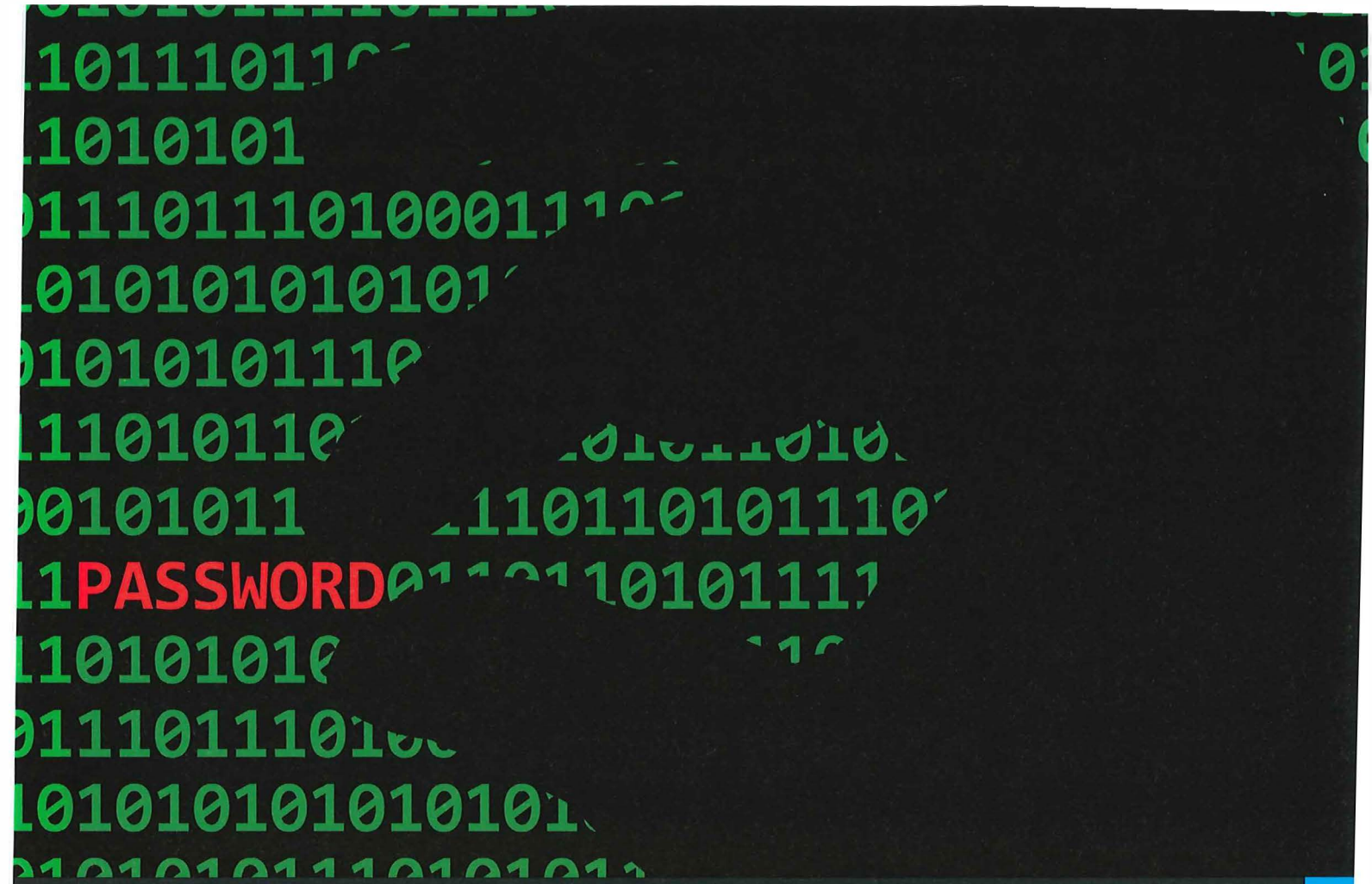


Chapter 9: Security

Learning objectives

By the end of this chapter you will:

- understand that data needs to be kept safe from accidental damage
- understand that data needs to be kept safe from malicious actions
- understand how to keep data safe when storing and transmitting, including use of passwords, firewalls, security protocols and symmetric encryption
- understand that online systems need to be kept safe from attacks.

9.01 Introduction

Computer systems are used to store and process data in many ways:

- Companies need to keep data about their customers' accounts.
- Doctors need to keep data about their patients.
- Research scientists need to keep data from experiments.
- Students need to keep data in the form of notes.
- Police need to keep data about their investigations and suspects.

Data has a value. The more accurate and complete the data, the more valuable it is. If data is lost, corrupted or accidentally changed, it loses value. For example, a doctor is less likely to be able to treat an illness correctly if the data held about the patient is not accurate or complete. Therefore it is extremely important to keep data accurate, complete and safe.

It is possible for data to be accidentally, or intentionally, changed or deleted. **Computer security** helps to keep data safe from loss, deletion, change and corruption. This helps maintain the value of the data.

KEY TERM

Computer security – the protection of computers from unauthorised access and the protection of data from loss.

Figure 9.01 Computer security

9.02 Security and prevention against accidental data loss or change

SYLLABUS CHECK

Understand the need to keep data safe from accidental damage, including corruption and human errors.

It does not matter how well a computer system is looked after, sometimes data can be damaged unintentionally. Data can be lost, deleted, changed or corrupted in a variety of ways:

- human error – for example, accidental deletion or overwriting of files
- theft – for example, having a laptop or smartphone stolen
- physical causes – for example, fire or water damage to equipment
- power failure – resulting in data in volatile memory (RAM) not being saved to permanent memory
- hardware failure – for example, a damaged hard disk drive
- misplacing portable media – for example, DVDs and memory sticks.

TEST YOURSELF

If a personal laptop was stolen, what personal or sensitive data might fall into someone else's hands?

Two methods of computer security can be implemented to help prevent unintentional loss of data:

- Backups of data help to retrieve data when it is lost.
- Verification helps to prevent data loss occurring.

Backups

Data can be accidentally lost. A laptop could be stolen or a computer hard disk drive could fail. Once data is lost we cannot get it back. A sensible safety measure is to make a copy of the data. A backup is a copy of data being used that we can keep in case of data loss. The data is copied onto a separate storage medium and this is kept separate from the main system. If we accidentally lose, corrupt or delete our data, the copy of the data can be transferred back to the computer system.

We can back up data onto various storage media:

- magnetic media – for example, external hard disk drives and magnetic tape
- optical media – for example, CDs, DVDs and Blu-ray disks
- cloud storage – for example, smartphone manufacturers provide online backup facilities so that phone data can be automatically backed up each day.

To learn more about backup storage media, see Chapter 8.

In order for a backup to be of any value we must update it regularly. How frequently a backup needs to be made depends on the situation:

- A bank might make backups several times each day because of the number of financial transactions taking place and the importance they have.
- A doctor's surgery may make a backup of patient records each evening.
- A school might make a backup of student and teacher records at the end of each week.
- A home user might make a backup occasionally.

Additionally, backups can be made automatically or manually. Most organisations employ automatic backups, where the computer system automatically makes a copy of the data. Home users frequently make manual backups, as and when they remember to, or feel the need to do so.

TEST YOURSELF

1 Find out what kind of backup storage media your school uses.

2 What would be the most suitable type of storage media for a hospital to use to back up their patient records? Justify your choice.

Verification

As we are human we can make mistakes. It can be quite easy for us to accidentally overwrite, change or delete a file. Although backups can help to retrieve lost data, it is also sensible to try and prevent data loss from occurring in the first place. To help guard against data loss many computer systems use a method known as verification.

Verification is a check that asks the user to confirm whether or not they wish to go ahead with an instruction. The confirmation usually takes the form of a question in a dialogue box, to which the user responds with a confirmation or cancellation. For example, computer systems usually ask for verification in the following situations:

- when attempting to save a file with a filename that already exists in that location
- when copying an older version of a file into a folder that contains a newer version of that document
- when deleting a record or amending data in a database.

Verification forces the user to stop and think about the action they intend to perform. However, verification is not foolproof. Users may still confirm an action, such as deleting a file, without realising the consequences until later.

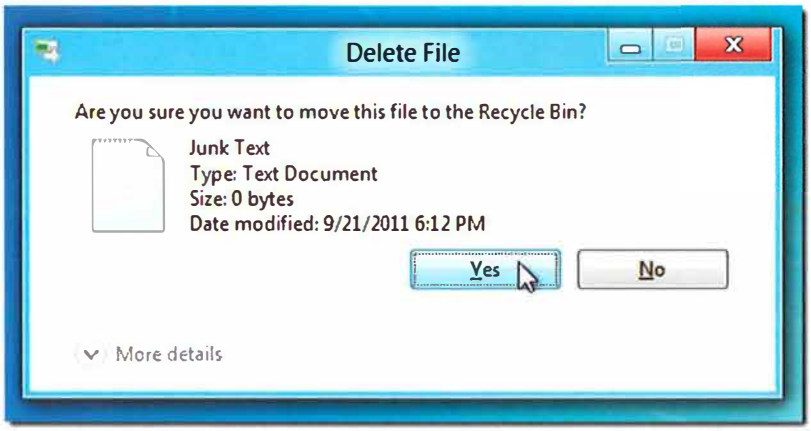


Figure 9.02 Verification message

9.03 Unauthorised access to computer systems and data

SYLLABUS CHECK

Understand the need to keep data safe from malicious actions, including unauthorised viewing, deleting, copying and corruption.

Understand the need to keep online systems safe from attacks including denial of service attacks, phishing and pharming.

As well as trying to avoid accidental loss of data, it also needs to be kept safe from unauthorised access. Data may be sensitive and private for example, patient data or a person's financial data. Preventing unauthorised users from accessing data is just as, if not more, important than protecting the data's value.

Data on a computer system can be accessed locally or online. With local access, the user has physical access to the computer system and its data. With online access, the user is able to access the computer system and its data via a network or the internet.

Unauthorised attempts at accessing data are known as 'attacks'. Attacks can come in several different ways:

- malware
- phishing
- pharming
- denial of service (DoS) attacks.

Malware

Some attacks come in the form of software called 'malware'. Malware is designed to disrupt or modify a computer system and its data. Malware is installed on a computer system without the user's knowledge. The software is accidentally downloaded from email attachments, USB RAM sticks and websites. Once installed, malware can cause considerable damage, or at the least, great inconvenience.

There are different types of malware:

- Viruses are self-replicating software that are designed to disrupt the normal operation of a computer. They can cause data loss by deleting and corrupting files.
- Worms are programs that do not delete or corrupt files. Instead they replicate themselves over and over, filling a computer's storage. This can cause a computer to run slowly or stop running altogether.
- Trojan horses are programs that disguise themselves as other programs. When run, they act like any other virus, deleting and corrupting files.
- Spyware are programs that collect personal and sensitive data, then send it to the spyware's authors.

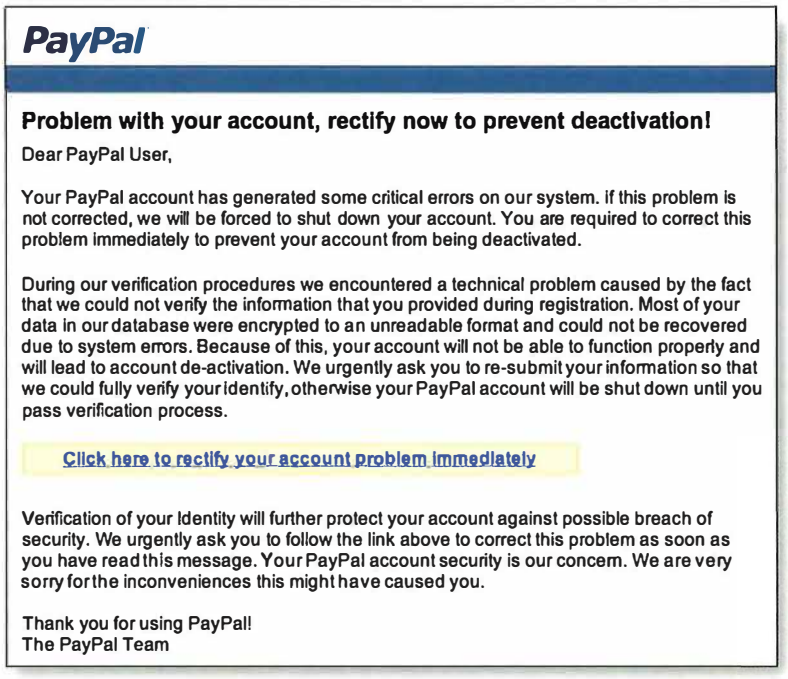
Figure 9.03 Internet risks

To learn more about malware see Chapter 2.

Phishing

One way of gaining access to data is simply to ask for it. This is the basis of phishing. Phishing was given its name because it is, like fishing, an attempt to gain something (in this case data) by using bait. A phishing attack usually comes in the form of an email. The email will look like it is from a person or organisation that is known to and trusted by the user. For example, many phishing emails look like they come from banks or online auction sites. The email often states that there is a problem with the user's online account and asks for confirmation of personal data to investigate the issue. It is designed to trick a user into giving data such as bank account details, or usernames and passwords to websites.

A phishing email normally looks like a genuine email, but usually asks the user to click on a hyperlink. The hyperlink transfers the user to a fake website that looks like the organisation's real website. The website then asks the user to enter their personal data. Once given, the data is used by criminals to steal money or buy items online.



PayPal

Problem with your account, rectify now to prevent deactivation!

Dear PayPal User,

Your PayPal account has generated some critical errors on our system. if this problem is not corrected, we will be forced to shut down your account. You are required to correct this problem immediately to prevent your account from being deactivated.

During our verification procedures we encountered a technical problem caused by the fact that we could not verify the information that you provided during registration. Most of your data in our database were encrypted to an unreadable format and could not be recovered due to system errors. Because of this, your account will not be able to function properly and will lead to account de-activation. We urgently ask you to re-submit your information so that we could fully verify your identify, otherwise your PayPal account will be shut down until you pass verification process.

Click here to rectify your account problem immediately

Verification of your Identity will further protect your account against possible breach of security. We urgently ask you to follow the link above to correct this problem as soon as you have read this message. Your PayPal account security is our concern. We are very sorry for the inconveniences this might have caused you.

Thank you for using PayPal!
The PayPal Team

Figure 9.04 Phishing email

Pharming

Phishing uses emails to help capture data by tricking a user into visiting a fake website. Pharming also attempts to trick the user into giving their personal data by using fake websites. When a user tries to visit a genuine website, they are instead re-directed to a fake website that looks very much like the real site. Once the user enters their personal data, such as their user ID and password, the data is passed to criminals.

Pharming can happen because of the way the internet works. Each website has a domain name that is translated into an IP address. The user's browser is directed to the IP address, giving access to the website. With pharming, malware installed on the user's computer looks for domain names of reputable sites and translates them into different IP addresses, those of fake websites. Instead of visiting a genuine website, the user is directed to the fake website instead.

To learn more about IP addresses and how the internet works, see Chapter 2.

Denial of Service (DoS) attacks

Denial of Service (DoS) attacks take their name from their purpose: to deny a service. DoS attacks are not designed to gain access to data. Instead they prevent access to data.

Websites and networks are accessed through **servers**. When a user's computer wants to access data on a server, it sends a transmission known as a **request**. The server acknowledges the request and sends the requested data to the user.

KEY TERM

Server – a computer which handles requests from other computers.

Request – a communication which asks for data to be transferred.

There are only so many requests that a server handle at any one time. The more powerful the server, the more requests it can handle. When a large number of requests are received, each request is placed into a queue and dealt with in turn. A DoS attack attempts to prevent access to a server by sending it more requests than it can handle. The request queue becomes so large that the server cannot respond to all requests within a reasonable time, preventing it from providing a service.

DoS attacks are usually attacks that come from one computer. Another form of DoS attack is where two or more computers attack a server at the same time. This is known as a Distributed Denial of Service (DDoS) attack because the requests are distributed among a number of computers. Usually, the attacking computers are infected with malware that instructs the computer to continually send requests to a server.

TEST YOURSELF

Hundreds of DoS attacks occur every day. Use the Internet to find out about two high-profile organisations whose websites have been subject to DoS attacks and research why they were targeted.

9.04 Security and protection against attacks

SYLLABUS CHECK

Understand how data are kept safe when stored and transmitted, including:

- use of passwords, both entered at a keyboard and biometric
- use of firewalls, both software and hardware, including proxy servers
- use of security protocols such as Secure Socket Layer (SSL) and Transport Layer Security (TLS)
- use of symmetric encryption (plain text, cypher text and the use of a key) showing understanding that increasing the length of a key increases the strength of the encryption.

Be able to describe how the knowledge discussed in this chapter can be applied to real-life scenarios including, for example, online banking and shopping.

There are several ways in which computer security can be implemented to keep data safe from unauthorised access, alteration and deletion:

- physical security
- authentication
- anti-virus software
- firewalls.
- proxy servers
- protocols
- encryption

Each method helps to prevent different forms of unauthorised access to data.

Physical security

KEY TERM

Physical security – security which prevents physical access to a computer.

Our data is often of a sensitive or private nature. We need to keep our data safe from users who do not have the authority, or permission, to access it.

Physical security prevents local access to the system and data. This security can be implemented in several ways:

- Locks – The computer system and data can be kept in a locked room. Organisations that hold sensitive and private data keep their computer systems, data and backups locked away. This way only authorised users can have physical access.
- CCTV – Cameras can be used to monitor who physically accesses a system. CCTV can help deter users who have no authority as they know they will be seen accessing the data.
- Security guards – Where data is especially sensitive, security guards are often employed as an extra level of security to help deter those users who do not have permission to access a computer system.

Physical security methods are simple to implement and can be quite effective. However, all they do is prevent or deter a user from accessing data without permission. Physical methods cannot help recover data that has been lost.

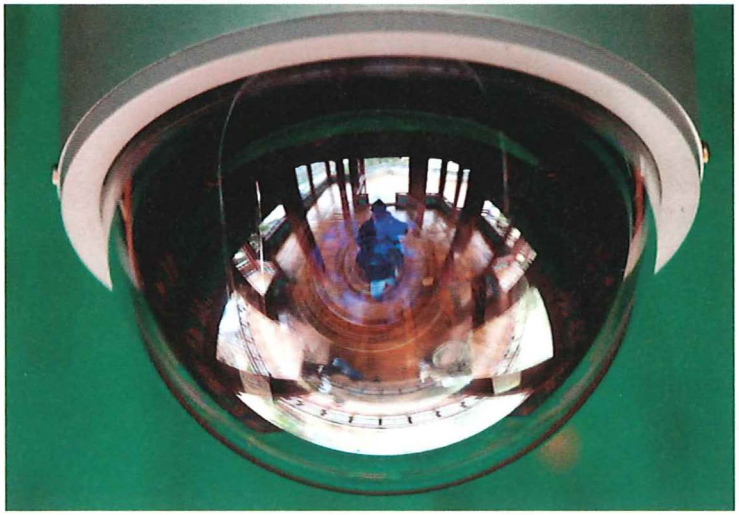


Figure 9.05 CCTV can be used to deter an unauthorised user from attempting to access a system

Authentication

A user can gain access a computer system and its data either locally or remotely. Physical security attempts to prevent physical access, but once physical access is gained another form of prevention is necessary. **Authentication** is designed to stop a user from being able to access the system once they have physically got to it. Additionally, it guards against an unauthorised user attempting to gain access remotely, for example over the internet.

KEY TERM

Authentication – security which prevents access to a computer even if the user has physical access.

In modern computer systems the most common form of authentication used is the combination of user identification (user ID) and password protection. A user ID is the name a user uses to identify themselves to a computer system. User IDs often take the form of the user's name. A password is a secret word or series of characters, known only by the user, that pairs with the user ID. Only the correct combination of user ID and password allows access to the system. For example, John Smith may use the string 'computingisfun' as the password for the user ID 'johnsmith'. Table 9.01 shows what happens when he enters certain values.

Table 9.01

User ID	Password	Result
John_smith	computing	Incorrect match. Access denied
johnsmith	computingisfun	Correct match. Access granted

A user ID and password can be a fairly secure method of preventing unauthorised access to a computer system and its data. However, some users can make it quite easy for someone else to guess their password by choosing a password that is data associated with them, such as:

- their date of birth
- the name of a daughter, son, brother, sister or other family member
- the name of their pet
- their initials
- a favourite item, hobby or place.

A password of this nature is often referred to as a 'weak' password. This is because it can be easily determined. A strong password is one that is very difficult for someone else to guess. A password is considered to be strong if it:

- is at least eight characters in length
- does not contain your user ID, real name, or organisation name
- does not contain a complete word
- is significantly different from previous passwords
- uses a mixture of characters from the keyboard, including upper and lower case letters, numbers and symbols.

Nancy Bauer enjoys computing. She has a pet called Felix. Her user ID is nancybauer. Passwords she might choose could include:

Table 9.02

User ID	Password	Strength
nancybauer	nancy	Weak – too few characters and features her name
nancybauer	felix	Weak – too few characters and is the name of her pet
nancybauer	F3l1x	Medium – too short, but uses a combination of letters and numbers
nancybauer	$0cC3ri5fuN	Strong – more than 8 characters, more than one word, a mixture of uppercase and lowercase letters, numbers and symbols

TEST YOURSELF

1 Think of a password you use regularly. How strong is it? How could you make it stronger?
2 Why is it important to have both physical security and authentication when creating a secure system?

Another problem that can occur is that users often use the same passwords for different systems. It is sensible for us to use different passwords for each system we have access to.

Passwords were first used with computers in the 1960s. Since then they have become the most commonly used form of authentication. Amongst other things, passwords are now used to:

- log on to a PC or network
- confirm banking transactions
- gain access to a wireless network
- log onto online services
- access emails.

Passwords are widely used but they can be easy to guess. As a result, security experts have looked for alternative methods of preventing unauthorised access to systems and data.

Biometrics

Humans have individual physical characteristics: fingerprints, voice patterns, face shapes and iris patterns.

As physical characteristics are unique, they provide a unique way to identify a user to a computer system. The use of physical characteristics as a means of identification is known as 'biometrics'. Several biometric systems have been introduced as alternative means of authentication. Unlike passwords that are typed in using a keyboard, biometrics use scanners or sensors to record input.

Fingerprint scanners require a user to place their finger against a scanner and an image of their fingerprint is taken. The computer compares the series of ridges and bumps recorded in the image with a fingerprint image previously taken. The user is only granted access if they match. Fingerprint scanners are fairly cheap to implement and are regarded as a reasonably reliable means of authentication. However, fingerprint authentication is unsuitable for children as a child's fingerprint pattern alters as they grow.

Figure 9.06 A finger print scanner

Voice recognition software requires the user to speak a phrase known to the computer into a microphone. Access is only granted to the system if the phrase and voice pattern match

those stored by the computer. Voice recognition is a fairly reliable technology but it suffers in noisy environments where the computer can have difficulty in hearing the voice amongst the background noise. The recognition may also fail if the user has a cold or a sore throat, as it may alter their voice.

Facial recognition uses a camera to take an image of the user's face. The computer notes the size and shape of facial features, such as eyes, nose and cheekbones, and the distances between them. Access is only granted to the system if the pattern matches that stored by the system for the user. Facial recognition is reasonably reliable, but can fail if poor lighting causes facial features to be incorrectly measured. Additionally, changes in hairstyle, or wearing glasses, can affect reliability.

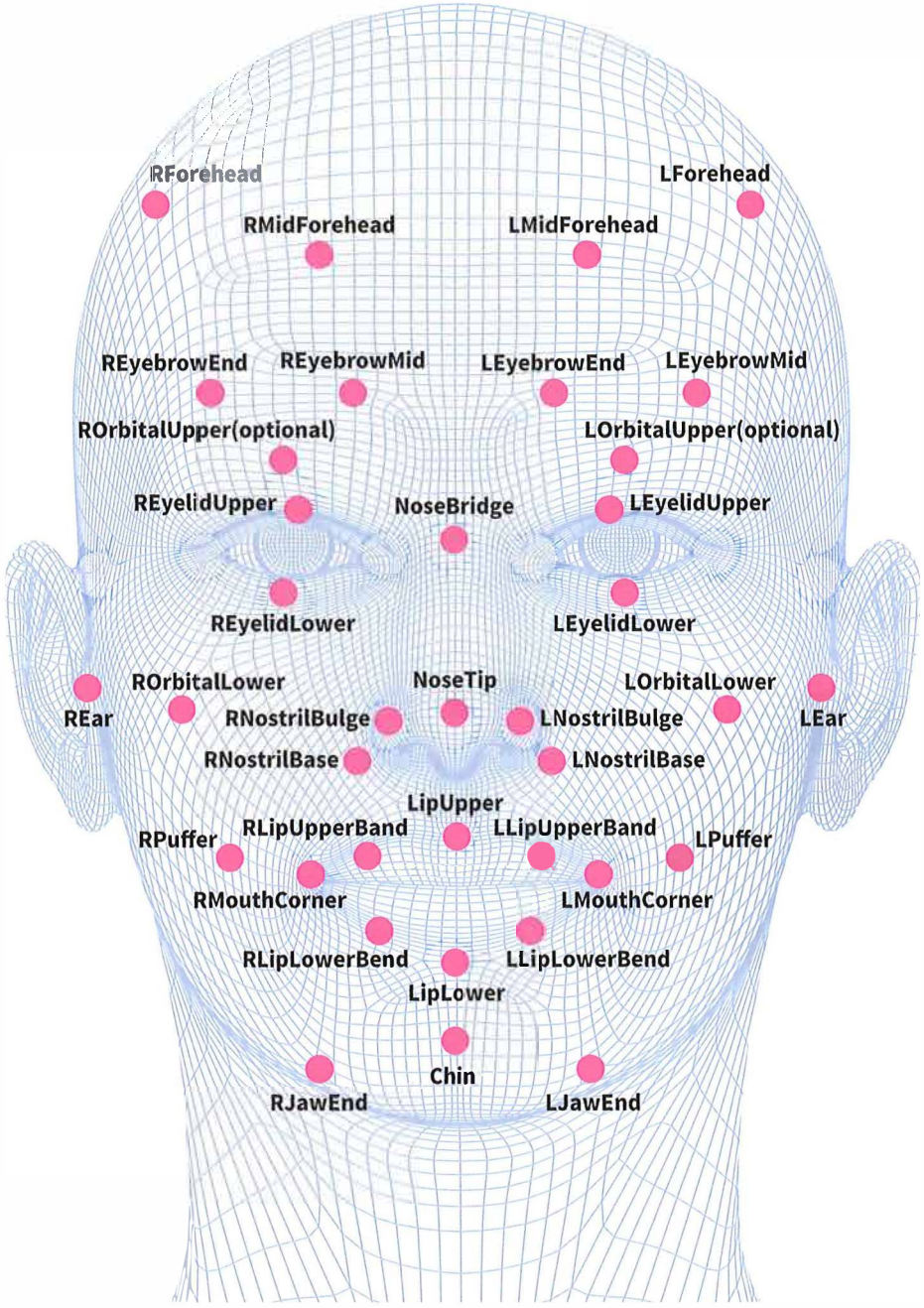


Figure 9.07 Facial recognition software measures many different facial features

Iris scanners require the user to place their eye to a scanner. This records a high resolution and detailed image of their iris pattern. Access is only granted if the image pattern matches that stored by the system. Iris recognition is highly reliable but expensive to implement. Some users can find having their eye scanned an uncomfortable experience.

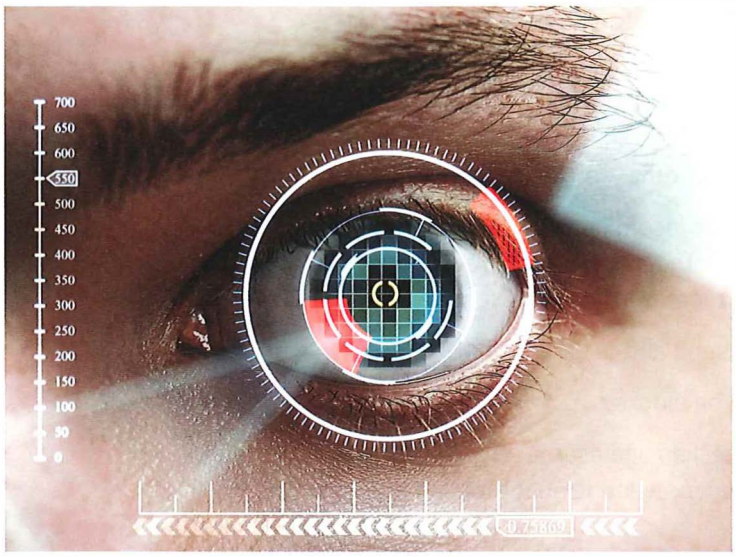


Figure 9.08 An iris being scanned

Biometric technology is improving but it is still regarded as far from perfect. As a result, many systems include an alternative method of authentication for situations where biometric authentication fails.

TEST YOURSELF

Think of potential problems that a disabled user might face when using biometric authentication?

Anti-virus software

It can be extremely difficult to detect and remove malware once it is installed on a computer. Special software known as **anti-virus software** is needed to find and delete malware.

KEY TERM

Anti-virus software – software which finds and remove viruses from a computer by scanning it.

Anti-virus software uses a list of known malware ('virus definitions') and how they work. The software scans the computer and looks for any malware that it can recognise. If it finds any malware, the anti-virus software attempts to remove it or block its access to the computer.

Anti-virus software can only detect infection from known viruses. New viruses are released all the time. In order to remain effective, anti-virus software needs to have up-to-date virus definitions.

To learn more about anti-virus software see Chapter 2.

Firewalls

Computers communicate and transfer data by sending messages. Messages that are sent and received by computers are known as 'traffic'. Although most of the traffic is of a genuine nature, such as the downloading of an email, other traffic is unauthorised. For example:

- spyware may transmit the personal data it has gathered back to its creator
- DoS malware may continually send requests to a server
- malware may attempt to download other malware
- email viruses might attempt to send spam to other computers.

A firewall is a security technology that monitors incoming and outgoing traffic. It provides a protective barrier between the computer and other computers. Firewalls work through the use of rules. Different rules exist for different types of traffic, for example:

- only certain programs can be allowed to send and receive traffic
- access to certain websites or servers can be blocked.

The traffic is examined by the firewall and checked against the set rules. If it meets the rules the traffic is forwarded, otherwise it is blocked, preventing unauthorised access to and from the computer.

Two types of firewall exist, hardware firewalls and software firewalls. Hardware firewalls protect a network, whereas a software firewall protects an individual computer. Many routers contain hardware firewalls that monitor traffic between a network and the internet. Software firewalls have to be installed on each computer on a network.

Firewalls are very effective at blocking unauthorised access. However, because users can modify the rules, unauthorised traffic may still occur.

Proxy servers

One way to protect a server from attacks is to prevent direct access to the server itself. This is done by directing traffic to an intermediary server. This is known as a proxy server. The proxy server sits between the main server and the internet.

The purpose of the proxy server is to direct traffic away from the network server. When a request comes in from the internet, the proxy server examines the request. If the request is thought to be valid, the corresponding data is retrieved from the network server and transmitted to the requesting computer. As a result, any attack hits only the proxy server, not the network server itself.

Proxy servers can also contain copies of data. This brings several benefits:

- If the data on a proxy server is lost, corrupted or changed (accidentally or maliciously) the original data is still safe and secure on the network server.
- A proxy server may hold certain data, but not other, more sensitive data. An external computer can only access the data on the proxy server, not the sensitive data held on the network server.
- As a proxy server can handle requests and transfer data, the network server is free to handle requests from computers on its own network, speeding up internal access times.
- A proxy server can hold copies of frequently visited webpages. This speeds up access to those pages from computers on the network as the pages do not have to be downloaded from the internet.

- A proxy server can be used to prevent users on a network from accessing external websites. Many schools use this system to prevent students from accessing unsuitable material.
- An organisation that receives large amounts of requests can use several proxy servers to help spread the load. Popular websites use this method to speed up response times.

Encryption

It does not matter how much protection a computer system has, the data it contains may still end up in the hands of an unauthorised user. Another method to protect the data is to convert it into a form that cannot be understood by anyone other than an authorised user. This process is called **encryption**. Encryption does not prevent data from being accessed. It prevents the data being understood by unauthorised user if it is accessed.

KEY TERM

Encryption – a way of modifying data to make it difficult to understand if intercepted.

Key – information that describes how a message is encrypted or decrypted.

Encryption works by using a **key**. A key is a particular piece of information that is required to disguise (encrypt) and reveal (decrypt) the data.

One of the earliest known methods of encryption is the Caesar cipher, named after Julius Caesar who is said to have used it to disguise private messages. The Caesar cipher works by taking each letter in the alphabet and replacing it with another letter several positions up or down the alphabet. The number of positions is called the offset. In this encryption method, the offset is the key.

For example, a cipher with an offset of 4 would replace each letter with that four places above in the alphabet. 'A' would become 'E', 'B' would become 'F' and so on as shown in Table 9.03.

Table 9.03

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Offset = 4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

To encrypt a message, each letter in the message is replaced with its offset equivalent. For example:

I LOVE COMPUTER SCIENCE

becomes

M PSZI GSQTYXIV WGMIRGI

To decrypt a message, the process is reversed.

This cipher is extremely simple to break, as there are only 25 possible keys that can be used. Modern encryptions use extremely complex algorithms and keys to encrypt data.

There are various encryption algorithms available and all of them use keys. An encrypted message can be decrypted by anyone who knows the encryption method and the encryption key. To make it more difficult for an unauthorised user to decrypt a message, a long key must be used.

Keys are created from numbers generated using binary digits. The number of binary digits used is known as the key length. The longer the key length, the more possible combinations there are to generate numbers.

Table 9.04

Size of key in bits	Number of possible combinations
1	2
2	4
8	256
16	65536
32	4 294 967 296
128	More than 300 000 000 000 000 000 000 000 000 000 000 000

Computers are used to generate keys, they can also be used to try and determine what key has been used. They do this by generating every possible number combination in a key length and trying it to decrypt the message. This is known as a brute force attack. Modern encryption methods use 128-bit keys. This gives a range of combinations so big that even supercomputers cannot generate every possible combination.

Encryption can be symmetric or asymmetric. In symmetric encryption (such as the Caesar cipher), the same key is used to encrypt and decrypt the message. This means that two people with the key can share messages. The problem with this method is that anyone who obtains the key can encrypt or decrypt a message. Messages sent over networks, or over the internet, can be intercepted. Therefore if the key is known by unauthorised users the encryption is useless.

This fault can be overcome by using asymmetric encryption. Asymmetric encryption uses two keys that work as a pair. The first key is used to encrypt the message. A message encrypted with the first key cannot be decrypted with that same key. It can only be decrypted with the second key. Similarly, a message encrypted with the second key can only be decrypted with the first key.

The first key can be sent to anyone from whom the user wants to receive an encrypted message. As a result, this key is called a 'public key'. The second key is kept secret by the user, so that only they know it. As a result, this key is called a 'private key'. As long as the private key is kept secret, the encryption is extremely difficult to break.

Asymmetric encryption is widely used by organisations who need to send confidential data, for example banks and online shops. When a user logs onto a bank's website, a copy of the bank's public key is downloaded to the user's browser. Any communications sent from the bank to the user are encrypted with the private key. The user's browser decrypts the message using the public key. Similarly, any messages sent from the user's browser are encrypted with the public key. Only the bank, which holds the private key, can decrypt them.

A further advantage of asymmetric encryption is that the source of the message can be trusted. For example, a user connected to an online bank can trust the messages they receive, because only the bank has the key to encrypt the messages.

9.05 Protocols

Different computers communicate in different ways. They are similar to people, who speak different languages. Before computers can communicate with each other they need to agree on how to communicate. They do this by determining and agreeing a set of rules, known as 'protocols'.

Various protocols exist and each one is specific to a purpose:

- Hyper Text Transfer Protocol (HTTP) governs communications across the internet.
- Hyper Text Transfer Protocol Secure (HTTPS) is a more secure version of HTTP, often used to handle financial transactions.
- File Transfer Protocol (FTP) governs the transfer of files across the internet.
- Simple Mail Transfer Protocol (SMTP) handles email communication.
- Transfer Control Protocol/Internet Protocol (TCP/IP) handles communications on a network.
- Voice Over Internet Protocol (VoIP) handles audio/visual communication.

To learn more about protocols, see Chapter 2.

KEY TERM

Secure Socket Layer (SSL) – a protocol which allows secure links between computers.

Transport Layer Security (TLS) – a recent, more secure version of SSL.

HTTPS makes use of another protocol known as **Secure Socket Layer (SSL)**. SSL makes it possible for the internet to be used safely for online transactions and for sensitive data to be safely transmitted. It uses asymmetric encryption to create a secure link between one computer and another. For example, a web server uses SSL to create a link between itself and another computer's web browser. A user can then transfer securely data such as a credit card number or bank account details.

SSL is used to secure:

- online credit card transactions
- any sensitive information exchanged online
- the transfer of files over HTTPS and FTP services such as those sent by website owners updating new pages on their websites
- web-based email
- the connection between an email client and email servers
- cloud-based storage systems
- intranets and extranets
- virtual private networks.

Transport Layer Security (TLS) is a more recent version of SSL. TLS works the same way as SSL, but is more secure as many security issues that arose with SSL were fixed with the development of TLS.

Summary

- Data is valuable. It loses its value if it is lost, accidentally changed or corrupted.
- Computer security is the protection of computer systems and their data.
- Data can be lost accidentally through human error, theft, damage to equipment, power failure, hardware failure or misplacing portable media.
- Backups and verification help protect against accidental data loss. A backup is a copy of data, kept away from the computer system.
- Verification is a check which asks the user to confirm whether or not they wish to go ahead with an action.
- An unauthorised attempt to access a computer is known as an attack. As well as physical attacks (where the user has physical access to the computer), attacks can be made through the use of malware, phishing, pharming and Denial of Service (DoS).
- Malware is software that is designed to affect the normal operation of a computer. Malware comes in the form of viruses, worms, Trojan horses and spyware. Each form of malware can cause data loss or provide unauthorised access to data.
- Phishing is a technique which uses email to trick a user into giving away personal data.
- Pharming directs the user to a fake websites where they may inadvertently give away personal data
- Denial of service attacks attempt to prevent access to data. A computer is used to overload a server with requests.
- Encryption is a technique that disguises the contents of a message using a key.
- Protocols are sets of rules that handle communication between computers.
- Secure Socket Layer (SSL) is a protocol that creates a secure, encrypted link between one computer and another. TLS is an updated, more secure version of SSL.

Exam-style questions

1 What is meant by data losing its value? (2 marks)

2 Explain what is meant by an automatic backup. (2 marks)

3 Explain how phishing and pharming trick a user into giving up personal data. (4 marks)

4 Explain how anti-virus software may help to prevent distributed denial of service attacks. (2 marks)

5 Explain why computer security is more effective when anti-virus software and firewalls are used. (4 marks)

6 Describe how a proxy server can help keep data safe. (2 marks)

7 Explain the difference between symmetric and asymmetric encryption. (4 marks)

8 Describe what a protocol is and how protocols help protect data. (2 marks)