

# Chapter 5: System Security

In this chapter you will learn:

- ✧ about a range of attacks or threats a network can be subjected to
- ✧ how we can identify the attacks and threats a network can be subjected to
- ✧ how we can prevent against the attacks and threats a network can be subjected to

## What forms of attack and threats can a network be subjected to?

**OCR specification point:**

- ☑ forms of attack
- ☑ threats posed to networks:
  - malware
  - phishing
  - social engineering
  - brute-force attacks
  - denial-of-service (DoS) attacks
  - data interception and theft
  - the concept of SQL injection
  - poor network policy

Networks provide many benefits, but they also come with a great number of risks. Many people recognise the security precautions they need to take with their physical belongings, but they do not exercise as much care with their security when it comes to using networks.

A network can come under attack in many different forms, and criminals are always inventing new methods of attack to overcome the increased security that is developed to prevent the attacks.

There are five main forms of attack a network can be subjected to:

Form of attack	Description
Active	This is when a network is attacked with a planned attack, such as trying to hack a network. <b>Prevention:</b> Use of a firewall
Passive	This is when data that is being transmitted around a network is monitored. The network traffic is monitored to find any personal or sensitive data that can be intercepted. <b>Prevention:</b> Use of data encryption
Distribution	This is when a person knows of a 'back-door' access into a network from manufacture. They use the back door to access the network and exploit it. <b>Prevention:</b> Use trusted software from reputable manufacturers
Insider	This is when someone that works for an organisation abuses their access to a network in order to steal personal or sensitive information. <b>Prevention:</b> Layers of security in place for confidential information
Close-in	This is when an attacker is very close to the device or system they are trying to attack. <b>Prevention:</b> Difficult to prevent; any sensitive systems should be away from access when not being used

**Discussion point:** Can you think of any other ways someone might attack a computer?

We need to realise the value of our personal data and sensitive information and put in place as many security measures as we are able to, in order to prevent it being stolen. Complete prevention is extremely difficult, as threats posed to a network are always developing and it is a constant battle to keep up the security to defend against this. Cyber-criminals see the value in your personal data – they spend much of their time devising ways to steal it – but do you really see its value?

**Discussion point:** Why might a cyber-criminal want to steal your personal information?

We have considered the approaches to attack of a network, but there are also many types of threat that can be posed to a network.

## Malware

**Malware** is short for malicious software, and this is what it is, software designed to cause malice to a person's computer system. It is designed to disrupt or damage the computer system and the data that it holds. Malware is an all-encompassing term for a number of threats; including:



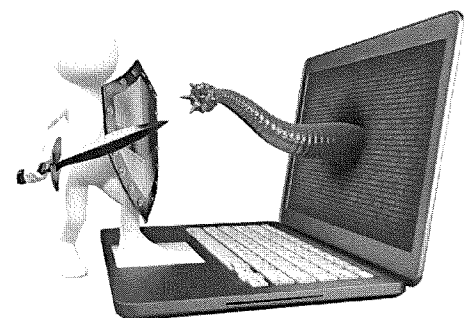
We all need to realise the value of personal and sensitive data and protect it

**Malware** – software that is designed to disrupt or harm a user's computer

Malware	Description
Virus	This is a computer program that infiltrates a computer system and replicates itself. It is intended to cause damage to a computer system by corrupting data or using up all the available memory, causing it to crash.
Trojan horse	This is a type of malware that is disguised as a harmless file or download. When the seemingly harmless file is downloaded, the malware is downloaded with it. Once the malware is downloaded, it can carry out the attack it was designed to perform.
Worm	This is a computer program that finds holes in a computer network and uses these to replicate itself. In doing this it will clog up bandwidth and slow a network down.
Spyware	These are computer programs that gather data about people without their knowledge. A common form of spyware is a key logger. This records the key presser from a user on a computer. When the records are studied, it can be possible to pick out personal and sensitive data, such as passwords.

We must be very careful when we choose to download a file from an email or a website. Most malware is disguised as a Trojan horse. It will look like an innocent application, file or game, but it could unleash a great deal of harm to your computer and files. If we are not certain that the download is from a reputable source, we should question whether it is safe to be downloading the file at all.

In addition to malware, there are other threats that are posed to a network. Some of these threats do not necessarily hide themselves in downloads, but rather coerce people into providing their information, believing they are giving it to a legitimate source for a legitimate reason. These types of threat include phishing and social engineering.

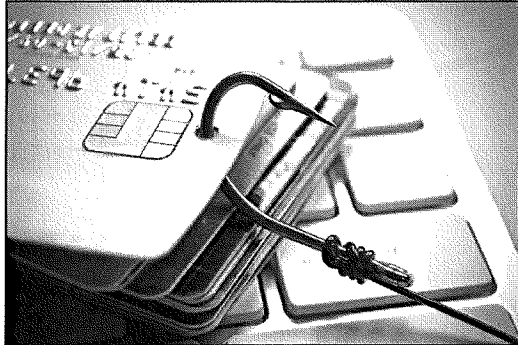


Malware is software that is designed to corrupt our computer system and network

## Phishing

**Phishing** is when an unauthorised person tries to collect personal and sensitive data by disguising themselves as a reputable individual or organisation. The kind of data they are looking to obtain are passwords and bank details. The perpetrator will send some kind of communication, such as an email, to their victim.

**Phishing** – sending emails pretending to be a reputable company to try to gain people's personal details



Criminals use phishing techniques to obtain personal data

The email will be designed to look very legitimate and will normally contain a link that a person will be asked to click to follow. The email will normally advise them that there is something wrong with an account they have, or that they need to verify a matter with an account they have. They will need to follow the link to do this. The link will take them to a replica website (to the official one from the organisation they are presenting themselves to be) and will ask them to input their personal details. The personal details will then be stolen and used in criminal activity.

We should be aware of any email or communication that we get that states they are from a legitimate organisation. Most organisations will not ask you to provide your personal details in this way over web communications, so we should be very wary of any organisation that is. If we look closely at an email, we can often tell when it is 'phishing' for our data:

- There will sometimes be spelling errors or bad grammar in the email. If the writing style is not professional, formal and grammatically correct, this can be an indication it is fake.
- The email is impersonal. Many phishing emails are set out in bulk. This means they are not always addressed to an individual, for example 'Dear Customer' and not 'Dear John'.
- The email will often want you to urgently respond to something and expresses that if you don't there will be some kind of detrimental effect, such as account closure, or a fee charged.
- When you click on the sender's email you will see that it is not actually from the expected person, and actually from a spam email. This is called spoofing!

## Social engineering

**Social engineering** preys on the issue that people are often the weak point in the security of a network. It preys on the problem that people can often be influenced into aiding access to network, often without them even knowing or realising it is happening.

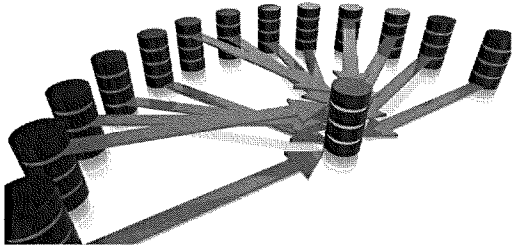
**Social engineering** – tricking people into breaking security procedures to break into a network

An example of social engineering is when a perpetrator calls an employee in a company presenting themselves as a network administrator from the same company. They will often act like the employee has reported a problem with their computer by asking them what the problem is that they have reported. Many employees probably haven't reported an issue and will think the administrator is confused, then just forget about the call. They may fall upon one employee that actually has reported an issue and will then seek to obtain details from them such as their login and password, advising that they need them to fix the problem. The employee may then give the details and the perpetrator then has a login and password to access the system.

Employees in a company should be wary of any telephone call that asks them for login details. They should also report any call they feel is suspicious, especially when it is asking about a problem that they don't have.

**Discussion Point:** The 'Band Name' game involves finding out what you could call your music band by adjoining the name of the street you first lived on and the name of your first pet. While this is good fun, why might you not want to play this game with someone you don't trust?

As well as malware, phishing and social engineering, a network can be subjected to the following threats:

Threat	Description
<i>Brute-force attacks</i>	<p>This type of threat is when a person tries to access a network by cracking the login details. This is done through the process of trial and error, by using automated software that will generate many different possibilities for the login details and try each one in turn.</p> <p>Having a limit set on how many times attempted access can be carried out on an account, and using strong passwords (such as those that are long and combine small case and capitals, along with letters and numbers) that are less likely to be generated by the software, make an account more secure.</p>
<i>Denial-of-service attack (DoS)</i>	<p>This type of threat is designed to flood a network with useless network traffic. This will make it run very slowly or grind to a halt altogether. This is often a threat that is carried out on a web server to 'take down' a website.</p> <p>Malware is used to obtain access to a number of computers that will be used in the attack. These computers are referred to as zombies, and a network of zombies is known as a botnet. When the attacker is ready to strike, they will use all of the computers they have managed to gather to create useless network traffic. This is done for a number of reasons, including demand for money to stop the attack, or to punish a company for something they have done, possibly unethically.</p>  <p>Many zombies are used to carry out a denial-of-service attack</p>
<i>Data interception and theft</i>	<p>This type of threat is when data packets are monitored that are travelling around a network. They are monitored to look for packets that contain personal or sensitive data. This kind of data is found by 'packet sniffers' that analyse the data in each packet.</p> <p>Using a VPN to send personal and sensitive data can deter a 'packet sniffer' from being able to analyse the data that is in a packet.</p>
<i>SQL injection</i>	<p>SQL is short for <i>Structured Query Language</i>, which is often used to search through data in a relational database. An <i>SQL injection</i> attack is when a hacker inputs SQL commands into a login form in order to gain access to a database. Login forms should always sanitise the input text so that it is treated as data (and not instructions) by the database. If it doesn't then it is open to exploitation from SQL injection attacks.</p> <p>When a user enters their login details to access their account, SQL is used to search through the many records in a database to find their account and to check whether the inputted login details are correct. A perpetrator could potentially use SQL commands to fool the website into thinking it has received a command to show user login details.</p> <p>For example, a statement such as <code>UserName OR 1=1</code> entered into the username input field could trigger all the records in the database to be displayed (as <code>1=1</code> is always true). This could then be used to steal users' information. Alternatively, if the hacker knows the name of the database, they could even input a command to delete the entire database!</p>
<i>Poor network policy</i>	<p>A network may become under threat if an organisation has a poor network policy. If an organisation does not regularly test their network for security issues and loopholes, they may find one can be exploited before it is found and fixed.</p> <p>The organisation should be making sure that all legislation is being correctly followed with regard to running their network. They should be making sure that regular backups are carried out. They should also be making sure that network users are being careful and correct in using the network and not opening it up to any security issues.</p>

## How can we identify these threats and prevent them from occurring?

### OCR specification point:

☑ identifying and preventing vulnerabilities:

- penetration testing
- network forensics
- network policies
- anti-malware software
- firewalls
- user access levels
- passwords
- encryption

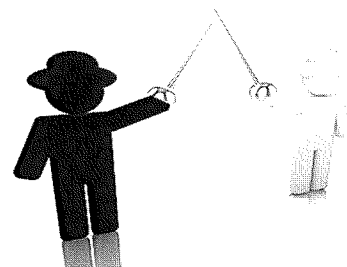
As we can see, there are many types of attacks and threats that a network can be subjected to. For this reason, we need to try to find ways to prevent attacks occurring. It can also be extremely helpful in preventing attacks if we are able to identify any threat. There are a number of methods we can use to identify and prevent areas of a network that could be vulnerable.

### Penetration testing

In order to find out whether there are any security vulnerabilities in a network, a company can employ a team of people to simulate potential attacks on their network. This is called penetration testing (or pen testing). Penetration testing can be carried out manually by individuals who carry out attacks and reveal any security weak points. It can also be carried out by automated software that will perform a series of attacks.

People who carry out penetration testing are often referred to as ethical hackers, or white-hat hackers. Once any vulnerabilities have been identified, the organisation can look to develop their network security and make sure that the attack can be prevented.

**Discussion point:** When someone gains unauthorised access to a computer system, do you think that the perpetrator is at fault for illegally gaining access, or that the organisation is at fault for having a vulnerability in their network?



White-hat hackers are employed to combat black-hat hackers (perpetrators who attack networks)

### Network forensics

Network forensics is carried out on a network to find out the cause of a network attack. The packets that have entered a network can be analysed to find the cause and source of the attack. This data can then be used to develop the security of a network and prevent further attacks from occurring.

Some organisations carry out network forensics on an ongoing basis. Data packets are analysed as they enter the network and the data from this is captured and stored. At periodic intervals, the stored data is analysed and checked for any issues. This is normally done in batches. In order for this level of forensics to be carried out, a company will normally need a large amount of storage to capture all the data.



Network forensics is analysing data packets that have passed through a network, to look for clues that lead to the source of an attack

### Network policies

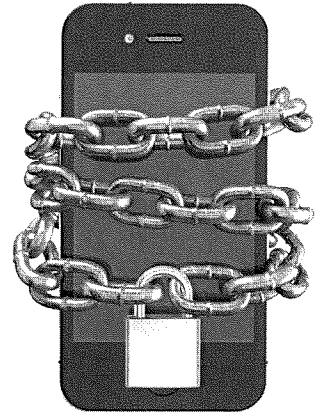
It is essential that a company has a well-thought-out and thorough network policy in place. This should include:

- Regular testing of the system to find any vulnerabilities
- Regular updating of the system to make sure both hardware and software are as up to date as possible
- Limiting the access of data to those who should only have access to it
- Installing and updating any security measures that will strengthen the security of a network
- Monitoring the use of the network by users and making sure it follows the acceptable use rules in place
- Regularly backing up data so that it is not lost in the event of an attack

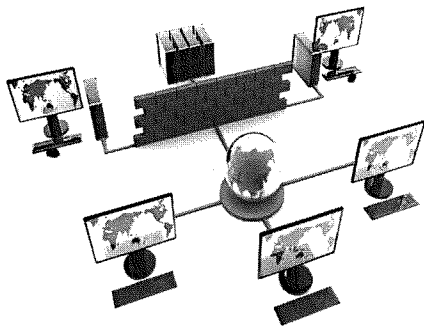
## Anti-malware software

This kind of software is designed to find any malware that has been downloaded onto a user's system. The anti-malware software will search a computer system to look for any malware. If it finds malware it will isolate it and quarantine it. The malware can then be deleted. If malware is found on a system, it may need to be scanned a number of times before the malware is completely eradicated. This is because it can often have the ability to hide in different files and folders.

Criminals are constantly developing new types of malware to bypass a security system. Anti-malware software developers are constantly trying to keep up with the new malware that is being created. A vicious circle is formed, which is why if our software is not up to date, it may not be able to detect some of the newer malware that has been developed.



We must protect our devices with anti-malware software to make sure our personal and sensitive data is not stolen



## Firewall

A firewall is a network security system that can either be hardware or software based. It uses sets of rules to control network traffic coming into and going out of a network. All traffic that is allowed into and out of the network is defined in the firewall policy. Any traffic that is unauthorised is rejected and does not gain access to the network, or is not allowed to leave the network. The rules that are set out in a firewall policy are designed to recognise malicious traffic and to deny it access.

**Firewall** –a security measure that prevents unauthorised traffic coming into or leaving a network, by using a set of rules.

## User access levels

The levels of access that are granted to users control the data and the parts of the network that users have access to. Limiting access to sensitive and confidential data with levels of access can help to keep data more secure. This helps mostly with any kind of insider attack that may occur, or with a social engineering attack.

The level of access that a user is granted is normally linked to their username.

## Passwords

To help prevent unauthorised access to a network, users must be encouraged to set strong passwords. A strong password is one that:



- Is more than a few characters in length, e.g. it must be at least eight characters in length
- Uses a combination of letters, numbers and symbols
- Uses a combination of lower-case and capital letters
- Is not identifiable data that is easily linked to the user, e.g. birthday, pet name
- A strong password will be much harder to crack and is far less likely to be generated by software in a brute-force attack. It is also advisable to regularly change passwords.

Many organisations will set rules for their password creation to make sure that a strong password is chosen. They often make their users change their password periodically too.

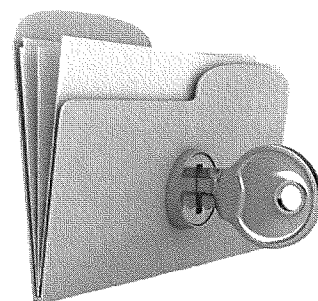
**Discussion point:** How well do you think your passwords would stand up against a cracker? Do you think they would be discovered quickly? Will you change how you set passwords?

## Encryption

When we store data on a network it is always going to be at risk. We need to do everything we can to protect this data, and one of the things that we can do is **encrypt** the data that we store. This way, even if a hacker gains access to the data, it will not be of much use to them as they are not able to read it.

**Encryption** – scrambling data to make it unreadable, to add to security in transmitting the data. The receiver can then decrypt the scrambled data to reveal the actual data.

To make it more secure, we can encrypt the data that we store with a key



## Chapter Summary

- A network can create risks as well as bring about benefits.
- A network can come under attack in a number of different ways; this includes active, passive, distribution, insider and close-in attacks.
- Malware is harmful software that is unknowingly downloaded onto a user's computer system. It is designed to disrupt or damage the computer.
- Phishing is when an unauthorised person tries to collect personal and sensitive data by disguising themselves as a reputable individual or organisation.
- Social engineering preys on the issue that people are often the weak point in the security of a network. It preys on the problem that people can often be influenced into aiding access to network, often without them even knowing or realising it is happening.
- There are number of treats that a network can be subjected to; these include brute-force attacks, denial-of-service (DoS), data interception and theft, SQL injection and poor network policy.
- There are a number of measures that can be taken to protect a network; these include penetration testing, network forensics, network policies, anti-malware software, firewalls, user access levels, passwords and encryption.



## Practice Questions

1. A company wants to make sure that its system is very secure. It hires an individual to carry out penetration testing to improve its network security. Explain what is meant by penetration testing. [2]
2. Describe two other security methods that the company could put in place. [2]
3. Explain how an individual could use SQL injection to steal personal data. [3]
4. James received an email advising him his social media account has been hacked. The email asks him to click a link and confirm his details to resolve the attack on his account.  
State the name given to this type of email. [1]
5. Explain two ways in which people can be the weak point in the security of a network. [4]