Get started
In small groups, research some examples of high-profile companies who have had their systems hacked. Answer the following questions

- Why do you think that company was targeted?
- What do you think were the intentions of the hacker(s)?
- How did the company respond to the attack?
- Do you think it is possible to create a secure network which will never be hacked? If so, how would you go about creating this?

Introduction
Online facilities, whether on public networks or private networks, are vulnerable to attacks from determined individuals. There have been many high-profile examples of people hacking into secure government systems, and of newspaper journalists hacking people’s mobile phones. It is extremely difficult to keep the hacker out if they are very determined, but there are things we can do to prevent access by the opportunist. This section also looks at why secure network access is important for individuals, businesses and society.

Types of threats
Threats to computer systems come in many forms.

- **Opportunist threats.** People who find an unattended computer which has been left logged in to a system may view, steal or damage information, programs or even hardware.

- **Computer viruses.** These are small programs which can replicate themselves and spread from computer to computer. They are never beneficial; usually they will make some changes to the system they infect and, even if they do no real damage, they are undesirable. They arrive by attaching themselves to files or email messages.

- **Other malware.** Examples of malware include: computer worms (essentially a computer virus which does not need to attach itself to a file or message); Trojan horses, which appear as some benign program allowing a hacker full access to a system; spyware; adware; and various other nasties. Malware is never beneficial.

- **Phishing.** This is a type of threat which attempts to gain access to passwords, financial details and other such privileged information. Often this is done by email messages pretending to come from trusted websites, instant messaging or social networks. Normally they try to divert you to a website which looks original and which asks for information about you.

- **Accidental damage.** This may be caused by a natural disaster (e.g. flooding), mischief or accidental mishap, and can result in losing all of a computer’s data.

Key term
Malware – A hostile, intrusive or annoying piece of software or program code.

Did you know?
The term Trojan Horse is taken from Greek mythology. The Greeks and the city of Troy had been at war for a very long time. The Greeks delivered a large wooden horse to the gates of Troy as a gesture that the war was over and they withdrew their fleet of ships from the harbour surrounding Troy. The people of Troy took this gesture as a sign that they had won the war and they celebrated their victory by allowing the Trojan Horse to enter the city gates. However, during the night Greek soldiers, who were hidden inside the horse, snuck out and opened the gates to allow in the Greek army, who had sailed back to port under the cover of darkness. The Greeks entered the city and destroyed it, thus ending the war.

Image to follow

Figure 1.16 Example of a phishing email
Importance of security

Computer/technology systems are under continuous threat of attack and the threats are continuous and ever changing. All computers and systems are vulnerable to attack and it is impossible to provide 100% protection.

An attack could result in some form of loss (data or financial) to an individual, organisation and/or society. Examples include:

- Organisations which trade online have to build up a reputation for being a secure organisation with secure network access. If this reputation is damaged, potential customers might be put off, costing the business money.
- When an organisation’s secrets are spread to competitors or to the wider public, any particular advantage the organisation has will be lost. An example is when an organisation has been doing research on a new product, and the results of that research find their way to a competitor.
- Identity theft could cause problems with obtaining loans and other contractual agreements (see page 41).
- Disclosure of information could cause legal problems. A company can be sued by its customers if it sells their personal information or fails to protect it properly. The obligations of organisations to protect customers’ data are covered by the Data Protection Act (1998). Organisations that store people’s personal information have to register with the Information Commissioner’s Office (ICO) and must undertake to treat the information responsibly.

Case study

In April 2011, the gaming giant, Sony®, has its PlayStation Network hacked in what is thought to be the largest internet security break-in to date.

Sony® revealed that the data for approximately 77 million users had been stolen during the attack. Users’ data stolen included:

- usernames
- passwords
- credit card details
- security answers
- purchase history
- address.

Research the attack.

1 How do you think online networks can protect users’ data from attacks of this kind?
2 How do you think an attack of this scale has affected:
   - The general public’s confidence in online networks?
   - The security protocols of companies who trade online?
   - The internet as a whole?
Introduction

As you saw on pages 38 and 39, there are ways in which information can be damaged, stolen or lost by malicious action or accidental events. There are many things we can do to limit the possibility of this happening. This section looks at some of the measures you can take to protect your data and your personal safety online.

Preventative and remedial actions

It is important to protect both IT systems and their data. Using the following can help:

- **Physical barriers.** These include turning off computers and locking offices when the systems are unattended to prevent damage by people, the environment (e.g. fire, flooding, electrical interference) or theft.
- **Password control of access.** Passwords are sequences of characters, known only to the computer user, which allow access to a computer, network or application. Passwords should always be strong so that it is hard for someone else to guess them or work them out.
- **Access levels.** These can be set up to allow individuals to have access to only specific levels of an application and to prevent unauthorised users from accessing particular data.
- **Anti-virus software.** This is set up to intercept computer viruses before they can become resident on the computer. The software can isolate the virus, remove it and sometimes repair any damage. Equivalent security programs exist for other types of malware.
- **Firewall.** This is a piece of software that monitors all data arriving at your computer from the internet and all data leaving your computer. It stops anything that it thinks is harmful or unwanted (such as viruses, spam, Trojan horses and hackers).
- **Encryption.** This is used to codify data so that it cannot be read by anyone who does not have the key to the code. An algorithm, sometimes known as a cipher, is applied to the data at the transmission end and the reverse is applied at the reception end.
- **Backup and recovery.** Making a backup of data is the only way of recovering from a total data disaster. Many individuals and organisations back up data to Flash® solid state storage devices or magnetic tape at night. The tapes are stored safely in a separate place, so that they are not destroyed by any disaster which could destroy the master system (fire, earthquake, etc.). Many types of backup exist, including:
  - Full system backup of all data held for a specific purpose.
  - Incremental backups of files or data that has been changed since the last full backup. This is faster than running a full back up every time.
  - Backups to removable media, such as a removable hard drive (if you have a large amount of data), USB sticks, CDs and DVDs.

It is also possible to back up data across a network (or across the internet) to a server in a completely separate location (for example, backing up data to the cloud).
Personal safety

The dangers of identity theft and of revealing too much personal information on social networks and via instant messaging are often reported in the news.

These threats can affect both your security and your reputation. Think about who has access to the information you put online. Before you put photos on your social networking profile, think about who might see them and whether you would mind. You might not want your employer or teacher to see something that might be embarrassing or harmful to your reputation.

Use security settings to protect your privacy and identity. Remember that not everyone is who they claim to be. Criminals access social networking sites trying to find out information about people. This may put you at risk of identity theft and password theft if you have revealed too much information about yourself. Be careful not to reveal information that you might use in a password, such as your pet’s name.

Assessment tip
Make sure you know the methods that can be used to protect and restore data.

Just checking
1. Give three examples of threats to computer systems.
2. Give the methods that you can use to reduce the threats you listed in question 1.
3. How can you help to prevent identity theft when using social networking sites?

Discussion point
Discuss the ways that companies and government have access to your personal information via online services. Discuss the pros and cons of this.

Key term
Identity theft – When someone steals your personal details in order to use them to open bank accounts and get credit cards, loans, a passport or a driving licence in your name.

Reflect
Technology can be used to monitor individuals’ movements and communications. Burglars, for example could see from a public social network site that someone is away on holiday and break into their house. Similarly, if you send unencrypted email, it can potentially be read by other people. Can you think of any other examples?

Remember
Emails and email attachments can contain viruses. It is important to run up-to-date anti-virus software.
This section has been written to help you to do your best when you take the assessment test. Read through it carefully and ask your tutor if there is anything that you are still not sure about.

**How you will be assessed**

You will take an onscreen assessment using a computer. This will be set over about 15–20 screens and have a maximum of 50 marks. It will last for 1 hour.

There will be different types of questions in the test:

**A Questions where the answers are available and you have to choose the answer(s).** *Tip: Always read carefully to see how many answers are needed and how you can show the right answer.*

Examples:

- Which of the following is an online commerce service? Select the correct answer. [1]
  - A Train timetable
  - B Online tax return
  - C Online auction websites
  - D Instant messaging
  Answer: C

- What name is given to the device which directs the traffic over the internet? Select the correct answer. [1]
  - A Modem
  - B Server
  - C Client
  - D Router
  **Answer: D**

**B Questions where you are asked to give a short answer worth 1-2 marks.** *Tip: Look carefully at how the question is set out to see how many points need to be included in your answer.*

Examples:

- What is the main reason for zipping files? [1]
  **Answer: To compress them (i.e. make them smaller)**

- What is Transmission Control Protocol (TCP)? [2]
  **Answer: The protocol which takes data from a user’s application and passes it to the Internet Protocol for transmitting across the internet. It controls the reverse process at the receiver.**
C Questions where you are asked to give a longer answer – these can be worth up to 8 marks. Tip: Plan your answer – think about how many points you need to make. Check through your answer – you may need to use the scroll bar to move back to the top.

Examples:

Explain what client-side processing is. What are the benefits and the disadvantages of this type of data exchange? [6]

Answer: Client-side processing enables interactivity within a web page. When a user opens the web page, the code is downloaded to the user’s computer.

Advantages include speed of interactivity and security. Once the code has been downloaded to a user’s computer, the interactive elements should run quickly. And because the web pages are downloaded, the chances for corruption are reduced.

A disadvantage is that the scripting language which creates the code might not work on every browser. This means you would need to create different browser versions. The download time can also be affected by your computer’s ability to download and process data. Complex or large amounts of interactivity means web pages might be slow to load, and it can also cause other programs to run slowly.

Many questions will have images. Sometimes you will be asked to click to play a video or animation. You can do this as many times as you want.

Sometimes you may be asked to do a calculation – you can use the calculator provided in the onscreen test system if you need to.

Hints and tips

- Use the pre-test time – make sure you have read the instructions, tested the function buttons, adjusted your seat and that you can see the screen clearly.

- Watch the time – the screen shows you how much time you have left. You should aim to take about 1 minute per mark. Some early questions will take less time than this and some later questions will take you longer.

- Plan your longer answers – read the question carefully and think about the key points you will make. You can use paper or the onscreen note function to jot down ideas.

- Check answers at the end – you should keep moving through the questions and not let yourself get stuck on one. If you are really unsure of an answer or cannot give an answer, then you can use the onscreen system to flag that you need to come back to that question at the end.

- Read back your longer answers – make sure you view the whole answer if you are checking back. There is no spell check facility.

- Do you find it harder to read onscreen? – talk to your teacher about how the system can be adjusted to meet your needs; for example, changing font size or colour.
How to improve your answer

Read the two student answers below, together with the feedback. Try to use what you learn here when you answer questions in your test.

Question

Give four examples of how data can be threatened and an example of how each threat can be minimised. (8 Marks)

Student 1’s answer

Opportunist threats which can be prevented by turning a machine off, virus threats by installing antivirus software, phishing by using a firewall and accidental damage by doing regular backups.

Feedback on student 1

The learner has not read the question which asks for specific examples of ‘how data can be threatened’ and not generic types of threats. In effect they have not answered the question and they have not indicated how the data can be threatened. There might possibly be a couple of marks for the minimisation (antivirus software and firewall perhaps) but that would be quite generous.

Student 2’s answer

People may enter an office and find a computer already logged into a particular program. They could use the software to amend or delete records or files used by that program, which may not be detected until much later.

Always log off when you leave your computer, and set up an appropriate auto logoff time if this function is available.

Viruses are small programs that can arrive as email attachments which run once the attachment is opened. They can do all sorts of damage including deleting or amending data files or records. This may not be spotted at the time and will cause problems later.

Up-to-date antivirus software will scan emails, attachments and files for known viruses and will delete or isolate them.

Trojan Horses are programs which appear to be from some trusted person or website. When they are activated, often by diverting you to a look-alike website, they give a hacker control of your computer so that they can find out your passwords, bank details, etc.

Installation of firewall software will intercept and prevent these attacks.

A natural disaster such as a fire is capable of totally destroying all files on a computer system.

Making regular backups of files will allow the data to be loaded on a different computer and brought up to date with missing transactions. It will provide continuity of operation.
Feedback on student 2

Four specific threats to data have been identified and described in sufficient detail to show why they are threats. It is clear the learner understands the nature of the threats.

The “remedies” have also been well described, again showing knowledge of the nature of the problems.

Full marks for this answer.

Assess yourself

Question 1
Which of the following terms is not a method of online information exchange? [1]

A Blog  C Cloud  
B Wiki  D Podcast

Question 2
What do you understand by the term “netiquette”? [2]

Question 3
State what the acronym VoIP stands for and give an example of a service which uses it. Describe one way how it may be used and give two examples of limitations to the service [5]

Answers

1) C

2) A set of rules which govern the behaviour of people using the internet. Or something similar: one point for knowing they are rules/conventions on behaviour, and one point for knowing that they have to do with networks/internet. A definition of network etiquette or internet etiquette would be worth one point.

3) Voice over Internet Protocol (1 mark); and an example is Skype™ (1 mark). It can be used by companies with many locations to hold video conferences over the internet (1 mark, but any acceptable use is valid). Limitations include quality of voice and video (1 mark) and an unreliable service from a network provider (1 mark, also anything similar or additional such as security problems could be used).