

# Skill Set 1

## Threat Awareness

By the end of this Skill Set you should be able to:

Identify IT Security Risks

Understand the Threat and Effects of Viruses

Recognise Other Forms of Malicious Software

Identify Hoaxes and Hackers

Recognise E-mail Threats

## Exercise 1 - Introduction

### **Knowledge:**

A world without computers is very hard to imagine today. Together with the Internet they have changed the way we live our lives, and most of the people you meet will use a computer at home *and* at work. They have revolutionised the way we communicate with each other and how we conduct business, and have forever changed how we think and work. However, despite making our lives so much easier, the widespread use of technology also brings with it many security concerns that IT users must be aware of. As such, this guide will try to explain some of the dangers of using IT systems and help you to avoid many of the pitfalls.



You must take steps to protect your computer, portable devices, and personal information from loss (e.g. hardware failure or theft) and any potential external threat (e.g. viruses or hackers). You must respect the confidentiality of any information that you have access to, and follow all laws and guidelines that apply. Indeed, the organisation that you work for should have a privacy policy to show you how to do this, as well as Internet and e-mail guidelines – make sure you find and follow them. Also find out who best to approach if you have any questions relating to the safe use of IT, or who to contact if you need to report a security concern.

**Note:** *Keep in mind that the following exercises are not designed to scare you, but to make you aware of the many potential dangers that exist when using IT systems and the Internet. With a little knowledge and common sense, you'll soon be using your computer confidently and safely.*

### **Activity:**

*Food for thought...*

1. Do you use a computer where you work or study?
2. Do you think you are fully aware of the many security issues related to protecting data and using IT systems?
3. Do you consider your computer adequately protected? Do you know how to check whether your computer is secure?
4. Do you feel that you have any responsibility for the security of the data on your computer or network?

## Exercise 2 - Viruses

### Knowledge:

The most well known and feared threat to computers is the computer **virus** – a small piece of malicious software (introduced to a computer system from an external source such as an e-mail or Internet download) with the ability to spread itself to other computers.

A virus is created by computer programmers to exploit security “holes” in popular programs. Once active, viruses can cause many levels of harm to your computer system – and even other computers connected to your network. Some simply cause a nuisance by altering the default behaviour of your software; others can cause significant problems by deleting files or damaging the *Windows* operating system itself, causing your computer to “slow down” or stop working altogether.



Fortunately, viruses can only affect your computer if they are introduced to it from outside (e.g. from memory sticks, CDs or DVDs, or from the Internet or E-mail). Furthermore, in most cases, viruses will remain inactive until you open or run an “infected” file or program, which then allows the virus contained within to run. However, if you are careful and follow some simple guidelines, it is very unlikely your computer will become infected.

Most importantly, always ensure you have **anti-virus** software installed and running (more on this in a later exercise). Also, be very wary of files downloaded from the Internet; if only genuine software and files from reputable sources are downloaded to your computer, in theory there should be no danger. If, however, programs or files are obtained from dubious or illegal sources, the chance of them containing a virus is much greater.

Also, as you will see in a later exercise, you must be especially careful of e-mail messages and their attachments – from unknown sources and from friends – as they can both contain potential threats to your computer. Even documents or spreadsheets used in applications such as *Microsoft Word* or *Excel* can contain harmful viruses! This is why you are sometimes given the option of opening files and templates in **safe mode** or with *features disabled* – if a virus can't run, it can't cause any problems!

### Activity:

1. What is a computer **virus**?
2. Name some common ways for a **virus** to get onto your computer?
3. What can you do to avoid **viruses**?

**Note:** Answers are listed in the **Answers** section at the end of the guide.

## Exercise 3 - Worms, Trojans and Rogue Diallers

### Knowledge:

In addition to computer viruses, there are many other types of “malicious software” (commonly known as **malware**) that can threaten IT systems and data. Most gain access to your computer without your knowledge (often via Internet downloads or e-mail attachments). Many are simply annoying and slow down your computer or Internet connection, but others are far more serious and can give others remote access to your programs and data.

### Worms and Trojans

A **worm** is very similar to a virus in that it can create and send copies of itself to other computers. It exploits security holes in your software and can significantly slow your computer down, as well as damage important files and programs. It can also open a “back door” to your computer, allowing other people to access the programs and information stored on it.

A **Trojan** is a file or program that, on the surface at least, appears safe and legitimate, but when opened does something unexpected and unwanted (including infecting your computer with viruses and other forms of malware).

Both worms and Trojans are often distributed in the form of programs or image files that you are encouraged to open (e.g. as an e-mail attachment or a website download).



**Note:** The term **Trojan** comes from the Greek story of the Trojan horse, where a gift that appeared entirely innocent turned out to contain a serious threat hidden within.

### Rogue Diallers

A **rogue dialler** can only affect dial-up Internet connections. It is a piece of software which deletes your **Internet Service Provider (ISP)** phone number and replaces it with that of a premium rate ISP. Each time you connect to the Internet, you inadvertently incur large telephone costs. Fortunately, if you have broadband Internet access, you cannot be affected by this type of virus.

**Note:** Good anti-virus software and safe downloading practices can prevent all the threats described here from gaining access to your computer.

### Activity:

1. What is a computer **worm** and how can it damage your computer?
2. What is a **Trojan** and why is it dangerous?
3. What is a **rogue dialler** and how can it affect you?
4. What can you do to avoid **worms, Trojans** and **rogue diallers**?

## Exercise 4 - Spyware and Adware

### Knowledge:

**Spyware** and **adware** are specific forms of malware that can significantly reduce your computer's performance levels and open your programs and data to unwanted change and exploitation. Some threats will simply display annoying advertisements as you use your computer, but others can monitor your online activities (or steal sensitive information such as e-mail addresses, passwords, and stored credit card numbers) and then send that information to another person via the Internet.

Importantly, most types of spyware and adware are not strictly classed as viruses, and so most anti-virus software will not always detect or remove them. To do that, you will need to install and use a dedicated **anti-spyware** program (more on protecting your computer from threats in later exercises).

### Spyware

The name **spyware** is given to software that gains access to your computer without your knowledge, usually when you install "free" programs downloaded from the Internet. Spyware can change computer settings, interfere with Internet browsing, and can even slow an Internet connection to the point where it becomes unusable. Far more seriously, it can also run silently "in the background" as you use your computer, gathering various types of personal information (e.g. your Internet browsing habits or the keys you type on your keyboard) and then sending that data to other people.



### Adware

**Adware**, unlike other forms of malware, is far more intrusive. It automatically downloads and displays advertisements on your computer (often in "pop-up" windows as you browse the Internet). Adware is often installed on your computer without your knowledge, and is usually itself a form of spyware.

**Note:** *As with most malware, spyware and adware usually gains access to your computer via Internet downloads or e-mail attachments. However, it can also be installed alongside legitimate software (many software companies use "sponsored" adverts in free software to cover their development costs). Be sure to read any license agreement or privacy statement before installing software to make sure you know what you're getting.*

### Activity:

1. What is **spyware** and why is it dangerous?
2. What is **adware**?
3. Will anti-virus software always detect and remove spyware and adware? If not, why not?
4. What can you use to avoid both **spyware** and **adware**?

## Exercise 5 - E-mail Risks and Spam

### Knowledge:

Today, e-mail is an extremely important and efficient communication tool and many businesses would come to a standstill without it. However, there are also many risks associated with the use of e-mail, and in particular with files attached to them.



### E-mail attachments

Always be very careful of e-mail messages containing **attachments** (enclosed files), from unknown sources *and* from friends, as they can potentially contain viruses and other forms of malware. If you do open a message attachment that contains a virus, the results can be catastrophic for your own computer and possibly all the other computers on your network!

**Note:** *It is highly unlikely that your friends will intentionally send you a virus by e-mail. However, if your friends do not have good anti-virus and anti-spyware software installed, they may not even be aware that a file is infected. Also, some viruses affect e-mail programs and automatically send copies of themselves to the e-mail addresses of listed contacts.*

As a rule, always save important attachments to your computer first, and then scan the files using your anti-virus software before opening them (you will learn more about anti-virus software in later exercises).

### Unwanted messages

Be prepared to receive *a lot* of unwanted e-mail (known as **spam**). Certain companies and individuals send out lots of junk mail, often in an attempt to sell you something (usually of an adult nature). For some people, junk e-mail can severely impact upon their productivity, forcing them to spend large amounts of their working day deleting messages. Indeed, the sheer volume of junk mail can affect the performance of their computer systems and the network they are connected to.

Of course, you can simply delete junk e-mail as you would throw away real unwanted mail (your e-mail program can even be set up to do this automatically for you). Many of these types of messages also have a means to allow you to unsubscribe from their mailing list, so no further messages will be sent to you. It is always worth scanning the message for this.

### Activity:

1. Why should you be wary of e-mail messages with attachments?
2. Are e-mail messages from friends and work colleagues safe?
3. What is unwanted e-mail better known as, and why can it become a problem?

## Exercise 6 - Hoaxes and Hackers

### Knowledge:

#### Hoax E-mail

**Identity theft** is as much a risk online as it is in real life! Hoax e-mails, such as chain messages or bogus petitions, are at best a nuisance, but they can also be considerably more dangerous if you act upon their instructions. Scam e-mails usually take a particular format, such as fake virus warnings, offers of cash, appeals to help people transfer savings, and even chain e-mails which you must forward to a specified number of other people. Simply delete them!



More subtle tricks also include official-looking e-mails allegedly from banks asking you to confirm account details or credit card numbers. Delete them immediately as this is a form of identity theft known as **phishing**. Remember: banks will never ask for personal or sensitive information to be put in an e-mail.

Unfortunately, the Internet makes it very easy to send hoax and scam e-mail, but there are some clues that can help you spot them. These include requests to forward a message to lots of people (sometimes to everyone you know); unsupported claims that you have won prizes or cash; language used in a way to create a sense of urgency (e.g. “act now to protect your computer from this devastating virus”), and requests for money - especially up front “fees”.

**Note:** *If you receive an e-mail from an unknown person that appears too good to be true, it probably is. At best it may waste your time, but at worst it can cause embarrassment and cost you a great deal of money.*

#### Hacking

A term often used by the media, **hacking** has come to mean changing computer software (or hardware) to do something other than what it was intended to do. More commonly, individuals known as **hackers** try to gain *unauthorised* access to computer systems in order to steal the data on them. Precautions such as installing a **Firewall** (described later) will help protect your computer from hackers.

**Note:** *Many expert programmers or network security specialists consider themselves to be hackers. These are professional people who are in no way interested in gaining access to your computer!*

### Activity:

1. What is **phishing** and why is a problem?
2. If you suspect an e-mail of being a **hoax**, what should you do with it?
3. What is a **hacker** and what does it do?

## Exercise 7 - Develop Your Skills

You will find a *Develop Your Skills* exercise at the end of each Skill Set. Work through it to ensure you've understood the previous exercises.

1. Name **fives** types of **malware** that present a threat to your computer's performance and your information security.
2. What is another name for **junk e-mail**?
3. What should you do if you receive an e-mail from an unknown source?
4. List some examples of the form **hoax/scam** e-mails can take.
5. What should you do with a message you think may be a **hoax**?
6. Is a **bug** the same as a **virus** or **malware**?
7. How can **malware** gain access to your computer?
8. What is **phishing**?
9. What is **spyware**?
10. What is **adware**?
11. What is the name given to malware that replaces your **ISP's** telephone number with that of a premium rate alternative?
12. What does **hacking** mean?

**Note:** Answers are listed in the **Answers** section at the end of the guide.

## **Summary: Threat Awareness**

In this Skill Set you have seen many of the potential threats that can damage your computer and those of others on your network. You have also learned how malware (in its various forms) can affect your system performance and information security.

You have seen how the current widespread use of technology has created a definite need for IT users to take sensible security precautions to avoid threats (such as anti-virus software), and learned how hoax e-mail, spam, and hackers are able to affect your privacy.

Your OCR ITQ evidence must demonstrate your ability to:

- Identify security issues that may threaten system performance:
  - Viruses, worms and Trojans
  - Rogue diallers
  - Spyware and adware
  - Unwanted junk e-mail
  - Potential sources of malware
  
- Identify threats to information security:
  - Information theft and phishing
  - Hackers and unauthorised access
  - Hoax e-mail
  - Malware (including viruses, worms, Trojans, and spyware)