

Section 1

Security Awareness

By the end of this Section you should be able to:

Appreciate the Security Risks involved in using IT

Understand Threats associated with E-mail

Be Able to Identify Unwanted and Hoax Messages

Be Aware of Viruses and other Threats to your PC

To gain an understanding of the above features, work through the **Exercises** in this **Section**.

For each **Exercise**, read the **Guidelines**, without touching the keyboard, then work through the numbered steps of the **Actions** on the computer. Complete the **Revision Exercise(s)** at the end of the section to test your knowledge.

Exercise 1 - Awareness

Guidelines

A life without computers would be hard to imagine today. They are used in almost every walk of life and the majority of people will use a computer at home and possibly at work too.

Although computers can make our lives so much easier, you must be aware of the security implications of using them. Steps must be taken to protect your computer hardware, systems and portable devices, your personal information and data and you must follow guidelines relating to IT security and privacy of information. You must respect the confidentiality of information that you have access to. All organisations should have a privacy policy to show you how to do this. They should also have an e-mail and Internet use policy and health and safety guidelines to follow. Make sure you know where to find the relevant guidelines and procedures for your organisation and make sure you follow them. Find out who to approach if you have any questions relating to the laws and guidelines governing the safe use of IT, or who to contact if you need to report a security concern.



The Internet and e-mail are useful tools for accessing information and communicating, but it's essential to be aware of the risk of attack from other users with hostile intent. This guide will try to explain the dangers and to help you avoid the pitfalls.

Actions

Food for thought...

1. Think about your computer use at home. What do you use it for?
2. Do you think you are reasonably aware of security issues?
3. Do you consider your computer adequately protected?
4. Do you use a computer where you work or study?
5. Do you feel that you have any responsibility for the security of the data on this computer?

Exercise 2 - E-mail Basics

Guidelines

Today, e-mail is an extremely important business tool and many businesses would, almost, come to a standstill without it. It has obvious advantages over the normal postal system: it is much faster - mail is delivered within seconds. Rather than pay excessive postage for sending paper copies of files through the post or by courier, electronic files can be attached to e-mail messages. All the sender pays is the cost of a local telephone call with a dial up connection, or a lot less if they have a broadband connection. Consider how much more quickly business documents can be sent overseas using e-mail than by using surface or airmail. A point of note is that some anti-virus software/firewalls prevent certain types of attachment, which contain macros (such as databases) passing through. This is because some viruses use macros to work.



Before using e-mail, familiarise yourself with the rules of **netiquette** - network etiquette. Always use accurate and brief subjects in the appropriate field on a message. Keep your messages brief and relevant rather than rambling. Ask before sending large attachments; don't send heated messages (flames); don't use all UPPERCASE – it is the same as shouting; when replying, always make sure the subject is still relevant to your reply.

Make sure your outgoing messages are spelled correctly, just as you would before sending a letter. Many e-mail programs allow you to format messages with different colours, fonts and backgrounds. This provides an opportunity to show some individuality.

Consider the implications very carefully before sending any sensitive information by e-mail. In a work situation, you must familiarise yourself with the e-mail policy in place. Usually, common business rules and regulations state that you must not send messages that might offend, or jokes, etc. Never send "chain letters". Basically only subject matter directly associated with the business should be sent via e-mail.

Actions

1. Why does some anti-virus software prevent file attachments containing macros from getting through?
2. What is the name for the etiquette that should be followed when using e-mail?
3. At work, what type of e-mails should be sent?

Exercise 3 - Unwanted & Hoax Messages

Guidelines

Unwanted messages

Be prepared to receive unwanted e-mails. Certain companies and individuals send out masses of junk mail (spam).

Any message, whether received via e-mail or through the door, which promises riches, prizes, or rewards in return for a cash payment or supplying your bank/credit card details should be regarded with the suspicion it deserves and be deleted or thrown away immediately.

Some more subtle tricks have included official-looking e-mails supposedly from banks, etc., asking you to confirm card details and/or PIN numbers. This is known as **phishing**. Delete them. Banks will never ask for such information to be put in an e-mail.

Be very careful who you give personal information to – identity theft is also a risk with e-mail. Take as much care to protect your privacy while using e-mail as you would in shredding normal mail before putting it in the bin.

Be suspicious of all e-mails from unknown sources. If in doubt, it is a good idea to get a second opinion. Preferably ask someone with experience of Internet and e-mail matters and whose opinion you trust.



These topics are covered in further detail in the following exercises: 5, 8 and 12.

Hoax messages

Hoax e-mails, such as chain messages or bogus petitions, are at best a nuisance, but they can be used to collect e-mail addresses and some are more ominous. These e-mails usually take a particular format, such as fake virus warnings, offers of cash if you forward the message, appeals to help a sick person, chain e-mails, which you must forward to a specified number of people for good luck. Spammers often use these e-mails to collect addresses; they can then send out a vast amount of spam e-mails, which appear to originate from your address.

There are some clues that can help you spot a hoax. Some examples are: requests to forward a message to lots of people (sometimes to everyone you know); unsupported claims that many other people have won prizes or cash; naming a legitimate company, e.g. Sainsbury's, who will give you a £50 voucher if you forward this to 20 friends; language used in a way to create a sense of urgency, e.g. "act now to protect your computer from this devastating virus", or "send money now" to pay for medical care for someone at death's door.

If you receive a message that you are afraid may be a hoax, delete it. Do not, under any circumstance, forward it to anyone else.

Exercise 4 - Viruses

Guidelines

A computer **virus** is a piece of malicious software code introduced to a computer system, with the ability to spread itself to other computers. This should not be confused with the term bug, which describes an error or fault in a piece of software code. The extent of the harm caused by viruses varies enormously.



In many cases the contamination remains unnoticed in its host file until a specific event triggers off its action. Viruses can cause many levels of harm to a computer system. The least harmful might cause slightly odd things to happen to a file, for example if a user typed text into a word processed document on an infected computer, certain letters or words might appear on screen in an unexpected text format. Another result of a relatively harmless virus could be the refusal of an application to save files to any area other than a specific folder on the hard disk drive, rather than the desired folder. The action that a virus carries out when activated is known as the **payload**.

At the other end of the scale, a virus might lie dormant until the built in clock within a PC reaches a certain time on a certain date, or possibly until the computer has been restarted a certain number of times, and then become active. This type of virus is variously known as a time bomb or logic bomb. It could then destroy the entire file structure on the hard disk drive and make the drive completely useless. If this type of virus infected a network, the effect could be catastrophic.

Macro viruses are those that are added to executable files within an application. The most common of these can occur within the template files in *Microsoft Word* and *Excel*. This is why you are sometimes given the option of opening such a file with macros disabled. If the macro can't run, neither can any virus that might be within it!

Be vigilant about e-mail messages; they can contain viruses. Ensure you have up to date anti-virus software installed on your computer. Messages without a subject or from an unknown source should be treated with caution. Save attached files to disk and scan them before opening if you are at all suspicious. If you do open a message attachment that contains a virus, the results can be disastrous for your computer.



Exercise 4 - Continued

A common type of virus is one that arrives in an e-mail attachment, installs itself within the recipient's *Outlook* or **Contacts** address book and automatically e-mails itself to some or all of the e-mail addresses it finds there. These viruses are particularly effective since the recipient may not realise that the virus has arrived, or they have spread the infection onwards. The new victims are less likely to be suspicious of attachments e-mailed to them by a known contact.

Viruses can only become active within a system if they are introduced to the system from outside and then activated.

The only pathways available to viruses are via input devices such as floppy disks, memory sticks, CDs or DVDs or the Internet. If only genuine application software from reputable sources is installed on a PC, in theory there should be no danger. If, however, disks containing applications or files are borrowed or bought from dubious or unknown sources, the chance of them containing viruses is much greater.

As mentioned earlier, e-mails received with file attachments are a major source of viruses and should be treated with particular caution, as should any files downloaded from the Internet that have a **.exe** extension. This extension identifies executable files, i.e. files that are actual programs that will open up and run. If the file contains a virus, the virus will run with the program!

Actions

1. What is a computer **virus**?
2. What is the name for the action carried out by a virus when it is activated?
3. What is the name for a virus that may lie dormant until a certain date and time?
4. What is a common way for a virus to get into your computer?
5. Which type of file should you be very careful about downloading from the Internet?

Exercise 5 - Other Threats

Guidelines

Worms and Trojans

A **worm** is a self replicating computer program, which uses a computer network to send copies of itself within a system to other computers on the network. It's not a virus, but can open a door for a virus to enter. At best, it simply clogs up the system resources.

A **Trojan** is **malware** (a malicious program) and its name comes from the story of the Trojan horse, because it is disguised as a link to a file that a user would be particularly tempted to open, e.g. a game or a graphics file. Once the link is opened, the Trojan gains access to the system.



Adware, Spyware and Rogue Diallers

Adware is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware.

Spyware is software that is installed without the user's knowledge on their computer to interfere with their interaction with the computer. This is done without their knowledge. These programs can gather personal information, such as Internet browsing history, can redirect your browser and can install additional software. Spyware can change computer settings, interfere with Internet browsing, slow down your connection and can sometimes result in loss of a functioning Internet connection or of other programs.

A **rogue dialler** is a piece of software which is installed on your computer without your knowledge, usually when you open a spam e-mail or visit a website which contains hidden malicious software. It affects dial up connections by deleting the internet service provider's phone number and replacing it with a premium rate number.



This means that each time you connect to the Internet you are running up a massive phone bill. If you have broadband instead of dial-up Internet access you should not be affected, as broadband connections work in a different way and cannot be changed by rogue dialler software.



Exercise 5 - Continued

Hacking

The term **hacking** basically means changing computer software (or hardware) to do something other than what it was intended to do. It can be used to gain access to systems thought to be secure in order to access or steal data on them.

However, hacking can sometimes be constructive. Many “hackers” are expert programmers and some companies or organisations employ them to find any flaws in their security system, so they can then repair them.

Actions

1. What is a **worm**?
2. What is **spyware**?
3. What is the name for software that deletes a legitimate dial up connection and instead dials premium rate numbers?
4. Which type of Internet connection will not be affected by the software referred to in question 3?

Exercise 6 - Revision

This Exercise covers the features introduced in this section. Try not to refer to the previous Exercises while completing it.

1. Why shouldn't you send an e-mail that has been typed in capital letters?
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 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**?
7. List the pathways to your computer that are available to a virus.
8. What is the name for software disguised as a link to a file that someone would be tempted to open?
9. What is **adware**?
10. What does **hacking** mean?



Answers to this revision exercise can be found at the end of this guide.

If you experienced any difficulty completing this Revision, refer back to the Exercises in this section. Then redo the Revision.

Once you are confident with the features, complete the Record of Achievement Matrix referring to the section, at the end of the guide. Only when competent move on to the next Section.