IINFORMATION GOVERNANCE TOOLKIT POLICIES: SAFE COMPUTING

What is malware?

Malicious software, or 'malware' as it is known, falls into a number of categories such as viruses, trojans, worms and spyware. The technical differences between these are subtle to a non-technical user, however, what they do have in common is that they are, to varying degrees, malicious and unwelcome.

The impact of the malware, known as its payload, can be as unobtrusive as monitoring the websites that you visit, possibly in order to target marketing, to taking control of your PC to either obtain personal information such as bank details etc or to use the computer to further propagate a virus around the world.

There are an ever increasing number instances of malware being released, with high profile and particularly virulent attacks such as the 'Nimda' and 'I Love You' viruses. The threat from malware is, therefore, ever increasing, with attackers seeking new ways of delivering the "product" to unsuspecting users across the globe.

Email hoaxes and phishing

Much has been written in the press about emails being received by users which appear to be legitimate correspondence from banks and other financial institutions that claim, for example, the user needs to reconfirm personal information.

The mails generally contain a link to a website requesting details, which will often include such information as name, address, bank account details etc. Rather than being communicated to their bank, these details will be provided to another, probably unscrupulous person or organisation.

This information can then be used for identity theft or to make unauthorised purchases.

Protecting against these threats

Make sure a firewall is installed
Because the internet is a public network, any connected computer can find and connect to any other connected computer. A firewall is a barrier between the public internet and your private computer system that protects you against a number of different online threats such as hackers breaking into your computer and some viruses, called 'worms' that spread from computer to computer over the internet. Some firewalls block outgoing traffic that might originate from a virus infection.

Your organisation will almost certainly have a firewall installed but further firewalls are available within Windows XP and Vista.

Make sure you have anti-virus software installed
Anti-virus software will provide protection against infected email attachments, viruses that attack over the internet (worms), and potentially spyware.

The anti-virus software, however, is only truly effective if it is up to date so it is important that you regularly download the update file.

In your work environment this will almost certainly be done for you by your IT department.

Make sure Windows and Office are up to date
Hackers try to find and exploit bugs and loopholes in popular software in order to get a back door into people's computers. Developers try to close these loopholes as they are discovered by distributing updates using 'patches'. These patches can be downloaded over the internet.

Use anti-spyware software
But be careful, some spyware is installed alongside advertising-funded programs downloaded from the internet. So wherever possible, buy or download software from reputable companies.

Be careful opening email and attachments
Email is a popular means for delivering malware. Your email address can be obtained from many sources, it could be the result of a hack of a website that you've given your address to or somebody simply guessing the address. Regardless of the method it can result in infected files being sent to you.
To protect yourself, be careful what you open. If the sender of the attachment looks suspect they probably are. If you're not sure about an attachment play safe and don't open it. Delete it straight away.

Protect wireless networks
Wireless networks are becoming more common both at home and in the workplace. They can bring about significant benefits through mobility and reducing the clutter and cost of cabling. However, as wireless access points 'broadcast' data your information is at risk of being intercepted or accessed without your authorisation. Furthermore, if not properly secured, your access point can be used by others to access the internet or other network services. It is essential that data transferred is encrypted and access restricted to only authorised users.

Take regular back ups and set system restore points

When all else has failed the existence of back ups or restore points are your last chance of recovering your PC or the data on it.

Back ups should be taken of your data on a regular basis. Ideally, data shouldn't be saved to your local PC but, rather, on the network, which your IT department will back up on a regular basis. If you have to store data on your PC you should copy it to the network or another form of storage media on a regular basis. [See also Good practice guide - removable media.]

System restore points are created by your Windows PC when significant events occur, eg when new software is installed. This process creates an 'image' of the PC prior to the event and allows the system to be rolled back in the event that something unexpected or untoward occurs.

These are the actions of last resort though, and while you should be aware of them and prepare for them you should not place reliance on them. Remember, prevention is better than cure.

Remember:

Do

- make sure that you have a firewall installed
- make sure you have anti-virus software installed and that you keep it up to date
- make sure you have anti-spyware software installed and that you keep it up to date
- make sure that you take regular back ups
- contact your organisation's IT department if you have problems or queries when using IT equipment at work.

Don't

- give out your email address if you are uncertain who is asking for it
- open emails or attachments if the sender is not known to you or if you suspect that the attachment is not what it seems
- provide your personal details unless the symbol is displayed in the bottom corner of your browser
- rely on back ups and restore
- bury your head in the sand and pretend it won't happen to you.