INFECTION CONTROL

Virus Protection Software

Although, by definition, *software* will have problems protecting you against the most recent viruses, it's still worth having it and using it. Many virus products use technology to attempt to detect unknown viruses and old viruses are still around.
What this means is:

- Install the software on all the machines that receive emails (or that may receive material on floppy disk).
- Set it up so that it always runs in the background, checking files when you open them.
- Keep the software and its virus database up to date - this usually involves paying an annual subscription fee.
- Scan your whole disk from time to time as an extra precaution.
- On a *network*, ensure either that each computer is individually protected or that you have protection covering the whole network.

The computer magazines survey virus protection software from time to time, without finding an obvious market leader. Some packages are slightly easier to use than others, while some have specific problems in an otherwise good package.

See the article “Choosing an Antivirus solution for your organisation for more information”

Internet Security Settings

Outlook Express and Outlook are widely used email programs that are commonly exploited by virus writers for security attacks. However, email software and web browsers usually allow you to specify your own security settings, usually via the Tools menu.

Be aware that some security settings may make web browsing less smooth. The highest security settings may even prevent some websites from functioning properly.

Changing the security settings in *Internet* explorer also changes the settings in Outlook and Outlook Express. For more information on changing your browser’s security settings and keeping your computer secure, see the CERT article Securing Your Web Browser and check your browser or email software’s help files.

Operating system and other software patches

Some viruses exploit security holes in the *operating system* or other software so it is important to keep up to date with the latest operating system patches. Windows users can visit the Microsoft site for the latest security patches or use Windows Update (click on start button and select Windows Update).
Apple users should visit the Apple Security Updates Page. For Linux and some other operating systems, see the Linux references on the CERT website.

Email Good Practice

There are other things you can do to make life easier and more secure, both for you and the people you send emails to. The two principles of good practice are to:

- Send emails and attached document which are inherently less likely to carry viruses.
- Make sure that people you email can tell who you are and can assess the likely content and value of your message.

Among the ways to make your emails less likely to carry viruses, you might like to consider the following:

1. Ensure that your email program only sends text emails, without any fancy*HTML* formatting. Set the mail sending format to Plain text, not HTML, (and ensure that there is no tick next to 'Reply to messages using the format in which they were sent' if available). Sending messages in plain text also makes them smaller (and therefore cheaper to send and receive for people with pay as you go dial up Internet access).
2. Before you attach document files, save them in the RTF format (which all versions of Word and many other word processors can use). In Word, when you are saving the document select RTF from the list of formats. This format preserves virtually all the layout and formatting, but cannot carry Word macro viruses (like Melissa or I Love You). RTF documents are also usually smaller than their .DOC equivalents - substantially smaller than most Word 97/2000 documents because these require two bytes per character to allow for international character sets. To make life easier for the recipients, adopt the following measures, and encourage others to do the same for you:
3. Ensure that you set up your system to identify you as the originator of the message. For example, in Outlook Express go to Tools | Accounts, select the account if there are more than one, then click Properties. Ensure that the Name field identifies you appropriately.
4. Whenever you send emails make the Subject line as informative as possible, so that the recipient can make their own decision about when (or, indeed, whether) to read it.
5. Put your proper name, the full name of your organisation and 'real world' contact details - a phone number at least - on all emails so that people both know who you are and have a choice of means to respond. You can set up a 'signature' in Outlook and Outlook Express to add the same information at the bottom of every message.
6. If you are attaching graphics or other files, try to save them in a compressed format (JPG rather than BMP, for example) or compress them using a program such as *WinZip*. If you have to send a file of more than a few hundred Kilobytes, you may want to warn the recipient and check that it is OK.
7. Remember that if you are sending emails to several people they can all see all the addresses that appear in the 'To' and 'Cc' field. If there is any danger that recipients might misuse these addresses, or might inadvertently pass them on to inappropriate people, you are better off putting all your recipients in the 'Bcc' (blind carbon copy) field. This may not be visible when you start a new mail message, depending on how your system is set up.

If other people don't follow principles such as these, you would have good reason for treating their emails less seriously. In particular, you should not open an attachment unless you receive it from a person you know, with a plausible, informative Subject line (I Love You from your bank manager does not count as 'plausible') and in a 'safe' format. If it's in .DOC, .ZIP or .EXE format you should certainly save it to disk and scan it for viruses before opening it.

In fact to be on the safe side it's wise to save all attachments to disk and scan them using up to date *Antivirus* software before opening them. Don't be afraid to delete emails without reading them if they appear to be dodgy in any way, either because of their format, or who they are from, or if they are offering you anything that sounds too good to be true (it won't be true).

Source : http://www.ictknowledgebase.org.uk/infectioncontrol