

Protect your PC from viruses

You can protect your computer from most viruses by taking the following simple steps:

1. Use caution and common sense

Don't open attachments that you are not expecting, even if they come from a trusted source. Often a virus can send out copies of itself using addresses found on the host computer, without the user of the computer being aware of it.

Be cautious about downloading games, screensavers or other software from the internet, particularly at work, and don't use illegally copied software. If your company doesn't have an IT policy yet, consider putting one in place to clarify this.

2. Use up-to-date antivirus software, and update it regularly

Syplex recommend using a reputable brand such as Symantec, Norton, Network Associates or McAfee, who offer a range of products suitable for corporate and personal use.

Once you have purchased antivirus software, it is important to ensure it remains up to date. The supplier will issue updates as often as new viruses are reported. Most antivirus software can be set up to check for updates automatically.

3. Use an Internet firewall

If you access the Internet and you don't have a firewall, your computer is vulnerable to attack. Corporate networks are best protected with a server firewall, but if you have a home PC, Microsoft Windows (XP and later versions) includes a built in firewall which can be easily activated to protect an individual machine.

Not sure how? Read our easy to follow guide "How to Enable the XP Firewall".

4. Download patches to update your computer software

Designers of viruses will exploit any reported faults in software and operating systems. However, if Microsoft reports a fault, they will issue software [never by email, only on their website] to fix the problem. You can download critical updates and patches from <http://support.microsoft.com>.

It makes sense for you to put these patches on your computer and fix any fault before you are caught out by a virus designed to exploit it.

Not sure how? Read our easy to follow guide "How to Install Microsoft Updates".

5. Don't be caught out by hoaxes

Sometimes it doesn't even take a virus to damage your computer. Malicious hoaxes often urge unsuspecting computer users to remove vital components from their computer software in order to fix a non-existent virus. If you suspect a virus hoax, you can check it easily at the following websites:

<http://vil.nai.com/vil/hoaxes.asp>

<http://uk.mcafee.com/virusInfo/>

<http://www.symantec.com/avcenter/hoax.html>

Please don't hesitate to contact Syplex Ltd if you have any questions about anti virus software, firewalls or other security related issues.