

Computer Viruses

June 2007

We're all at risk from computer viruses - but what exactly are they, and how can we avoid the damage and annoyance they can cause?

Our E-Business Advisers discuss:

1. What is a Computer Virus?

The term "**computer virus**" is often used to describe all kinds of malware (malicious software).

They're developed by programmers across the world, who, for whatever reason, use their talents to cause potential destruction, mayhem, disruption and annoyance to millions of PC users.

2. How do we catch viruses?

A virus can be passed to your PC via any type of (non virus-checked) data storage device (e.g. floppy disks, CD, memory stick).

More commonly these days, we face the threat of virus infection via the Internet. This has opened up the possibility of every PC using it to become infected at some time or other.

A virus can hitch a ride to your email InBox on the back of an innocent - looking email. They can hide themselves on unscrupulous Web sites, pretending to be something they aren't, when they're really a malicious program you innocently download and run.

3. Sneaky little things!

A computer virus is probably the best known and most dangerous threat to computer security. Just like an organic virus, which attaches itself to a healthy organism and causes damage, a computer virus attaches itself to healthy computer programs and data files.

With many different types of viruses, there are a wide variety of things they can do.

The most common symptoms that indicate your computer has been infected are:

- You begin to realise files or data is missing or deleted.
- Your PC takes longer and longer to load applications.
- Images on your screen are distorted, or unusual image and text appear.
- Unusual noises come from your keyboard or hard disk.
- Your PC hard drive operates excessively or is inaccessible.
- Hard disk space or filenames change for no reason.
- Maintenance or system tools such as Scandisk return strange results.

Some viruses can be intentionally destructive, others merely annoying, whilst some have a delayed action ("time bombs" and "logic bombs").

Fact Sheet

The time bomb causes something to happen at a particular date or time, whereas a logic bomb occurs when the user of a computer takes a specific action (or series of actions) - which then inadvertently acts like pulling a gun trigger.

4. How can you protect yourself?

Some viruses cleverly use stealth techniques to try and fool attempts to exterminate them.

A virus can hide itself, and send a message back to the anti-virus software to say the file it has attached itself to is "clean".

Modern anti-virus software employs the latest knowledge and techniques to counter even the most up-to-date viruses.

In a constant state of war with the virus writers, the anti-virus software companies employ highly developed techniques to counter sneaky and stealthy mechanisms of viruses.

The best way to protect yourself against viruses is to buy industry standard anti-virus software such as Symantec Norton Anti-virus or McAfee Anti-virus - and ensure you regularly update it.

A mistake many firms make is that they don't bother paying for the updates for this software after the first year of free updating.

As virus writers are constantly writing new viruses, this means that your PC very quickly becomes vulnerable, even though you have an aging copy of anti-viral software on the machine.

Anti-virus packages may not always protect you fully, though, if you were unlucky enough for your PC to be one of the first infected of a newly created virus - but they offer the best security solution possible.

Top tips to ensure you are as protected as possible are:

- **Install** anti-virus software.
- Keep your anti-virus software **up-to-date** (you can set the programs to automatically retrieve updates over the Internet).
- **Install** a personal firewall (software to prevent hackers and other security gaps).
- Use the latest **software updates** from Microsoft and other vendors to patch known security problems. You can set this to happen automatically too.
- **Don't open** email messages that look suspicious.
- **Don't click** on email attachments you weren't expecting. You don't know what they contain!

5. Common types of Virus

WORMS:

Usually a self-replicating malicious program, which attaches itself to, and becomes part of, another program.

Some worm viruses can remain self-contained and do not need to be part of another program to propagate themselves. They are often designed to communicate between computers to spread themselves more widely.

TROJANS:

Similar to a worm virus but generally does not replicate itself. Just like the Greek wooden horse, users mistake the Trojan for a useful or interesting program which they innocently download.



Fact Sheet

Once installed and run, Trojans can secretly open remote access channels over the Internet to hackers, relay passwords and credit card data or destroy your data.

There are also a much a wider range of virus types, which include "Polymorphic", "Stealth", "Slow", "Retro", "Multipartite", "Armoured", "Companion", "Phage" and "Revisiting" virus types.

6. Useful Links

www.symantec.com or
www.mcafeestore.com -
Web sites of two of the major anti-virus software companies: both give useful information on virus types and safety too.

Disclaimer: we have no commercial links with these companies or their products, and their appearance in this fact sheet is not an endorsement.