

Viruses and I don't mean the common cold.

By Jamie Grant [IT Guru solutions.](#)

One of the biggest threats to computers that are connected to the internet is Malware. In English this covers viruses, worms, Trojans, spyware and adware. I will explain what each category does and why they are a problem.

Viruses.

Viruses are defined as self replicating, that is code designed to cause trouble by replicating. They use the resources of the host computer to create new versions of themselves which can be spread through casual PC to PC contact via moving file over a network, floppy disc or CD/DVD.

Worms.

Worms are not dissimilar to viruses but their method of propagation is over a network. As the majority of PC's are now connected to networks it is very difficult to distinguish between them.

Viruses invade other applications while worms run as separate programs.

Trojan

The Trojan is possibly the nastiest version of malware, since it relies on the users trust to infect their PC. It poses as legitimate or wanted software and hides itself beneath innocuous looking code and lets the user install it. This is mainly found on Peer 2 peer network shares like Kazza. You think you have downloaded a program you want, however it installs fine but it also installs a Trojan. Once installed the Trojan is free to run riot on the PC!

Spyware and Adware

Spyware and adware focus on profit rather than damage. The mildest versions find demographic information to give you 'pop ups' that might be of interest to you, but are annoying and will slow your PC down but not damage it. The worst type are key loggers which will log all the information that you type, username, passwords, bank details and send it to a predetermined e-mail address where the writer can use it to break into your company or bank.

One of the most increasing uses of malware is for Distributed Denial of Service (DDoS) attacks. A web company is targeted and a ransom note is sent to that company to pay a ransom or be attacked by DDoS. If the company doesn't comply then the PC's with the malware installed (Zombies) are put to use by trying to access the companies web site. If you have 10,000 PC's trying to access a web site at the same time it will stop working! Nasty!

How do you protect your self?

It is very easy to protect yourself. Get an Anti-Virus program with anti-spyware modules. Any of the big companies have good products. Make sure you **keep them up to date** and make sure you subscribe to the update service. There are about 25 new viruses a day. A list of new virus descriptions are available at www.itguru.me.uk.

If you have a PC that is infected and you are having problems with it then it will be quicker and easier to re-format the hard drive and re-install the system than try to figure out how to remove malware yourself. What you will find is the anti-virus program will find the infection and delete that file, however as soon as you re-boot a dormant program will recreate the virus files. At the end of the day all that an anti virus package can do is to stop the virus from working, but the majority of the time it can't kill it completely.

Prevention is better than cure.