IS BIG BROTHER WATCHING YOU?

Surfing on the internet or www (world wide web) can deliver more than you would expect. The threat of virus attacks, spyware or mal-ware on computers is greater today than it has ever been. Whilst there are programmes that prevent or eradicate such infections, the code writers of this software are always playing a 'catch-up' game. They have to wait for a new threat to appear before they can write the preventative measure.

The 'Cyber terrorist', as the offenders are becoming known, are using more and more devious tactics to encourage us to allow malicious code onto our computers. They may send an e-mail as a survey, 'click here if you agree', or try to imitate a friend, hijack an existing e-mail address and forward a virus so it appears to come from someone you know. It has to be said, that generally, a virus has to be 'invited in'. But there are always exceptions to the rule. Some viruses or malicious codes simply prey on weak areas of the operating system, accessing through a known vulnerability. Again, these vulnerabilities are usually eradicated, but not before a lot of damage has been done to a lot of machines.

Some mal-ware gets onto your computer from simply visiting a web page or using P2P (peer to peer) sharing software (such as accessing music sharing sites). Again most, but not all, of these are presented as 'cookies', a small package of code which is placed on your computers hard drive. Most cookies are relatively harmless; they allow a website originator to record how often you visit their site and which pages you viewed. Helpful when they want to keep their website fresh & up to date. Other cookies, however, are not so harmless. These software packages can perform functions such as recording key strokes and forwarding this information to a third party. This is something you don't want to happen if you use your credit card, for instance, over the internet. Other codes allow adverts to 'pop-up' on your computer screen when a certain key combination is pressed. This can be quite embarrassing if a child is on the internet and a 'dubious' advert appears. Whilst some people recon that it is up to computer manufacturers/suppliers to install appropriate software onto new computers (it has to be said that most new computers do come with some form of anti-virus installed, even if only a limited time trial-before-buy version), the end user has the most responsibility. The 'Cyber terrorist' exists on the back of ignorance. They tantalize, invite, and hoodwink people into allowing them access to their machines. In a nutshell, you have to be constantly vigil. If you are not expecting an e-mail from, say, an infrequent friend; then ask yourself "Is this legitimate?"

Never, ever open an e-mail attachment from an unknown source before scanning for viruses (at least!). Always have up-to-date antivirus software installed. Look into having a firewall fitted (a software or hardware device that isolates you from the internet and helps to hide your presence). Microsoft have a rudimentary one installed in their XP operating system, but it may be worth considering a more intensive third party version.

Run spyware software on a regular basis, (typical examples are listed at the end of this article), this software helps to detect and remove spyware/ malware and operating system registry unauthorized alterations.

So, be vigilant, be 'untrusting', and beware at all times.

Happy surfing.

The software below is typical but not limited to those named.

Software firewall:
Zonealarm (www.zonelabs.com)

Spyware software:
Spybot (www.tucows.com/preview/310138.html) or Ad-aware (www.lavasoft.nu).

Don't forget up-to-date antivirus software (search on www.google.co.uk)

Steve Wright (stef@copywright.co.uk)