



Advice on Viruses and Spyware

Disclaimer:

This document is intended to provide basic information to help PC users to avoid system problems caused by malware on the Internet. Following the practices described may reduce your risks; however, no guarantees or warranties are offered or implied. The information is relevant to users of Windows 98SE, Windows Me, Windows 2000, Windows XP and Windows Vista only.

Document Version 2.2, 2007-09-14

Contents

- What is malware?..... 2**
- Avoiding picking up malware infections..... 2**
 - How do you get infected? 2*
 - Get yourself Web-wise 2*
 - Be wary of what you download from the web..... 2*
 - Be wary of all emails you receive 3*
- Protect Your Computer System..... 3**
 - Keep your system up-to-date 3*
 - Run an Anti-Virus (AV) software package..... 3*
 - Don't allow inbound connections from the Internet to your PC system(s)..... 4*
- If you think have an infection on your PC 5**
 - Warning signs of infection problems 5*
 - What to do if your system is infected 5*
- Why do people create malware? 6**
- Be alert and vigilant, but not paranoid..... 6**

What is malware?

The term *Virus* is used in everyday conversation to mean software that is bad for computers. However, technically a virus is only one type of such software; other types include *Trojan Horses*, *worms*, *backdoors* and *spyware*. The generic term used on the web for all of these is **malware**.

Avoiding picking up malware infections

How do you get infected?

There are basically two ways a computer system can become infected:

- An external attack from another computer breaches the defences of your computer and delivers malware.
 - This is analogous to burglary i.e. if your home doesn't have any door or window locks, or they don't work properly, or you don't set the locks on – an intruder will have an easier time getting in.
- Malware is delivered at the invitation of the user, i.e. via email or download from a web site.
 - The conman analogy applies here – you allow someone to have access to your home who betrays your trust.

Once infected, the malware on your system will try to carry out its own intended actions. It may also open up your system further to attack by disabling your defences and thus enabling and even inviting other intrusions.

Get yourself Web-wise

This is by far the most effective measure. It is analogous to how you need to be 'street-wise' to survive in other aspects of modern life:

- Most people are wise to everyday scams and threats such as unsolicited phone calls telling you you've won a prize in a competition you've never heard of, cold-calling salespersons on your doorstep, letters offering credit cards or 'low-cost' loans, TV adverts for debt consolidation, etc.
- We teach our children to become streetwise: don't accept gifts from strangers, never go off with someone you don't know no matter how plausible they sound, don't go alone to certain areas late at night etc.
- Assume 'No' is the right answer to 'pushy' activities whilst you are browsing the Internet, unless you are sure you know better.

Be wary of what you download from the web

- Browser toolbars, search enhancers, Internet download managers, pop-up killers, multimedia content decoders and line speed tweakers etc are typical web freebie offers that may result in delivering malware to your system. Even some (alleged) anti-malware programs are now known to include undesirable software.
- Never obtain software from "warez" sites or peer-to-peer (P2P) services like Kazaa. Get software from known, trusted sources only.
- Never open a file directly from a web site - always download and save it first to ensure that your AV software gets a chance to check it out.
- Watch for pop-up messages asking you to approve some seemingly innocuous action e.g. "Would you like to make <some name> your home page?", "Click here to install the ***FREE*** XYZ streaming media player". You may get more than you bargained for so unless you are sure - just say "No".

- If you want to use P2P file sharing, choose a 'clean' service - see here: <http://www.spywareinfo.com/articles/p2p/> for information on what is clean or otherwise. Many P2P file sharing services require you to install their client software which often includes malware infections.
- P2P services often offer attractive downloads such as pirated software, film clips and music files which may contain malware in disguise. - even 'clean' P2P services are specifically targetted by malware, to assist them in spreading.

Be wary of all emails you receive

- Treat email with the same suspicion you that would junk paper mail, unsolicited phone calls and uninvited door-to-door callers.
 - There's no such thing as a free lunch.
 - If it looks too good to be true, it almost certainly is.
- Recent Internet worms generate forged emails using addresses 'harvested' from compromised systems. That means you could receive a mail apparently from someone you know, with a plausible subject and content, aimed at inducing you to lower your guard and click on its malicious attachment.
 - Some types of email-borne malware are particularly sneaky, posing as an official-looking announcement from a respected organisation e.g.
 - A security patch for your system from a (spurious) Microsoft source address
 - An alert about your email account, apparently from your Internet Service Provider (ISP).
 - A software update apparently from your anti-virus software provider.
- If, after verifying the source of an email with an attachment, you decide to go ahead and open it, always save the attachment to your local disk first to ensure that your AV software gets a chance to check it.

Protect Your Computer System

Keep your system up-to-date

- Keep your operating system and Internet-related programs (browser, email client etc) patched with the latest security-related fixes.
- For most of us that means using the www.update.microsoft.com web site to keep your system up-to-date with the latest "Critical Updates and Service Packs" from Microsoft.
- Automatic updating is available from Microsoft for critical updates to Windows.
- The Java runtime software on your system should be kept up-to-date, via downloads from www.java.com .

Run an Anti-Virus (AV) software package

- Most new PCs are delivered with an AV package installed, e.g. Norton, McAfee, etc. However, be aware that it will usually be time-limited, typically 60 or 90 days, after which you are asked to pay a subscription (typically £30 or so per annum) to allow you to receive further updates. If you don't subscribe, the package will usually continue to operate but with out-of-date virus data - which makes it worthless within a few days. An alternative is to use a freeware anti-virus package, such as AVG from Grisoft.

- Ensure you enable the continuous real-time protection capability of your chosen anti-virus software - this means that every file you open will be checked.
- Keep your AV software and virus profile database up-to-date by checking for updates regularly because new viruses are appearing all the time. Check for updates at least daily, more often if you use the Internet extensively.
- Run regular full AV scans on your system - preferably daily, but at least weekly - to catch any new virus that may have slipped through the net.

NOTE:

- Most anti-virus packages can automate the regular update and scanning functions, if you set the appropriate configuration options.
- It is tempting to think that running more than one anti-virus software package will reduce your risk of infection even further: however, that is not advisable because AV packages tend to interact adversely, causing system instability, lock-ups and crashes.

Don't allow inbound connections from the Internet to your PC system(s)

- If your system is directly connected to the Internet (e.g. via a dial-up modem or a broadband modem), check your configuration and make sure that you are not offering services to the Internet unintentionally. In particular, avoid offering file and print services.
- If you aren't sure, run a software firewall package configured to block inbound connections. Windows XP and Vista have this capability built in [Windows Firewall], but you need to make sure it is switched on for your Internet connection.
- If you have two or more PCs connected together in a local area network (LAN), it is preferable to connect your LAN to the Internet via a hardware router device and to enable its firewall capability.
- Set your Microsoft Internet Explorer and Outlook Express security settings correctly:
 - Microsoft's advice on security settings to avoid problems, including step-by-step instructions, can be found here: <http://www.microsoft.com/security/incident/settings.msp>
- Be wary of virus warnings you may receive via email; there are many hoaxes around:
 - Forwarding a hoax virus warning fulfils the intent of the perpetrator - to clog up network links and email systems with unnecessary messages.
 - Don't follow any instructions to take action on your own system until you have checked out the advice - a recent hoax led to thousands of people causing self-inflicted damage to their systems by deleting perfectly innocent files.
 - Software vendors do not send out patches in email attachments - do NOT click such an attachment, it is almost certainly malware.
 - You can check out a suspected hoax at the <http://hoaxbusters.ciac.org/> web site.
- Fixes for Windows security problems *should* be downloaded and installed as soon as possible. But only get them directly from a Microsoft.com web site, never from an email attachment or any other web site.

If you think have an infection on your PC

Warning signs of infection problems

There is often no unique warning sign, usually a combination of issues such as:

- Alerts from anti-virus software.
- Markedly slower start-up of the computer.
- Sluggishness, instability and lock-ups in general use.
- Home page of your web browser is changed and you cannot reset it.
- Search requests are redirected to a different search site.
- Pop-up messages occurring randomly, i.e. not linked to a user action.
- Anti-virus software no longer working correctly.
- System hanging during shut-down.

What to do if your system is infected

If, despite your best efforts, you still manage get a malware infection on your system:

- **Don't panic!** Ill-considered recovery attempts in the heat of the moment may do more harm than good.
- Don't assume you need to reformat and reload your system - in most cases it is possible to clean a system without any loss of user data.
- Isolate a suspected PC: disconnect it from the Internet and from your local area network (LAN), to reduce the risk of it spreading infections to other systems or of picking up more infections [malware often opens 'backdoors' into your PC].
- Run a full anti-virus scan of your system. This may clean up the problem, but bear in mind that the main function of an anti-virus package is to prevent an infection by detecting it before it becomes active: if an infection is detected after it has become active, your AV software may not be able to clean it up: in such cases specialist tools will be needed.
- If your AV software is unable to clean up the infection, seek professional guidance to help plan and implement the recovery.
- The key to efficient and effective recovery is to be able to positively identify the specific infection(s). So it is important that you take steps to help with the diagnosis process:
 - DO NOT DELETE any infected files at this stage, quarantining is preferable if available.
 - Take careful note of the alert messages raised by your antivirus software.
 - Note any unusual symptoms and error messages that preceded the infection.

Why do people create malware?

This is the question I get asked most frequently by customers who have suffered malware-related problems. The motivations behind perpetrators of malware are thought to include:

- Commercial
 - Con-trick: e.g. inducing the user to pay for a removal tool to rid their PC of the malware infection.
 - Hi-jacking the user's web browser can enable advertising content to be foisted on the user, e.g. by overriding the user's home page, displaying pop-up advertising windows and modifying search results.
 - A compromised system can be used to host software that can act as an untraceable relay of spam emails or a 'Denial of Service' attacker.
 - A compromised system can be made to behave as a 'zombie' web site visitor, helping to click up 'hits' on a commercial website, hence earning money for the perpetrator.
- Peer-group kudos - Internet geeks displaying their 'skills' to their peers in the user communities they inhabit.
- Political or other belief-related motives - targeted actions against specific user groups, e.g. particular software or computer system users, certain countries, religions etc.

Be alert and vigilant, but not paranoid

Having read thus far you may be feeling that the risks of the Internet are too great for you. However, if you take a little time to understand the issues and prepare your defences, you can use it safely. As stated earlier, the key factor is to become Web-wise.

Bear in mind also that:

- Just because your PC doesn't behave as you expect, don't immediately leap to the conclusion you've caught a virus.
- Viruses aren't generally as rife or disruptive as the press sometimes portray.
- The sleazier areas of the Internet pose a higher risk (obviously), so tread carefully.
- Reputable Antivirus packages and firewalls generally do a good job.



Call **BRG Computer Services** **07817 630 362**
or via email: **mail@BRGservices.co.uk**
Microsoft | Partner Programme - Registered Member