

Systems and Software Safe PC Setup - Malware

Overview

Computers require more complicated protection than they did just a few years ago. In the 1980s, the only threat to a computer was from a floppy disk infected with a virus. Today, with PCs connected to the internet 24-7 via fast broadband links, virus attacks can come in many forms and spread across the globe in seconds.

Malware is the name for software designed to infiltrate or damage a computer system without the owner's informed consent. This includes adaware, trojan horses, viruses, worms, spyware, and targeted phishing attacks.

Vulnerabilities

It has been known for commercial CD-ROMs to be infected with malware, but it is very rare. Attacks are more common from the following sources:

- 1) Internet connection
- 2) USB Pen Drives
- 3) Email
- 4) Instant Messenger
- 5) Wireless (Wi-fi) connection
- 6) Browsing web sites (click-click-what-was-that...)
- 7) Downloaded *Free* Software or *Pirated* Software
- 8) Floppy disks!

Types

The first wave of virus attacks were mildly annoying, and generally harmless. There were a few that corrupted or destroyed files, but these were the exception.

The second wave of attacks were designed to be destructive and caused large financial losses to corporations that had to be locked down until they were *cleaned*.

The latest forms of attack are much more dangerous. Infected PCs continue to operate without any visible change. The malware sits hidden on the PC, secretly monitoring the web sites visited or worse, every key typed. In the latter case, the keystrokes can reveal usernames and passwords for online banking.

What Software Packages

Broadband access to the internet offers a great opportunity to download and try free software. Resist. Ask the question why are they offering free software, what are they going to achieve?

The majority of free software is probably safe, with free versions of the tool used to entice users to purchase the *Professional* versions. Others bundle advertising. I.e. Incredimail is a free email package, but they append advertising to the end of every email sent.

The following lists the basic minimum protection for a PC. The software packages listed are examples of the industry leaders.

- Firewall – Zone Alarm Pro (www.zonelabs.com)
- Spyware - Spyware Doctor (www.pctools.com)
- Virus - Norton Anti Virus (www.symantec.com)
- Virus – Kaspersky (<http://www.kaspersky.co.uk>)

One of the differences between the Free and Professional versions, is the ability to detect Spyware as it occurs. It is worth paying the money to stop the Malware attack when it happens rather than waiting for a daily scan to catch it.

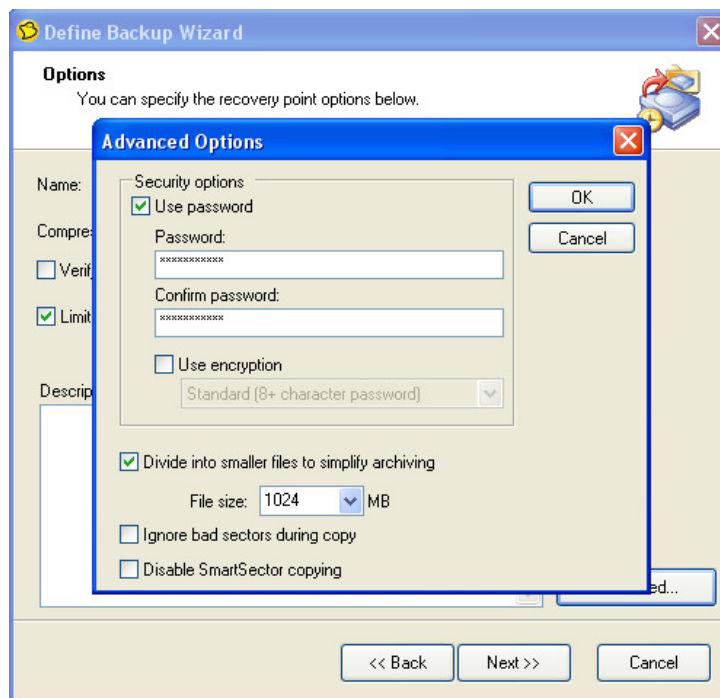
There is overlap with the coverage offered by these packages. Zone Alarm also includes Spyware protection and Norton now includes firewall protection.

Until recently it was worth buying software that is the company's core skill rather than relying on an all inclusive package. This has now changed and the complexity of having multiple packages offering the same service causes system setup problems. Choose one company and buy their all inclusive package.

New PCs often come bundled with 30, 60 or 90-day trial versions of software like MacAfee. It is possible, but not easy, to remove or disable the trial software and install your own, so the choice of software may have already been decided.

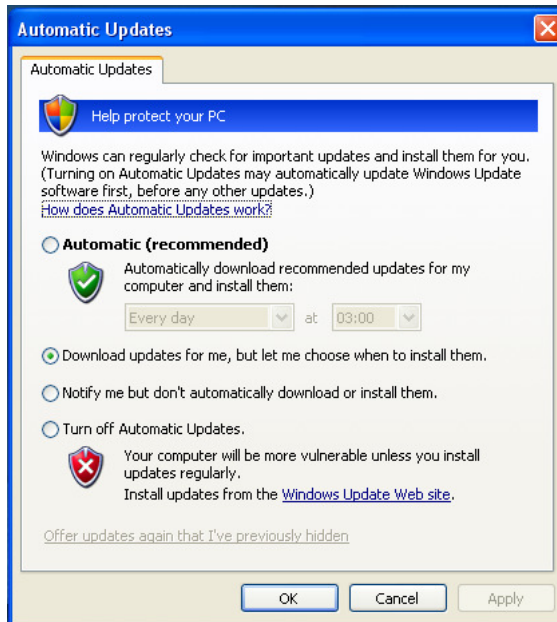
Good Practice

- Install Symantec's Ghost backup software, and configure for weekly full backups to an external USB hard disk, and nightly delta changes. Choose the option to break up the files to a size that can be burnt onto a DVD disk. This is in the Advanced Options. Selecting a size of 1024 ensures that it can be burnt to one or more DVDs. It is also best to reduce the chance of the backups being misused by using a memorable password.

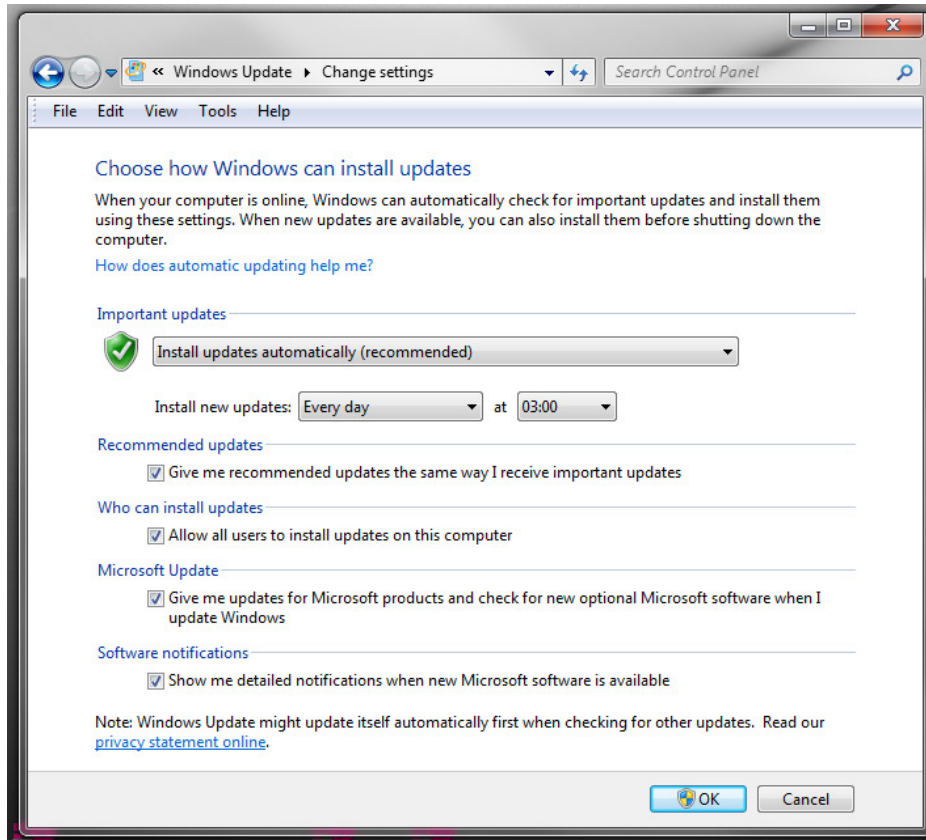


- Periodically burn a DVD copy of the Ghost backup. A Malware infection could be hidden on the PC for several months. A backup from before the infection allows the system to be restored back to a safe point. Individual files can be restored from the latest backup if they are known to be clean.
- Use Google's Chrome or Mozilla Firefox instead of Internet Explorer. Malware developers will concentrate on attacking Microsoft products because they will get the biggest number of people and because it is Microsoft!

- Enable Windows to check for updates. This is enabled in the Security Setting application in the Control Panel. Select the “Download updates, but let me choose when to install them” option.



Example screen for Windows XP



Example screen for Windows 7

- Configure Zone Alarm, Spyware Doctor, Norton Antivirus etc to check for updates at 1am every day when your PC is idle. Schedule the scans to run after the updates. I.e. 2am.
- Configure Norton AntiVirus to check sent emails as well as received emails.
- Only open emails with attachments if the person sending them is known, and the attachment is expected. If not, use SHIFT-Delete to permanently delete the email. I.e. Shift key and Delete key at the same time.
- In general, never divulge any personal details in response to an email, either by replying directly or by following an embedded link to a web site. This may appear obvious, but the fraudsters are becoming very clever. One of the latest scams is called *Phishing*. For more details see [Identity Theft \(Phishing\)](#).
- Treat USB memory sticks like Floppy Disks and perform a virus scan on them before opening any files. Right clicking on the disk name from Windows Explorer will give you the option of running an anti virus scan.
- Parental Control software prevents access to suspect web sites that contain Malware. One example is IprotectYou from <http://www.softforyou.com/>.
- Web sites and software packages often have so many NEXT and CONTINUE buttons to press; it is easy to just click away. Slow down and read them carefully. The safest way to close a web page is the cross in the top right corner. CANCEL buttons in the window may do something completely different...