

Home & SOHO Users Guide to PC Security



Today, computer security is of the utmost importance and the software required to keep your computer safe has increased to such a degree that your best option is to have a Broadband Internet Connection. Anything less requires great patience and lots of time.

Home & SOHO Users Guide to PC Security:

The following programs and processes are highly recommended for the protection of your computer(s). In choosing programs we have tried to keep the cost of the software down to an absolute minimum. However, circumstances sometimes demand a commercial strength program to remove some of the more insidious infections.

Today, no-one should be using Windows 95/98/98SE/ME/NT, because they are unsecured Operating Systems (OS) and as such are no-longer supported by Microsoft however, we have included information on how to semi-protect these OS, because some users can not afford the upgrade, but be warned you should not use these OS online or for any financial matters.

Please read any and all accompanying manuals or help files before installing any software.

Today there are several things one must do before using a new computer, namely you must configure and setup an Internet Connection and to do this several pieces of information are required. Information gathered from your ISP (Internet Service Provider).

- 1) Your email address: i.e. john.smith@myisp.com.au or john.smith@gmail.com
- 2) A user name – which in most instance is your full email address or just the name part i.e. john.smith (Do not forget the dot).
- 3) Set the mail protocols i.e. POP and SMTP, which are ISP dependant. For example, if your ISP is Bigpond your POP & SMTP settings are the same i.e. mail.bigpond.com However, if you are with Internet Express they are set as follows: pop3.ix.net.au & smtp.ix.net.au
- 4) The next thing to put in your ISP's National Telephone number, which for Bigpond is 0198 308 888.

Once all these protocols have been set you should be able to connect to the Internet, and once this has been completed you MUST update you systems software.

- 1) Updates for both your Anti-Virus and Windows Operating System (all critical updates) must be downloaded and installed, before you attempt to do anything else over the Internet.
- 2) Next setup, run all your Anti-Spyware services and remove any spyware you find.
- 3) Using your Anti-Virus program do a complete scan of your Hard Drive.
- 4) Check for any critical updates for your installed programs including programs from other software producers like Adobe, Corel, IBM, Real etc.

At this point we should also mention that in some instances, like when registering your software online, you may be asked for your **Microsoft Passport login and password**. If you do not have one, you will be shown how to obtain one then-and-there, all of which will be confirmed by email. Now, your system should be clean and fully protected i.e. PC Security is up-to-date, and now you can install additional programs on to your computer.

Recommended Programs & Processes

Anti-Virus

For individuals we recommend AVG Free Edition (www.grisoft.com), or Avast Home Edition (www.avast.com), both of which, are free for home users only. For commercial, non-profit, educational or government users the following are available: Computer Associates (CA), McAfee Internet Security Suite, Norton (Symantec) Internet Security, Trend Micro PC-Cillin Internet Security, Zone Alarm Security Suite or one of the many the commercial options from AVG and Avast.

Firewall

Our recommendation is Zone Alarm Free Edition for Windows 2000/XP/Vista or Jetico Personal Firewall (www.jetico.com) for Windows 98/98SE/ME/NT, and for commercial, non-profit, educational or government users select from one of the about mention commercial suites or the individual Firewall program or Microsoft's own Firewall.

Anti-Spyware

Please note: Only (1) anti-virus program and only (1) firewall program can be operational at any one time on any computer otherwise your system will experience operational difficulties i.e. crashes. However, when it comes to using Anti-Spyware programs one is not enough, it takes several programs to ensure your computer is free from infections. Today, Spyware infections are consider more invasive and can cause more damage that viruses. The programs which we recommend you consider come in two types 1) Preventative and 2) Removal. Preventative programs are commercial programs and two of the very best are Process Guard (www.diamondcs.com.au/processguard/), an Australian company (US\$30) and Spyware Blaster (www.javacoolsoftware.com), which cost only US\$9.95/year for updates.

Removal programs include: Lavasoft's Ad-Aware (www.lavasoft.de), Safe Networking's Spybot Search & Destroy (www.safernetworking.org) and Microsoft's Windows Defender (www.microsoft.com). Also, one of the very best in this category is Spyware Doctor (www.pctools.com/en/) a commercial program its strengths are such, its well worth the investment (US\$30). At the end of this pamphlet you will find instructions on how to best configure Ad-aware and Spybot for maximum protection of your computer.

Back-up

It is one of the most important security measures one can preform, but it is the one that most people neglect. If your data is important, please get in to the habit of backing-up your files on to removable media, such as, CD-R/RW or DVD±R/RW or some other removable media like a tape or an external hard drive or even Zip disks. Once you have your data safely recorder to external media please store back-ups off-sight. To loose your data the worst case scenario could be bankruptcy.

Windows Updates

All the above will account for nothing if you neglect to keep your Operating System (OS) patched and up-to-date by downloading and installing the latest critical and security patches from Microsoft. Microsoft updates are released or made available on the second Tuesday of each month, American time. Meaning, in Australia you should check for these updates, on the second Wednesday of each month. Forget this process and you are truly in trouble! The size (number of Megabytes) and the time it takes to download these updates will all depend upon what programs you have installed on your computer and your Internet service.

Other Precautions

The reason why Microsoft is targeted so often is because they are the biggest software developers in the world. If software terrorists (crackers/hackers) targeted the smaller software developers they would not get the notoriety they seek. This means Microsoft are always on their guard to prevent the destruction of your/their software, but like the dog chasing its tail Microsoft and other providers of Security Software are always playing catch-up. The two programs besides the Operating System itself, which come in for most attacks by these software terrorists (crackers/hackers) are Microsoft's Browser, Internet Explorer and Microsoft's email client Outlook Express (known as Windows Mail in Vista). At this moment in time, if you wish to have better protection from infections experts suggest NOT using Internet Explorer or Outlook Express, but USE the Mozilla Web-Browser FireFox and the Mozilla Email-Client Thunderbird, both of which can be downloaded and install onto your computer from www.mozilla.com. **DO NOT** try and remove either Internet Explorer or Outlook Express (Windows Mail), because you will damage the Operating System. Also, Windows Updates can only be sourced and downloaded using Microsoft's Internet Explorer. No other browser can preform this task. Please take note of this warning.

Email

DO NOT open any unsolicited email messages from people or companies you do not know, delete them immediately. Remember, curiosity may never kill your cat, but it may kill your computer, and it could lead to bankruptcy. Above all – **DO NOT** provide your ID or Password to anyone online. Banks and or Financial Institutes (including eBay, PayPal and the like) will never ask you to check or to confirm such information in an email. Also, you can employ a SPAM Filter to remove junk mail, and one of the very best is an Australia product SPAMbayes (<http://spambayes.sourceforge.net>).

Ignore the above warnings at your own peril!

In Summary

Windows Updates – check and apply updates each and every month

Back-up – all your import data to Zip/CD/DVD or floppies

Anti-Virus – AVG Free Edition or Avast Home Edition (Windows 98/98SE/ME/2K/XP/Vista)

Firewall: - Jetico Personal Firewall for Windows 98/98SE/ME/NT and Zone Alarm Free Edition for Windows 2K/XP/Vista.

Anti-Spyware

- Ad-Aware Personal (Windows 98/98SE/ME/2K/XP)
- Spybot Search & Destroy (Windows 98/98SE/ME/2K/XP)
- Process Guard (recommended for very experienced users only)
- Spyware Blaster (Windows 98/98SE/ME/2K/XP)
- Windows Defender (Windows XP/Vista)
- Spyware Doctor (Windows 98/98SE/ME/2K/XP)

Others Precautions

Use the more secured FireFox Web-Browser (Windows 98/98SE/ME/2K/XP/Vista) and Thunderbird Email Client (Windows 98/98SE/ME/2K/XP/Vista).

How to configure two of the best Anti-Spyware Programs: Spybot and Ad-Aware

How to best configure Spybot-Search & Destroy

Boost Internet Explorer's security by adjusting Spybot's settings. First, click the Immunize button on the left, tick "Enable Permanent Blocking of Bad Addresses in Internet Explorer" and tick the Immunize button at the top.

To enable scheduled scans go to Mode → Advance mode → Settings → Scheduler. Click the Add button and then "Edit" to adjust the scheduling options.

Click Tools and, in the right-hand pane, tick all the tools. However, doing so does not activate the tools; it merely adds them to the list of tools you can use and configure. To turn on Spybot's real-time monitor, click Resident in the left-hand pane and tick both "Resident Protection Status" options.

If you like to beef up IE security even more, click "IE Tweak" and "Lock Host File" and "Lock IE Start Page".

How to best configure Lavasoft's Ad-Aware

Click "Scan Now", select "Use Custom Scanning Options" and click Customize.

Enable "Scan within archives", "Scan active processes", "Scan Registry", "Deep-scan Registry", "Scan my IE Favourites for banned URLs" and "Scan my Hosts file".

In the same dialog, click "Select drives & folders to scan" and ensure each of your hard drives are selected.

Click the Tweak button in the same dialog. Then, in the "Scanning Engine" section, tick "Unload recognized processes & modules during scan" and "Scan Registry for all users". In the "Cleaning Engine" section, tick "Always try to unload modules before deletion", "During removal unload explorer and IE if necessary", "Let Windows remove files in use at next reboot" and "Delete quarantined objects after restoring". Click Proceed to activate these options and then click Next to start the scan.

Simple House-Keeping

There are several things you can do to help protect your computer and have it running as efficiently as possible like:

- ❖ DO NOT install software programs just because you can or because they are free!
- ❖ Every so often run **Disk Defragmenter** (Accessories → System Tools) this will reorganise your files on the Hard-Drive into an orderly manner and speed-up access.
- ❖ Every so often run **Disk Cleanup** to remove all unnecessary files (TMP - temporary files) from your system. Every time you download and install or uninstall software some temporary files are left behind even some compressed parts of the installed or uninstalled program are also left behind and by doing a Disk Cleanup (Accessories → System Tools) you remove this left-over rubbish.

- ❖ To help with Backup try and organise all you data under the one main folder. This simplifies things when it comes to doing a backup to Zip/CD/DVD or to Floppies. My Documents/Documents (Vista) are the default folders the Operating System and your installed programs like Word/Excel use as the default location when seeking to open or to save data. In other word Microsoft has tried to keep things simple when it comes to finding and storing data on your computer so, follow their lead!

How to Spot an Infection(s)

Some common signs of infection are:

- An increasingly sluggish response from your computer
- Browser windows opening automatically when you start Windows
- Pop-up windows appearing constantly when you are online
- Your Browser's Home Page or default search engine being changed
- Frequent Browser and program crashes
- New toolbars or bookmarks appearing in your Browser
- Sites added to your Browser's Trusted Sites or exception list
- Unpredictable Browser behaviour
- Blocked access to sites, especially anti-virus or anti-spyware sites
- New programs in the system tray

As well as Anti-Virus, Anti-Spyware, and Firewall software you could also investigate:

BHODemon	www.spywareinfo.com/downloads/bhod
CoolWWWSearch.SmartKiller	www.safer-networking.org/minifiles.html
CWShredder	www.trendmicro.com/ftp/products/online-tools/cwshredder.exe
HijackThis	www.spywareinfo.com/~merijn/downloads.html
IE-SPYAD or IE-SPYAD 2	http://netfiles.uiuc.edu/ehowes/www/resource.htm
Itty Bitty Process Manager	www.spywareinfo.com/~merijn/downloads.html
LSP-Fix	www.cexxorg/lspfix.htm
Process Explorer	www.microsoft.com/technet/sysinternals/default.msp
SpywareBlaster	www.javacoolsoftware.com/spywareblaster.html
SpywareGuard	www.javacoolsoftware.com/spywareguard.html
Startup Inspector	www.windowsstartup.com
Startup monitor	www.windowsstartup.com
ToolbarCop	http://windowsxp.mvps.org/toolbarcop.htm
Winsock XP Fix	www.spychecker.com/program/winsockxpfix.html

Also, check out all the tools available at www.spywareinfo.com/~merijn/downloads.html for some program specific tools.

In Addition, to all the above listed Web-Sites there is one other which we have found over the years to be most helpful, Malware Help (www.malwarehelp.org/).

Maximum PC-Security Toolkit for a Home/SOHO PC

1. Anti-Virus Software (AVG Free Version)
2. Zone Alarm Free Firewall in conjunction with Windows own Firewall
3. Spybot Search & Destroy (Freeware)
4. Lavasoft's Ad-Aware (Commercial or Freeware)
5. Windows Defender (Microsoft's own Anti-Spyware - Freeware)
6. Spyware Blaster (commercial software)

7. Spyware Doctor (commercial software)
8. Process Guard (commercial software)
9. Microsoft Baseline Security Analyser (Freeware)
10. Spambayes (Freeware – junk mail removal)
11. FireFox (Freeware)
12. Thunderbird (Freeware)

Stop the Regeneration Process (experienced users only)

Some Spyware can run a background process to watch whether you attempt to uninstall it. As soon as you delete its executable file, it restarts itself from another copy. To deal with this behaviour, you may need to do some side-by-side process-stopping and file deletion.

1. Open the folder where the suspect program resides and resize the window, so it occupies only a small portion of your desktop.
2. Press Ctrl-Alt-Delete to open the Task Manager, click the Processes tab, locate the Spyware process in the list and click it.
3. Click 'End Process' to halt the process and immediately delete the associated executable file displayed in the file window you have open. You may need to repeat this step a couple of times to ensure the process and to ensure the file does not regenerate. Watch for regenerated file using the same name with a number appended and delete it, too.

You can simplify this process by using either the Itty Bitty Process Manager (IBPM - A standalone version of the little process manager included in HijackThis) or Process Explorer. Both are freeware. IBPM is quick and dirty: Process Explorer is comprehensive. By right-clicking a process and selecting Properties in Process Explorer, you can immediately see which executable is associated with which process.

Technical Terms

- **Browser hijack** - The alteration of your browser's settings so you are redirected to Web Sites of the Hijacker's choosing.
- **Drive-by download** - A download that occurs without your consent. Such downloads are often initiated by pop-ups or deceptive links on Web sites or in dialogue boxes.
- **Keylogger** - A program or hardware device that records everything you type on the keyboard.
- **Malware/scumware** - Generic terms for threats such as spyware, viruses, worms, and Trojans. Also known as PUPs (potentially unwanted programs) and PUS (potentially unsafe software).
- **Phishing** - Email that purports to come from one source - usually a financial institution - but which is designed to lure to a fake site, where you are then asked to enter your username and password or account details.
- **Spoofing** - Mimicking a Web site or Web address in order to fool visitors into thinking they're on a legitimate site. Email can also be spoofed, so that it appears to come from someone other than the actual sender.
- **Ransomware** - A new form of spyware that requires you to pay a fee for a key (code) to unlock your computer before it starts deleting files off your computer. However, there is no guarantee once you pay the Ransom the problem will not return at some later date.

Timetable

You may have notice that today PC-Security experts are suggesting that you run all your security programs on a daily bases i.e. before and after you start and complete your day's work. Therefore, set aside at least 30 minutes (or more) at the beginning and end of each day to do this very important and very necessary procedure.

Diagnostic Tools

When a computer is not behaving it can be suffering from any of a dozen things, such as corrupt files, a bad application, or even a moribund CMOS battery. An indication of something is wrong with your computer are: computer freezes, odd warning messages or auto-rebooting just to name a few.

The following programs can assist you in keeping your computer operating as its best, if and only if, you have applied the necessary security options and programs as outlined in this pamphlet.

1) **CleanCache** 3.5 (www.buttuglysoftware.com): This free program removes Window's "temporary files, Office's most recently used history and browser cache files. We prefer judicious cleaning, so we use the "Clean Checked Item" option rather than "Run Complete Cleanup". One grip: CleanCache has a setting to preserve useful cookies, but even with it turned on, you will have to click "Remember my Address and Password" again on many of the websites you visit. Note that CleanCache requires Microsoft's .Net Framework.

2) **FileMon** (by Sysinternals): This free program gives you a real-time view of every running program and lets you know what its doing, recording and time-stamping each action an application takes; watch for a specific program's behaviour just before a malfunction i.e. freeze.

3) **RegMon** (by Sysinternals): Also free, does the same as FileMon, but for the Registry.

4) **Process Explorer** (by Sysinternals: Again free, and like FileMon and RegMon Process Explorer does the dirty work on Windows processes.

The above four (4) diagnostic programs will help keep your computer working efficiently if you are prepared to learn how each one works.

Please note: Sysinternals is a wholly owned subsidiary of Microsoft Corporation. When using the sysinternals software you may need to deactivate the Protection mode in ProcessGuard. As stated before ProcessGuard is only recommended for use by experienced users. If you do not disable Protection in ProcessGuard, the sysinternals software may fail to run. To see all the tools offered by Sysinternals go to their new website now locate within the Microsoft organisation (www.microsoft.com/technet/sysinternals/default.aspx).