

Firewalls

Firewalls prevent others from accessing your PC. The Windows firewall (available from Windows XP SP2 onwards) is fine, but, hardware firewalls, found in routers, are much better.

USB modems have *no* firewall. If you use such a device, or if you use public wireless networks, upgrade to a third-party firewall.

Spam

Spam is unauthorised bulk email, sent out to achieve sales or malicious results. It accounts for more than 80% of email traffic To cut down on spam:



- 1 Don't use a simple email address. Some spammers will try common or short email names. Instead of your given name or surname (e.g., joe@myisp.com.au), use parts of your surname, or include numbers (e.g., joeb@myisp.com.au).
- 2 Most webmail sites have good spam filtering - use it!
- 3 If your ISP's email service has a spam filtering facility, sign up for it.
- 4 Spammers search the web for email addresses. If you must have your email online, post it as an image.
- 5 **Never, ever** respond to spam. A response will add your address to a spam list, which means more spam.
- 6 Use an email program that includes a spam filter, or get a third-party spam filter for your email program.
- 7 Be on the lookout for scams asking you to enter your personal details onto a website, even if they appear to be from your bank or a service provider.
- 8 If you get repeated unwanted email from a firm, they may be breaking anti-spam laws:
 - a) If there is an unsubscribe link, use it.
 - b) If not, or if emails keep coming, send the company an email asking to be removed from their mailing list.
 - c) If that doesn't work, report the company at www.acma.gov.au. Look for the "Report Spam" link.

Also, don't forward unverified emails about new viruses, sick people, etc.! Find a unique phrase in the email and paste it into a search engine. If you get results from sites like BreaktheChain or Hoaxbusters, it's probably a hoax!

Excellent free software exists to help many of these tasks:
[go to \[netsensecomputers.com.au/services/freeware.html\]\(http://netsensecomputers.com.au/services/freeware.html\)](http://netsensecomputers.com.au/services/freeware.html)

Tidy Your Disk

Every few months, tidy up your hard disk:

- 1 Go to Start > Accessories > System Tools > Disk Cleanup. Select the drive you want to clean.
- 2 When the utility has finished inspecting the disk, select the items you no longer want. Remove at least 'Temporary Internet Files', 'Recycle Bin' and 'Temporary Files'.
- 3 Go to Start > Accessories > System Tools > Disk Defragmenter. Select the drive you want to clean. Click Analyze.
- 4 Follow the recommendations of the analysis. Don't defragment more than monthly.

Delete Unwanted Programs

Unused programs clutter up your hard disk and may run background processes that use memory. Regularly check for and remove such programs:

- 1 Go to Start > Programs; check each unwanted program. If an Uninstall option exists, use it.
- 2 Go to Start > Control Panel > Add or Remove Programs. Search the list for unwanted programs, and click the remove button.
- 3 If you are not sure what it is, **leave it**.

Deleting menu items will not uninstall a program.

If you're not sure what
you're doing - it may be better to I
eave it to experts
(like us 😊)!



Ph: (02) 4233 2285; Fax: (02) 4233 2781
79 Barney St, Kiama 2533
info@netsensecomputers.com.au
www.netsensecomputers.com.au



Tips for Reducing Computing Costs

There is much you can do to minimise the costs
of your computing activities.

Viruses

Viruses can render your computer useless and corrupt your files. So scan for viruses at least weekly. Some programs also scan emails and files as they are opened or closed. Systems that use active malware defences are even better.

To prevent email virus infection:

- 1 Don't open attachments or click links in emails from strangers.
- 2 Don't open an attachment if it's unexpected, doesn't "look right", or is an EXE, COM, PIF, SCR file.
- 3 Consider using alternatives to Outlook or Outlook Express - they are not bad programs, but *are* the target for many email viruses.

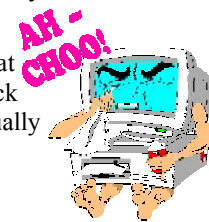
Any program can be attacked (e.g., Outlook & Outlook Express, Internet Explorer, Office and Acrobat), and when it is in common use, a good alternative may improve security.

To prevent an infection from a website:

- 1 If your security software has a browser "plug-in", enable it. Alternatively (or additionally) install "Web of Trust" (www.mywot.com); to visually rate websites before you visit them.
- 2 If a web-page opens asking you to download a file you didn't ask for - **don't**.
- 3 If a web-page displays a warning and asks you to click on a button to fix problems or download security software, **don't**.

If you download files, use a downloader that checks files with your virus-scanner, or check the file with your scanner manually (usually right-clicking the file allows this).

If your ISP offers virus filtering, use it.



Updates

Microsoft releases updates to fix flaws in its software. It's best to install them automatically; if that fails, you can also do it manually:

- 1 Click on Start > Programs > All Programs > Windows Update.
- 2 Make sure all high priority updates are installed. If not, install them!
- 3 Switch to Microsoft Update to include updates for other Microsoft products (e.g., Office). Start Windows Update from Programs > Accessories, then choose the upgrade option.

Other software updates to ensure you install are updates to Security and Internet software.

Remove Unwanted Startups

Many programs install utilities that start at boot, some of which you will not need. Some software supplied with digital cameras, MP3 players and mobile phones is completely unnecessary, as the operating system provides similar. These programs slow booting, slow use, and may conflict with other programs causing instability:

- 1 Identify each item (they often have icons in the system tray). Identify those you want to retain (e.g., anti-virus software).
- 2 Try clicking or right-clicking on the icon to find a properties or configuration option. Look for a ticked checkbox that says something like "Start automatically with Windows". Untick it and it should not restart at the next boot.
- 3 Go to Start Menu > Run. Type "msconfig" and hit Enter. Click the Startup tab and uncheck any items you can positively identify that don't need to run when your computer starts up, and hit OK. For a more complete analysis, contact us.
- 4 If you are not sure what it is, *leave it*.

Rebooting

- 1 When software freezes or starts popping up error messages, close it down and restart it.
- 2 If you can't, hit **Ctrl+Alt+Del** and choose **Task Manager**. Click on **Applications**, select the problem program, and click **End Task**. Close Task Manager and restart the program.
- 3 If this doesn't work, reboot your computer.

If you can't connect to the Internet, power cycle the router and/or modem (turn off, wait, then turn on). If your printer or scanner stops working for no apparent reason, power cycle it. If using a USB modem, stop the software, remove the modem, wait around 30 seconds, then reinsert and restart the software.

Backing Up

Backup your key files regularly. DVDs, USB memory sticks or hard drives are both cost-effective and simple ways to do this.

The simplest way (if you have plenty of space) is to back-up your entire personal folder. You can do this manually or automate it.

If you have limited space, you can select the most appropriate information from your personal folder - "My Documents" will get most of your files, but remember that some programs store their files in special folders. Check for all programs you use where they store their files.

Don't, however, keep your only copy of files on memory sticks. In general, their value is in their low cost, not their long-term reliability.

Malware

Malware is malicious software.

Adware displays advertisements during use of free software. It is *usually* benign, but annoying. Spyware installs with useful software, but reports your Internet activity (or other details) for malicious use. Scareware is scam software sold using unethical practices causing shock, anxiety or fear. Some forms of spyware and adware also use these tactics.

Malware also uses your memory, hard drive space and Internet connection, and may slow computers or cause them to crash.

Use an up-to-date Malware system (or an anti-virus system that includes Malware protection) to protect your system.

Downloading

- 1 Be suspicious of offers to download something. These often appear as a flashy ad or popup window. They may come as email, often as an attachment or a link in the content.
- 2 Before you download some program or toolbar, enter "[program-name] virus OR spyware OR malware OR malicious" into a search engine. Review the results to decide about the program. Also ask yourself "Do you really need it?"
- 3 Before installing, check the downloaded file with a virus and spyware scanner.
- 4 Use trusted sources for downloaded software. The list below includes some of the major ones. Many offer descriptions, and sometimes ratings of the software.

www.tucows.com
www.nonags.com
www.snapfiles.com

downloads.zdnet.com
download.cnet.com
www.freewarehome.com

Power Matters

Probably the most commonly replaced PC component is the power supply. This is the part most susceptible to fluctuations or interruptions in the electricity supply. Large surges and spikes (e.g., nearby lightning strikes) can pass through your power supply and affect other components: motherboards, RAM and graphics cards are not uncommon, but even Hard Disks (i.e., your files) are not unknown.



The best protection is to install a high quality surge & spike filter. These are not the modified double adaptors or power boards sold by many retail stores, but high performance electrical filters; they can tolerate surges of over 5000V and 100,000A. And when they have sacrificially blown to protect your PC, they let you know you are no longer protected. Better still, they cost around \$40 - \$50 for 6- or 8-way devices.

The most commonly replaced laptop component is the battery. Laptop batteries should last for around 3 years, but the life is shortened if they are not periodically fully discharged.

So run your laptop on battery at least once a month, and, whenever the system is run on battery, run it until the battery is fully discharged. This will maximise battery life.

Cleaning Your Computer

Check the inside of your computer case every 12 months. If it's on the floor (especially in a desk footwell), put it on the desk — the fans inside computers make them excellent vacuum cleaners.

- 1 Remove the cover (usually the left side as you look at the front of the PC will be sufficient).
- 2 Restart the computer with the cover off briefly to check for noisy components (especially disks or fans). Replace them if necessary (after turning the computer off!)
- 3 With the computer off, check for dust around fans, air vents, and heat sinks. If excessive:
 - a) Unplug your system from power and other connections.
 - b) If you have access to clean, dry compressed air, blow the dust out of the computer.
 - d) If you cannot use compressed air, remove the dust with a small paintbrush and work your way from the top to the bottom of the case.
 - e) Remove all the dust from the case.
 - f) Use a (very) slightly damp cloth and clean the dust on the bottom of the case.