

# Security Central

The internet has its potential pitfalls but there's no need to fear – Windows supplies many of the tools you need to stay safe. Here we explain the Windows Security Center

**T**he way in which the dangers of the internet are portrayed by some parts of the media means it's surprising that anyone connects to it at all. From **hackers** to **viruses** and **spyware**, unknown threats and the fear they engender can seem overwhelming. But of course people do access the internet in their millions every day. Most do so quite safely too because, for all the security risks the internet presents, there are ways and means to keep your computer safe online.

In this feature, we are going to show you how to use the tools built into Windows to use the web safely, whether you are using Windows Vista or XP.

always this way. Early versions of the **operating system**, such as Windows 98, had absolutely no protection built in. That was partly because Microsoft misunderstood the significance of the internet and the ways in which it would touch upon the lives of home computer users. Security was seen as a barrier to simple computing.

It may have been well intentioned but it was a huge miscalculation. From Windows 98 to XP, viruses and hackers penetrated computers linked to the internet with ease, bringing irritation in some cases and wilful destruction of data in others – sometimes wiping the contents of a disk completely.

By the release of XP, Microsoft had begun to realise that internet security was a pressing concern for home users. XP included a **firewall** but it was not switched on by default. Given that many home users had no idea what a firewall was, let alone how to activate it, this didn't really help.

So in August 2004 Microsoft released a major update for XP called Service Pack 2, which contained a new element – Windows Security Center (WSC).

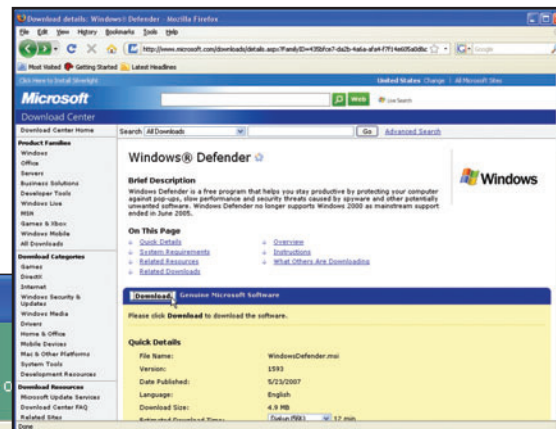
WSC was a real step up in protecting home PCs. It provides the ability to view a number of crucial security settings in a single place and monitors Windows security tools, as well as those from other software providers. If one program is not behaving as it should, or a vital application such as an **anti-virus** program is not detected at all, then WSC alerts the user (we will see how shortly).

Let's start, though, by introducing the main elements of WSC and explaining their role in keeping you safe online.

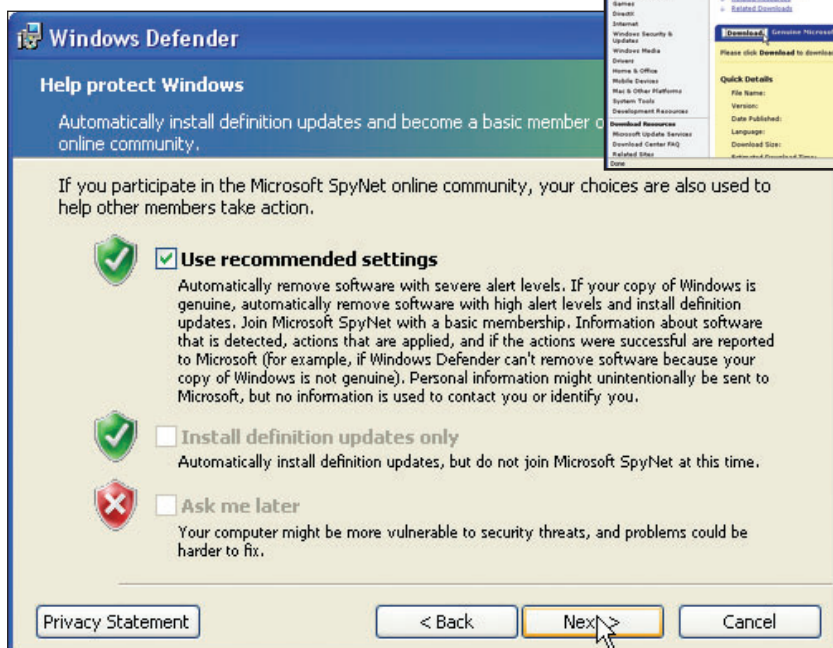
## Security Center

Microsoft likes to make a big fuss about just how safe Windows is to use. It's a claim the company can make today, but it wasn't

▼ Windows Defender can be set to scan your PC for spyware



▲ Download Defender online



## How Security Center works

WSC splits security into three broad categories: the firewall, software updates for Windows and protection against malicious software, such as viruses. The look and content of the Security Center is different in XP and Vista, while in the latest version of Windows (which is called Windows 7 and has only just been released), WSC will be renamed as the Action Center.

Let's open WSC now; in XP or Vista, click the Start button, followed by Control Panel and then double-click Security Center. The two screens on this page show the respective views in XP and Vista. Each panel displays a bar with the name of the category of protection. At the right-hand side of this bar, you will see a status message informing you whether the tool is on, not found or requiring some attention, or off. A 'traffic light' system of coloured **icons** focuses attention on these states using green, amber and red respectively. Next to the traffic light is a down-facing arrow; click this to display more information.

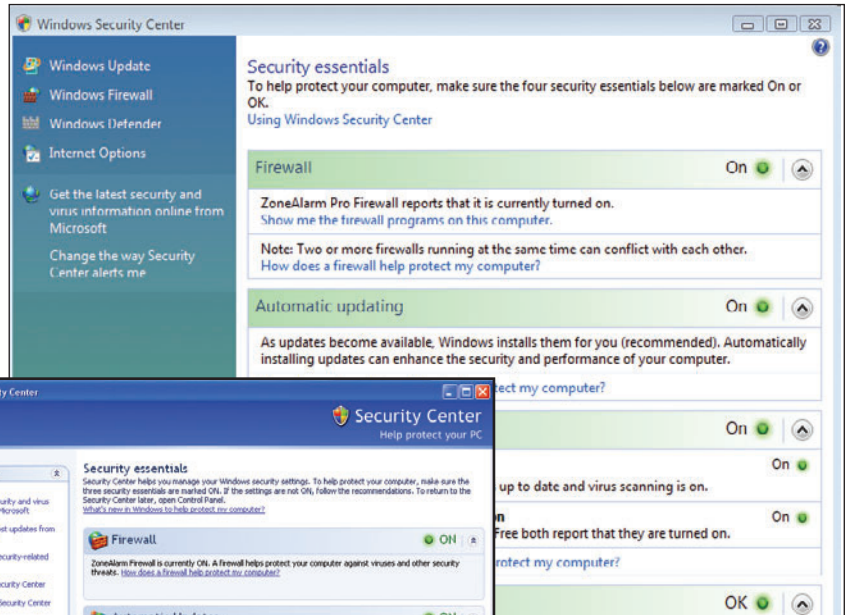
Incidentally, if you are using Vista and have tried to access some of the controls in WSC, you may see a warning message. This warning is generated by a tool called User Account Control (UAC), which was introduced in Vista to stop unauthorised changes to settings – security settings in particular. We'll come back to that shortly but while following the tips in this feature, it is quite safe to click Continue if this warning does appear.

## Snuffing out web threats

Top of the list is the Firewall section. Firewalls protect your computer by checking the information flowing to your PC from the internet to see if it might be dangerous. Some firewalls also take a look at applications that want access to the web. The reason for this is that some malicious software – should it find a way onto the **hard disk** – may try to send information back to its creator.

The status message of the firewall should say On, with a green light next to it. If it doesn't, click the down-pointing arrow on the firewall and then the button labelled 'Recommendations...'. A new window opens giving you the option to switch on the Windows firewall.

Hopefully you won't have to do this as Service Pack 2 for XP switched on the firewall by default. You may even have installed a firewall from another company – if you have read *Ultimate Guides* before, you will know that we recommend the free version of Zone Alarm (which is included on our cover CD – see page 26 for instructions on how to use Zone Alarm). If you decide to use Zone Alarm (or another alternative to Windows' own firewall), the name of this firewall will appear in WSC. Beneath it is a link that says: 'Show me the firewall programs on this computer'. It's worth checking this because, as WSC itself



▲ Windows Vista's Security Center provides easy access to tools



▲ Windows XP's Security Center looks slightly different to Vista's

points out, having two firewalls active at once can actually hinder your security efforts as they may clash. If more than one firewall is shown as active when you click the link, you need to disable one.

Most third-party firewalls have the ability to intercept any application on the PC that requests internet access – while the Windows Firewall can be set up to do this, it's far more difficult than it should be so you might as well switch off the Windows version if Zone Alarm, for example, is present. The WSC window has a link to the Firewall on the left in Vista and at the bottom in XP; you will also find easy access in those locations to the tools we're about to cover.

## Staying up to date

If your PC is connected to the internet, you have almost certainly experienced a program asking you to download and install an update. One of the beauties of the internet is that

## Phishing net

Not all the threats to your security and personal information are technical in nature. Phishing is a decidedly low-tech twist on the old-fashioned confidence trick. Put simply it is an attempt to trick you into revealing personal information such as bank account details, which is then used to defraud you.

The most common type is the phishing email, which appears to be a message from your bank asking you to

'confirm' some personal details by linking to a site that looks like the bank's.

To avoid this threat, remember that no financial institution will request this kind of information by email, but the problem is so common that web browsers now include tools to help. Internet Explorer 7 and 8, and Firefox 3, can detect websites that are not what they claim to be. On page 38 we show how to set up and use phishing filters.



▲ Set when and how often Windows downloads security updates

software developers can improve or fix flaws in programs. Windows is the greediest software of all for updates and, while they can be irritating, it's vital to download security updates. Criminals are constantly probing software for vulnerabilities that simply aren't known about. Windows is a tremendously complicated piece of software and those with the ability can find ways to exploit parts of it.

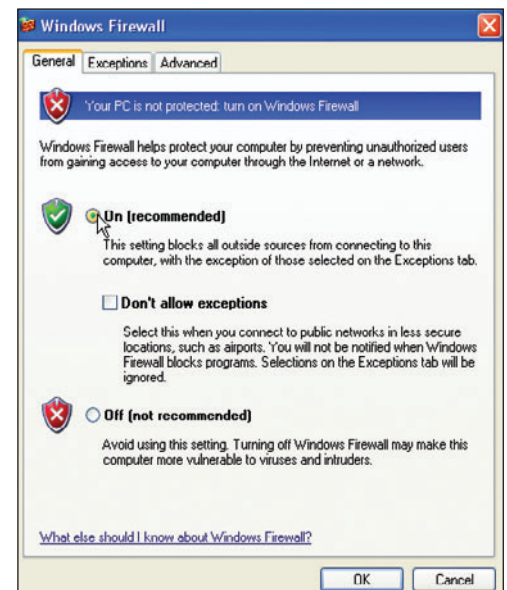
You can cut the irritation to a minimum, though. Immediately beneath the firewall section in WSC is Automatic Updates (called Automatic Updating in Vista). To adjust settings for this tool in XP click the Automatic Updates link at the bottom of the screen – in Vista, click Windows Updates on the left-hand side followed by Change Settings. The options in each version of Windows are almost identical. Select the top option to download updates automatically and you can use the **dropdown menus** to specify how often and at what time Windows checks back with Microsoft HQ for updates. The other options are to download the new software but decide whether to install it, or to have Windows notify you of available updates. Make your choice and click OK.

Vista users can click the blue arrow at the top-left of the window to go back a step and

view some more options. Vista will tell you if any new updates are available and whether they are merely optional or of vital security importance, and prompt you to download them without waiting for your next scheduled check. You can also view a list of updates that have been applied by clicking 'View update history'. You'll see an option here to remove selected updates; unless you're a very confident PC user, we suggest leaving this well alone.

## Thwart malicious software

Malicious software, such as viruses, is still a problem for home PC owners, although these days viruses are more likely to be used to open a door for spyware rather than disrupt or delete files stored on a hard disk. Spyware can record various types of information about the way you use a PC or copy personal information before sending it back to its creator. The aim is to defraud you, so clearly spyware is something we have to defend against. You should



▲ Firewalls check data flowing to your PC

also see the box on page 11 on how to deal with **phishing** emails.

Spyware is another area of PC security where Vista has advantages over XP – although it's not difficult for XP users to add the tools they need. In Security Center, XP users have a section called Virus Protection, which reports whether you have an anti-virus tool installed and if it requires an update. Vista has this too but the section in WSC is called malware protection – the term malware is derived from the words 'malicious' and 'software'.

Vista comes with its own anti-spyware tool called Windows Defender and the Malware protection area of WSC reports whether it, and any other anti-spyware tools installed, are up to date (unlike firewalls, you can have more than one spyware detector installed simultaneously). We'd recommend only using Defender if you have no other anti-spyware installed; running two simultaneously increases the potential of conflicts.

XP users can download a version of Defender

## Parental control

Most home PCs are used by families, so parents and guardians need to take extra care to ensure their time online is safe. One of Vista's best tools is Parental Controls, which enables you to set restrictions on how the PC is used by younger family members.

You will need to set up a user account for each person with access to the PC; this is covered in our guide on page 58. Once that's done you can specify times

of the day when children cannot use the PC at all, stop them from playing unsuitable games and control the types of website you think are inappropriate.

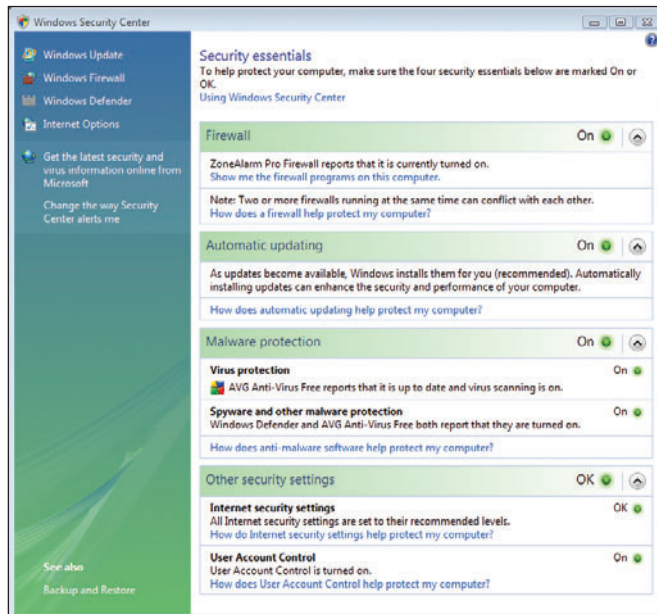
Parental Controls also generates reports about what each user has been doing with the computer, which only you get to see. It is a useful tool but we recommend that you discuss its use with children so they understand that their best interests are foremost.

at [www.snipurl.com/fubxl](http://www.snipurl.com/fubxl) although it will not appear in the Security Center. Like Automatic Updates, Defender can be set to scan your PC at a time that suits you. Open Defender (it's listed as an option on the left-hand side in Vista's Security Center; in XP you need to click the Start menu followed by All Programs and then Windows Defender) and click Tools then Options. Now you can set Defender to run with a quick or full scan – a Quick scan delves into folders where spyware is most likely to be found, while a Full scan checks every nook and cranny of your computer.

### Extra safeguards

Windows and its **web browser**, Internet Explorer (IE), offer other protection for web users. In Vista you can monitor these from WSC. In the final section labelled 'Other security settings' you will see information about internet security settings and User Account Control, which we touched upon earlier. Internet settings cover tools that are a part of IE7 and the new version, IE8. The information given by WSC, though, seems rather pointless as, even after we turned off all the security settings in IE7, it still reported that everything was fine. So we recommend checking these settings yourself in IE by clicking the Tools menu.

User Account Control is a useful, if controversial, addition to Windows. It's designed to prevent malicious software or other PC users from changing settings for applications but many people find it intrusive, as it requires them to click OK in a **dialogue box** when certain Windows tools are used. But if you have separate User Accounts set up for other household members – especially youngsters – UAC is very useful. If another user attempts



▲ Vista comes with its own anti-spyware tool called Windows Defender

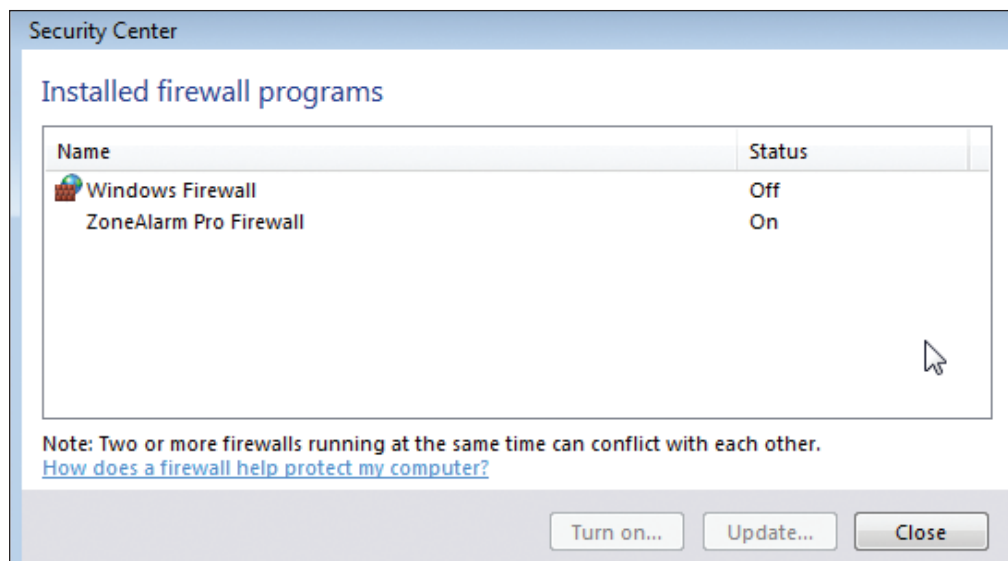
to change a crucial Windows setting or install a program, they are asked for the administrator password. This puts you as the PC's owner in complete control.

Windows 7, which was launched recently, has gone to lengths to make this handy tool less intrusive. You can't access UAC from the Security Center. Instead you will have to click Start and type 'user accounts' into the search bar. It will then appear in the Start menu, where you can click it to turn the tool on or off.

### Safe and sound?

While Microsoft has clearly improved PC security with Windows Security Center, don't assume that it will keep you totally safe. We noted earlier that the Windows Firewall, for example, can be improved upon and that's the case for other tools too.

So turn the page to get started on the features and step-by-step guides that will give you complete confidence when using the internet.



▲ You can have multiple firewalls installed but having them both switched on may cause conflicts

## Jargon buster

- ▶ **Anti-virus** Software that detects repairs, cleans, or removes virus-infected files from a computer.
- ▶ **Dialogue box** A window that pops up to display or request information.
- ▶ **Dropdown menu** A list of options that appears beneath a menu bar when you select a menu option, or when you click on a down-pointing arrow in a dialogue box.
- ▶ **Firewall** A piece of software or hardware that prevents unauthorised access to a computer over a network, such as the internet.
- ▶ **Hackers** People who break into other people's computers and networks, often in an attempt to steal sensitive information.
- ▶ **Hard disk** A high-capacity disk fitted in almost all PCs and used to store applications and files.
- ▶ **Icon** A small image used by Windows to identify a file or application.
- ▶ **Operating system** Governs the way the hardware and software components in a computer work together.
- ▶ **Phishing** A form of internet fraud that tries to trick you into revealing personal details.
- ▶ **Spyware** Software installed (usually surreptitiously) to monitor and report back on a computer's use.
- ▶ **Virus** A malicious computer program designed to cause at best annoyance and at worst, damage to computer data.
- ▶ **Web browser** A program developed for navigating the internet, particularly the world wide web.

# Glossary

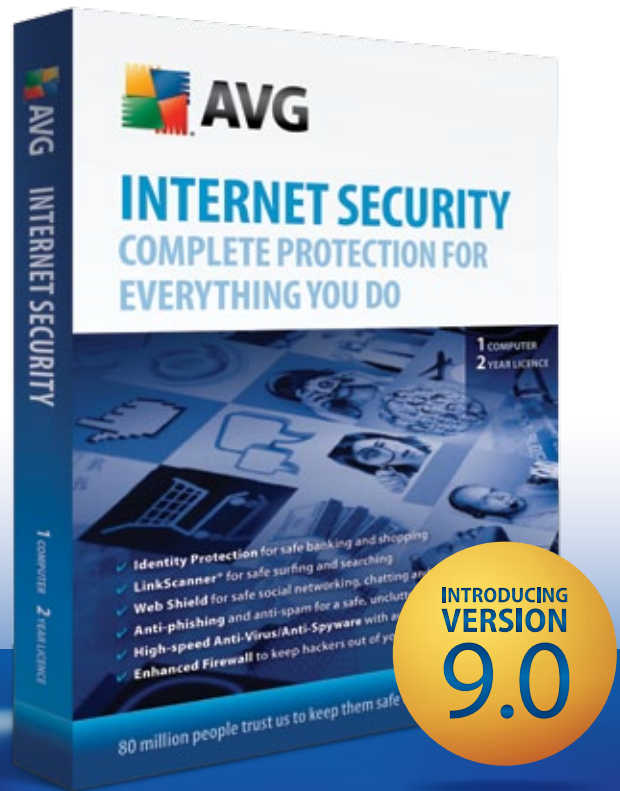
## Jargon buster

- ▶ **Add-on** Program that adds features to a web browser or applications, and is loaded only when needed.
- ▶ **Adware** Advert-supported software. Often installed surreptitiously on a PC and can compromise privacy.
- ▶ **Anti-virus** Software that detects repairs, cleans, or removes virus-infected files.
- ▶ **Bandwidth** The maximum amount of data that can be transferred over a connection at one time.
- ▶ **Beta** Version of software still in development.
- ▶ **Bios** Basic Input Output System. Software built into all PCs to control the basic operation of devices.
- ▶ **Bittorrent** File sharing software that enables users to download data from PCs anywhere in the world.
- ▶ **Boot** The process a PC goes through after it is switched on.
- ▶ **Broadband** A fast internet connection, such as ADSL.
- ▶ **Cache** Store for frequently used data or files.
- ▶ **Compression** The process of reducing a file's size by encoding the data.
- ▶ **Cookies** Text files generated by websites and stored on your hard disk.
- ▶ **CPU** Central processing unit. The brain of a PC.
- ▶ **Cursor** A moving pointer indicating a user's position on the screen
- ▶ **Dialogue box** A window that pops up to display or request information.
- ▶ **Disk image** A file containing all the contents of a floppy disk CD or DVD.
- ▶ **DNS** Domain name service. Translates website addresses into a language computers understand.
- ▶ **Domain name** The name used to identify a site on the internet.
- ▶ **Dropdown menu** A list of options that appears beneath a menu bar when you select a menu option.
- ▶ **Encryption** The science of scrambling data to hide it from prying eyes.
- ▶ **Firewall** Software or hardware that prevents unauthorised access to a computer over a network.
- ▶ **Floppy disk** A small, rigid square of plastic used to store data.
- ▶ **Format** To prepare a disk for use.
- ▶ **GB** Gigabyte. A measurement of storage capacity.
- ▶ **Hackers** People who break into computers, often in an attempt to steal information.
- ▶ **Hard disk** A high-capacity disk in almost all PCs, used to store data.
- ▶ **Icon** Image used by Windows to identify a file.
- ▶ **Internet Service Provider (ISP)** A company that provides you with an internet connection.
- ▶ **Internet Protocol (IP) address** An identifying number of a computer attached to a network.
- ▶ **JPEG** A common format for image files.
- ▶ **Keylogger** A malicious program that tracks your key presses and then sends them back to criminals, allowing them to commit fraud.
- ▶ **Malware** Software that performs harmful or surreptitious acts.
- ▶ **MB** Megabytes. A measurement of storage capacity, usually for computer memory.
- ▶ **Memory key** A thumb-sized USB storage device.
- ▶ **Modem** A device that enables two computers to communicate with each other over a telephone line.
- ▶ **Network** A way of connecting several computers and devices so they can share data.
- ▶ **Network Adapter** A socket for connecting a PC to an office network or some broadband internet connections.
- ▶ **Optical drive** Disc drive that uses a laser light to read and write data.
- ▶ **Partition** A large hard disk can be split into partitions or 'virtual' drives, which are treated by Windows as separate, smaller hard disks.
- ▶ **Phishing** A type of internet fraud that has the aim of tricking you into revealing your personal details to cyber criminals.
- ▶ **Plug-in** A program that adds extra features to your web browser or to other applications, and is loaded only when it's needed.
- ▶ **Reboot** To restart a computer.
- ▶ **Registry** A file in Windows that stores information on all hardware and software installed on your PC.
- ▶ **Rootkit** Software that gives a malicious user administration rights and access to a computer.
- ▶ **Router** A device used to connect more than one device to the internet.
- ▶ **Server** A computer on a network that distributes information.
- ▶ **Spyware** Software installed to monitor a computer's use.
- ▶ **SSID** Service Set Identifier. A naming convention for wireless networks.
- ▶ **Trojan** A malicious program disguised as a harmless one.
- ▶ **Universal Serial Bus (USB)** A standard that allows quick and easy connection of external peripherals to your PC.
- ▶ **URL** Uniform Resource Locator. The unique address of a web page.
- ▶ **Virus** A malicious computer program designed to cause damage to computer data.
- ▶ **Web browser** A program developed for navigating the internet.
- ▶ **Webmail** An email account accessed via a website.
- ▶ **Wep** Wired Equivalent Privacy. A security standard for wireless networks.
- ▶ **Wifi** An umbrella term for various standards for wireless networking.
- ▶ **Wireless network** Several computers connected without network cables.
- ▶ **Wizard** A step-by-step process that helps you choose settings.
- ▶ **WPA** Secure protection for wireless networks.
- ▶ **Zip file** A file that has been compressed to save disk space or so it is quicker to email.



# SAY HELLO TO AVG 9.0

Faster, Safer, Easier to Use.



## HOME SECURITY

**Complete protection for everything you do**  
AVG Internet Security with Identity Protection

**Surf the web with confidence**  
AVG Anti-Virus & Firewall

**Essential protection that won't get in your way**  
AVG Anti-Virus

**Up-to-the-minute protection for online banking and shopping**  
AVG Identity Protection

- 1-year and 2-year licence options available
- Free updates and product upgrades for the licence duration
- Fast, automated scanning and updates
- Free local telephone support, plus 24/7 e-mail support

AND MUCH MORE...

## TOUGH ON THREATS.

- ✓ Total protection against the latest threats
- ✓ Virus-free chat and instant messaging
- ✓ Anti-spam and phishing prevention
- ✓ Blocks hacker attacks
- ✓ Blocks poisoned web pages in real-time

## EASY ON YOU.

- ✓ Won't slow your PC down
- ✓ Easy to use — install and forget
- ✓ Simple set-up and automatic free updates
- ✓ Works in the background
- ✓ Free local telephone support

110 million people trust us to keep them safe online – and so can you.

NZ 0800 284 000  
**avg.co.nz**

AU 1300 284 000  
**avg.com.au**