

# Surviving a malware attack



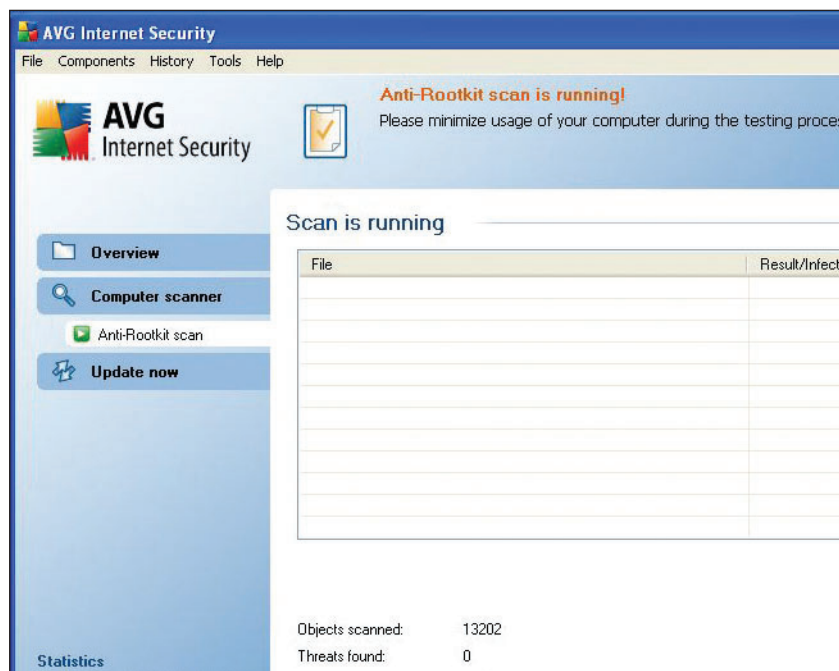
We explain how to spot an infection and show exactly what steps to take if you suspect your PC has been infected by a virus or attacked by malware



**T**he majority of this magazine concentrates on what to do to keep your computer safe from all the various threats that lurk online. By following our advice and using some of the free tools on our cover CD, you can keep your PC completely protected. But what if you think your PC might already be infected with a **virus**? Is your PC behaving strangely? Could it be **spyware** or some other kind of malicious attack? How can you tell and what do you do if something nasty really has wormed its way into your system?

In this article, we will show you how to spot when your PC has been infected and, if it has been targeted by **malware**, we will explain what to do to tackle the problem.

▼ If you suspect a virus, it's worth running a rootkit scan as well



## Identifying an attack

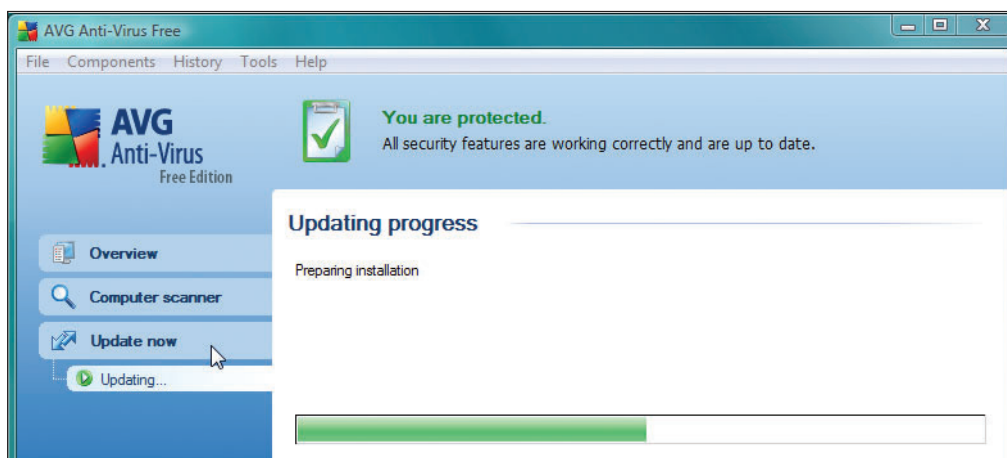
Occasionally, a virus or other form of malware will make it plainly obvious when it has infected your PC – some will even flash up messages proudly claiming your PC as their latest scalp. However, the vast majority will prefer to keep their presence as low-key as possible – the longer they can stay undetected, the more havoc they can wreak.

It is therefore important to be aware of the signs of an infected computer. After all, the sooner you identify the attack, the quicker you can take steps to remove it and therefore limit the damage caused.

Perhaps the most frequent indication of an infected PC is a sudden drop in performance – Windows takes longer to load, double-clicking **icons** results in a good minute's wait before anything happens and even simple tasks, such as closing down applications, becomes laborious. The reason performance takes such a hit is that your PC's resources are being put under strain by the malware. However, as we'll explain in more detail later, it's important to understand that a slow-running PC doesn't necessarily mean it's been infected.

Although crashes and freezes aren't exactly uncommon in Windows, if you start experiencing such behaviour on a regular basis it could be an indication of a resident virus. Similarly, applications that exhibit strange behaviour or odd error messages popping up should set alarm bells ringing. Another common indication of an attack is that your security software reports that it can't update itself – some viruses will even attempt to disable any such software running on your PC, including your **firewall**.

Other signs of infection include your browser's home page changing to an unknown site, and new icons appearing both on the desk-



▲ Run manual updates every so often to check everything is working properly

top and in the notification area in the bottom right corner of the screen. You may also be informed by friends, family and colleagues that they have received strange emails from you. If you experience any of these symptoms, it is vital that you run the appropriate checks, which we will come on to in a moment.

### False warnings

Anyone who has spent time on the internet will have occasionally noticed pop-up windows appearing with messages such as 'Warning: your PC is infected! Click here to remove the virus' or 'Virus detected! Click here to scan your PC'. Needless to say, such warnings are almost always bogus. However, they can often look extremely authentic – some will even mimic a Windows **dialog box** with OK and Cancel buttons. More often than not, though, clicking on one of these **pop-ups** will result in an attempt to download some form of malware to your PC.

A common trick is for the pop-up to suggest downloading specific anti-virus software, but this software is almost always not what it seems and will often end up hiding the malware's activity from you – you may even be asked to pay for the software.

Although most of these pop-up windows will have a Cancel option along with the usual cross in the top right-hand corner, these are usually fake buttons – clicking anywhere in the pop-up window could result in malware being downloaded. The best way to close an unwanted pop-up window is to start Task Manager by holding the Ctrl, Alt and Delete buttons simultaneously (Vista users will need to select Start Task Manager at this point). Next, from the list of running applications, simply highlight the pop-up window entry and click the End Task button – this will ensure the pop-up is closed without causing any harm.

When you see a pop-up such as this, treat it with the utmost suspicion. Very few reputable companies will tell you to download their software in this manner. If you want to follow one up, don't click on the pop-up but instead do a little research on the company name first. As always, if in doubt, simply leave it well alone.

If the warning message looks much like a standard Windows message and you are

unsure whether or not it's legitimate, try searching for the message on Google (remember to put quote marks either side so only results relating to that exact message are returned) – if it's a fake message, it's quite likely other people have reported it.

### Virus or slow PC?

Often, PCs will be misdiagnosed as having a virus simply because they're running slowly. Although viruses and malware will indeed cause a slowdown in performance, they're not the only culprits. More often than not, a PC runs slowly simply because it's old – over time, **hard disks** become cluttered, which can result in the slow loading of Windows and applications. Similarly, if your other hardware, such as the **processor** and **memory**, is old it may struggle to cope with the demands of modern software. However, if performance has suddenly taken a dramatic hit, a virus or malware attack could be the cause.

### Take action

Now you know what to look for, we will go over the steps you need to take to remove malware from your PC. Suspecting you have a virus on your PC is never a nice feeling, but the most important thing is not to panic – simply deleting files you believe to be suspicious is only likely to cause more problems.

## Malicious software removal tool

If you are having trouble removing a virus or just want to add an extra level of protection, it's worth installing the Windows Malicious Software Removal Tool from Microsoft.

This tool requires very little in the way of interaction – you simply install it and it will start scanning your PC for viruses known to Microsoft, automatically removing any it finds.

However, it's by no means a replacement for anti-virus software. Unlike standard anti-virus packages, which are usually updated on a daily basis, this tool only gets updated once a month.

It will also only scan for known viruses, so it won't do you much good if you get infected by a virus that appeared a few days after the last update.

That said, you may find it is more effective at removing a specific virus compared to your standard software. And it won't interfere with any other security software running on your PC.

To download the Malicious Software Removal Tool, head to [www.microsoft.com/security/malware/remove](http://www.microsoft.com/security/malware/remove). Once installed, it will then download each month's updates and scan your PC automatically.

## Jargon buster

▶ **Dialog box** A window that pops up to display or request information.

▶ **Firewall** A piece of software or hardware that prevents unauthorised access to a computer over a network, such as the internet.

▶ **Hard disk** A high-capacity disk fitted in almost all PCs. It is used to store both applications and the documents and files they create.

▶ **Icon** A small image used by Windows to identify a file or application.

▶ **Malware** A generic term for software designed to perform harmful or surreptitious acts.

▶ **Memory** The computer's temporary storage area, measured in megabytes (MB).

▶ **Memory key** A generic term used to describe thumb-sized USB storage devices.



▲ Rogue pop-up warnings can look very convincing



With any luck, this scan will unearth the problem and fix it for you immediately without you having to worry any more. If not, it's probably worth trying a different anti-virus package (head to our special Security Software feature from page 16 onwards for a few choice ideas in that regard), but be sure to uninstall your current anti-virus software first as having two installed at the same time can cause conflicts. If you don't want to install additional software, there are plenty of online scanners available. These will download a small application to your PC and will scan for known viruses and other malware – most will also offer to remove any they find. Always use a trusted site for this, though – examples include Trend Micro's Housecall (<http://housecall.trendmicro.com/au>).

If you believe your PC might have been infected by some form of potentially dangerous malware, your first step should be to ensure that all your security software is running and, most importantly, that it is completely up to date. Most security software will perform regular automatic updates, but by attempting a manual update you will be able to see whether or not it was successful – all software differs, but more often than not you will find an 'update' option from within the software's main menu.

Once your anti-virus software is up to date, the next step is to instruct it to run a full scan of your entire hard disk – this is sometimes referred to as a deep scan. Again, exactly how you run this scan will depend on your software, but you should find a 'Scan now' or similar option. A full scan will inspect every nook and cranny of your PC for rogue software and will therefore take much longer than an ordinary quick scan; on slower computers or those with large hard drives it can take up to an hour, sometimes even longer.

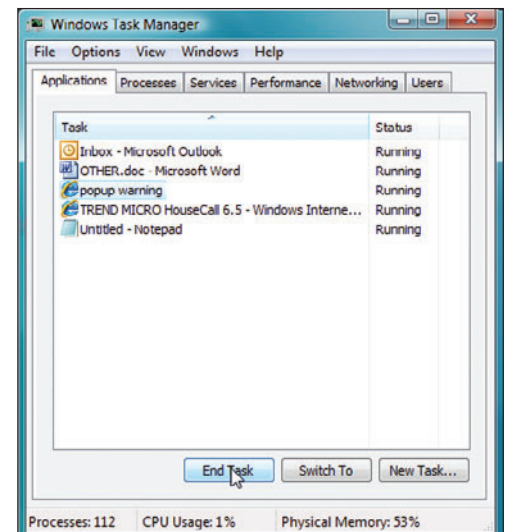
### Can't update?

Some forms of malware will attempt to prevent your anti-virus software from updating and, if your software doesn't have the most recent updates, it might not be able to detect or remove the malware in question. If this happens to you, try downloading the latest updates using a different computer and then transfer them to the infected PC – most anti-virus software will then let you install the updates manually. For example, if you use AVG you can download the latest updates using a different PC by heading to <http://free.avg.com/download-update>. These can then be transferred to a **USB memory key** and subsequently copied to the infected PC. Now all you need to do is go to the main AVG screen,

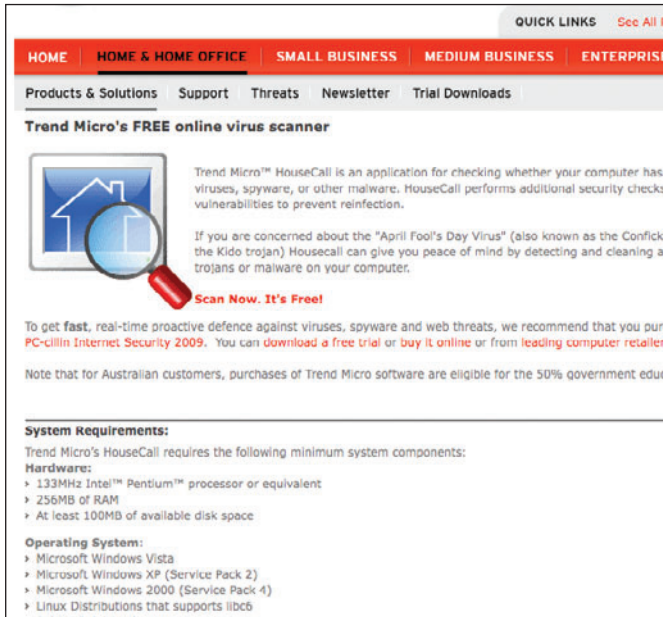
## Malware spotting

Make sure you know the warning signs of an infected PC – here are the most common:

- Sudden slowdown in your PC's performance
- Frequent crashes and restarts when running Windows
- Being bombarded with pop-up windows, whether online or not
- Certain websites won't load or your homepage keeps changing
- Browsing the web is much slower
- Error messages start to appear more often than usual
- People tell you that they received a strange email claiming to be from you
- Security software reports that it cannot update itself
- New icons unexpectedly appearing in the notification area and on the desktop
- Windows applications, such as Security Center, look different to normal
- Hardware, such as a printer, attached to your PC becomes unavailable.



▲ Always use Task Manager to get rid of suspicious pop-up warnings



▲ Housecall from Trend Micro also offers a free online security scanner

click on the Tools menu, select the 'Install from directory' option and point AVG to where the updates are stored. If this still doesn't work, it's best to uninstall the anti-virus software and then either re-install it or switch to a different anti-virus package.

As well as keeping your security software up to date, it's equally important to ensure Windows is kept similarly updated. Microsoft frequently releases updates that repair security flaws in Windows – if you don't have the latest updates installed, you are leaving yourself open to attack. Both XP and Vista users can make sure Windows is kept fully up to date with the latest patches by switching on Automatic Updates within Security Center, which you'll find in the Control Panel. Alternatively, you can head to Microsoft's Windows Update website at [www.windowsupdate.com](http://www.windowsupdate.com), which will scan your PC and offer recommended updates for download.

### Spyware and rootkits

It may be that the problems you are experiencing are caused by spyware. Unlike viruses, spyware doesn't usually attempt to damage your PC. Instead, it will monitor your usage and collect personal information. What sort of data it collects and what it does with

it will depend on the type of spyware, but it could be as serious as collecting information such as passwords for online banking.

However, it could also be the work of a rootkit. Most free solutions don't include anti-rootkit scanners, and although the paid anti-virus or internet security solutions generally do, they don't include it as part of their scan. With this in mind, you should try a separate scan for rootkits, which is easy to do with AVG Internet Security, of which we've included a free 90-day trial on our cover disc.

### Last resort

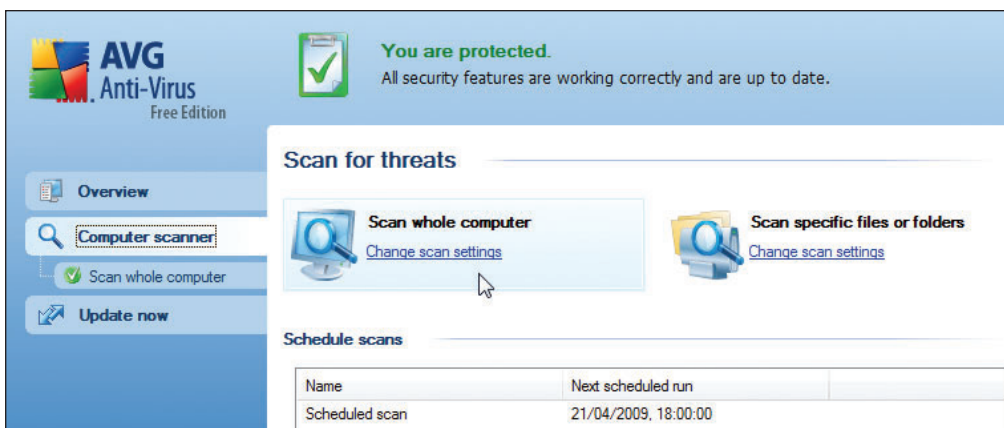
In particularly bad cases, a virus or other forms of malware can bring your PC to its knees completely – anti-malware programs may not install or work properly, Windows may freeze shortly after loading, or it may not even load at all. If this happens, you may have to take some drastic steps in order to reclaim your PC, such as restoring your computer from a recent backup (see page 68) or, in the case of a very bad situation, completely reinstalling Windows from scratch (see page 84). Head to our Worst Case Scenario feature on page 78 to find out more.

Once you get things back to normal, it's best to be on your guard the next few times you use your PC. If the anti-virus software didn't wipe all traces of the malware, your PC may very quickly become infected again. Keep an eye out for any unusual behaviour and, as always, make sure all your security software is kept up to date.

Sadly, even the most protected of PCs running fully up-to-date security software can occasionally fall victim to the devastation of a malware attack. Security software might be getting more sophisticated, but unfortunately, so are malware developers. However, armed with the information we've provided in this feature and throughout this Ultimate Guide, you will be far better placed to spot when an attack occurs and how to remove the threat before it gets a stranglehold on your PC.

## Jargon buster

- ▶ **Pop-up** A window that is displayed by a website, usually over material already on the screen.
- ▶ **Processor** The chip that is the 'brain' of the computer. The faster the processor, the better a computer will perform.
- ▶ **Spyware** Software installed (usually surreptitiously) to monitor and report back on a computer's use.
- ▶ **Universal Serial Bus (USB)** A standard that allows quick and easy connection of external peripherals such as storage devices to your PC. Devices can be added or removed while your PC is switched on.
- ▶ **Virus** A malicious computer program designed to cause at best annoyance and at worst, damage to computer data. Viruses usually spread from computer to computer by email.



◀ Running a full system scan should be a priority if you suspect a malware attack

# Glossary

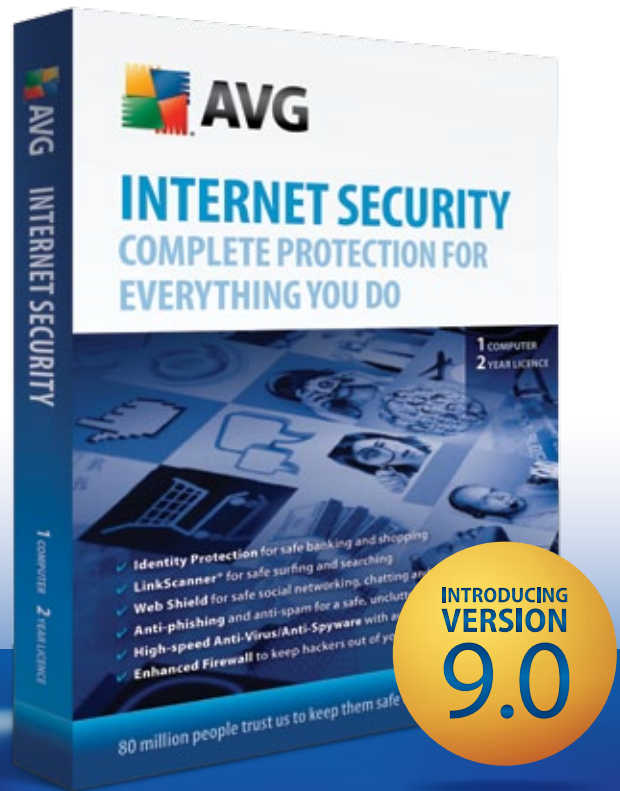
## Jargon buster

- ▶ **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**