



Viruses & malware

If you assume the only threat to your PC and data is a virus attack, think again. We investigate the various types of malicious software you may encounter

Top 10 worst ever malware attacks

The computer world has seen some pretty devastating viruses, worms and other malware attacks in its time. According to the experts at computer security website IT Security (www.itsecurity.com) the worst ever offenders are, in chronological order, as follows:

- 1 Morris – 1988
- 2 Melissa – 1999
- 3 VBS/Loveletter – 2000
- 4 Code Red – 2001
- 5 Nimda – 2001
- 6 SQL Slammer – 2003
- 7 MS Blaster – 2003
- 8 MyDoom – 2004
- 9 Sasser – 2004
- 10 Witty – 2004

The word 'virus' has come to be used as an umbrella term to describe many of the security threats that can affect our computers, but the truth is that viruses are just one of the many different types of malicious software – or 'malware' for short – that we need to ensure we're protected against. In addition to viruses themselves, there are Trojans, worms, spyware and other nasties to contend with, all of which can have potentially disastrous consequences for you and your PC.

To give you an idea of just how bad the situation is, a recent report from security company Symantec estimated that its software helped to block more than 245 million malware attacks around the globe each month in 2008 alone. That's a lot of malicious code.

Know your enemy, they say, so in this feature we'll be identifying the main types of malware and explaining precisely why you need to protect yourself against them.

Viruses

As we said earlier, it's quite common for the 'v' word to find itself bandied about whenever somebody talks about computer security, but

it actually refers to quite a specific type of malicious code. A genuine computer virus is a program that can infect its host and then replicate itself – just like a real virus. Interestingly, a virus cannot run on its own. It's basically a program and it needs to be run unwittingly by the person using the computer. Thus, if a virus arrives as an email attachment, for example, your PC wouldn't

be infected until you double-clicked the attachment to open it. Some viruses – known as 'macro' viruses – come hidden within Microsoft Word and Excel documents. If you open an infected document with **macros** enabled, your PC could be the next victim.

The effects of a virus infection can vary from virtually imperceptible to completely disastrous, depending on what the malicious program was created to do once run. Viruses have been known to do all kinds of things, from presenting an annoying message or emailing themselves around the planet, to corrupting documents or trashing the PC it infects.

In some cases it's possible to have a virus infection without even knowing it. Only a thorough virus scan will reveal and remove it.





Worms

A worm is similar to a virus – its basic mission is to spread itself as far and wide as possible by replicating itself, either over a **network** or by harvesting email addresses from your computer and mailing itself out to all your contacts. There's one big difference, however; worms can run themselves and they don't need you to do anything to accidentally kickstart an infection.

The thing you're most likely to notice if you're infected by a worm is slowdown. Worms don't tend to send your PC spiralling into meltdown, but they cause a lot of background and network activity, particularly if they are busy emailing themselves to everyone in your address book. There are some types of worm, however, that can provide criminals with a back door to your computer, usually to turn it into a 'zombie' to send out **spam**.

Most worms are created to take advantage of security flaws in Windows itself, which is why it's vitally important to keep your **operating system** up to date using Security Center (see page 12). On top of that, you'll need a **firewall**, anti-virus and anti-spyware utilities all running if you want to keep worms at bay.

Trojans

To mix metaphors slightly, a Trojan is a wolf in sheep's clothing; a malicious program that comes disguised as a legitimate application. They're named after the device used to sneak Greek soldiers past the gates of Troy because Trojans have a similar behaviour – ie they sneak malicious code past your defences by pretending they're something else.

The Trojan itself is not usually harmful. It's the so-called 'payload' it delivers that can cause you headaches. This could be a virus, a worm or a rootkit (see below), or even something like a keylogger, which can monitor anything you type into your keyboard – including internet bank logins, credit card numbers and sensitive passwords – and deliver them into the hands of criminals.

The easiest way to avoid Trojans is to be very careful about what you install on your PC. If you're not sure of the origins of a program and can't verify that it's genuine, don't install it. Anti-virus and anti-spyware software should also pick up on a malicious payload.

Rootkits

A rootkit can find its way onto your PC as a result of a virus infection or via a Trojan. It's basically a nasty



piece of code that allows other users access to the inner workings of your PC. Criminals can then enjoy administrator-level control over your computer via the internet.

It's often easier to block a rootkit than it is to remove one, so it's vitally important that you have up-to-date security software on your PC.

Spyware

Although potentially less physically damaging than a virus or Trojan, spyware (and its close cousin adware) can be a serious threat to your privacy and, in some cases, change files or settings on your PC.

The main function of a spyware program is, as the name suggests, to spy on and gather information about a computer user, which is then usually reported back to someone over the internet. A mild spyware attack, for example, could monitor your internet use and send a list of sites you visited to a marketing company. A more serious spyware event could see all your login details, passwords and credit card numbers delivered directly into the hands of criminal organisations.

Some types of spyware can be delivered via a Trojan, others can enter your PC via loopholes in your **web browser's** security or by inadvertently clicking on a bogus **pop-up** window that is masquerading as a genuine Windows or security message.

Often, a spyware attack can go unnoticed.

Symptoms can range from a mild slowdown to an all-out pop-up infestation. You may also find that your browser's home page has been changed or that your **bookmarks** have been hijacked. Keep your anti-spyware and your anti-virus applications up to date, however, and you shouldn't need to worry.

Fighting back

If all that seems a little worrying, take heart in the knowledge that it's fairly easy to protect your PC from all of the above threats. All you need is some software installed on your computer to act as a barrier against any malicious software it encounters. As we saw on page 16, there are plenty of options in this regard, many of which are completely free.

And if you turn the page, you'll find out how to set up and use AVG Free Anti-Virus (page 22), AVG LinkScanner (page 24) and AVG Internet Security (page 26), all of which you'll find on this issue's free cover CD. Simply follow our instructions and, as long as you keep your security applications up to date at all times, you'll be protected from all the above mentioned nasties and more.

Jargon buster

▶ **Bookmark** A way of storing favourite websites in the Firefox web browser for later reference, much like marking a page in a book. The equivalent in Internet Explorer is a Favorite.

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

▶ **Macro** An automated series of commands or operations that can be run at any time. For example, if you always carry out a series of operations on your text to put it into a certain typeface and size, then you can set up a macro to perform this function.

▶ **Network** A way of connecting several computers and devices so they can share data.

▶ **Operating system** Governs the way the hardware and software components in a computer work together.

▶ **Pop-up** A window that is displayed by a website, usually over material already on the screen.

▶ **Spam** Junk email sent to large groups of people offering such things as money-spinning ideas, holidays, and so on. Named after the Monty Python Spam sketch.

▶ **Web browser** A program developed for navigating the internet, particularly the world wide web.

Protect against viruses with **AVG Free**

Meet your basic security with award-winning protection that won't cost you a cent



If you're looking for free protection from the threats of malware, then look no further than AVG Free. While it doesn't have all the functionality of a full Internet Security suite, this offering is full of effective tools for keeping you safe online.

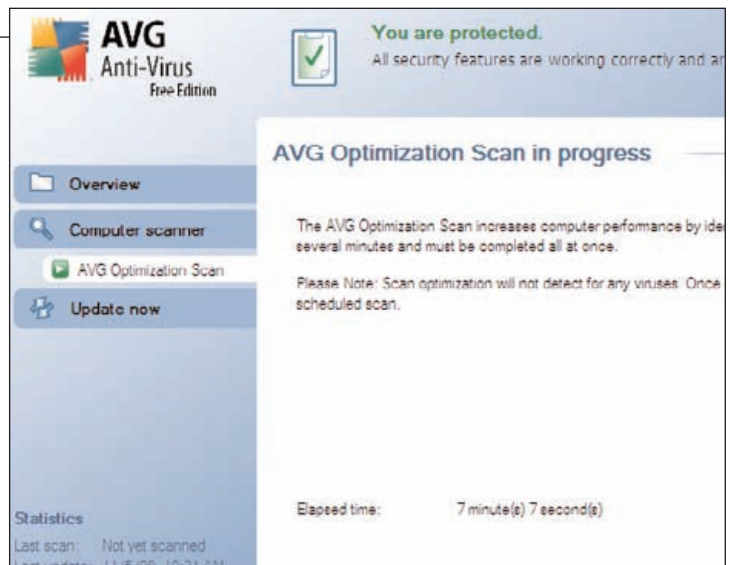
It has always been the philosophy at AVG that everyone should have the right to basic computer security at no cost, and tens of millions of users have taken advantage of AVG Free software since AVG first offered its free protection package back in the year 2000.

With AVG Free, you can scan your PC for viruses and spyware, as well as scanning websites and incoming emails for signs of danger. Scanning is easy, and we'll show you exactly how in this guide.

All you need to do to get started is install the software from our cover disc, or alternatively you can get it from the website at www.avgfree.com.au. Downloading and installing the program is easy and should only take minutes. Read on to find out how to use AVG Free.

Step 1

Once you have installed AVG Free you'll see the AVG Optimization Scan dialog window. The scanning optimization functionality searches your Windows and Program files folders, where it detects appropriate files (at the moment those are the .exe, .dll and .sys files) and saves the information on these files. With the next access these files will not be scanned again, and this reduces scan time significantly. Select 'Optimize scanning now (recommended)' to continue. This whole process should only take a couple of minutes, and when you're done you'll have a list of trusted files at hand. Bear in mind, however, that this is not a virus scan – you'll have the option to run a regular scan later, and we'll show you how it works in the coming steps.



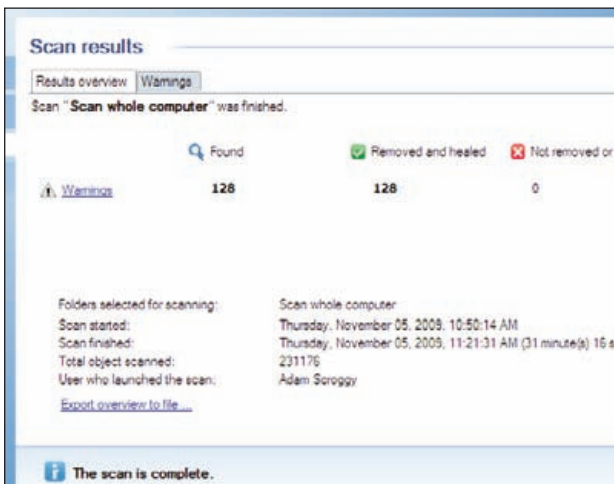
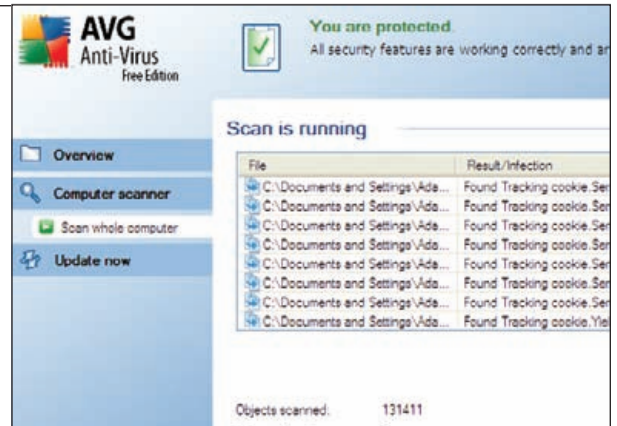
Step 2

Once this is done, you'll then be presented with the AVG Free User Interface, which we have shown in our screenshot to the left. This interface can be accessed at any time by double clicking the AVG icon on the system tray in the bottom right corner of your screen. You may also have an AVG icon on your desktop, and you can usually find one in the 'All Programs' section of your Windows Start menu as well. Remember, there is a possibility that a computer virus has been transmitted to your computer prior to AVG Free's installation. For this reason you should now run a scan of the whole computer to make sure there are no infections on your PC. Click the 'Computer scanner' tab on the left of your AVG Free window.



Step 3

You'll now find yourself in the 'Scan for threats' dialog. In this dialog you'll have two options: Scan whole computer and Scan specific files or folders. For the most comprehensive scan, we're going to focus on the first option, which scans your entire computer for possible infections and potentially unwanted programs. This test will scan all hard drives of your PC, will detect and heal any virus found, or remove the detected infection to the 'Virus Vault'. Click 'Scan whole computer' to begin the scan. The length of time it will take for the process to complete varies depending on the size of your PC. For us, it took around one hour, so be sure to give yourself plenty of time.

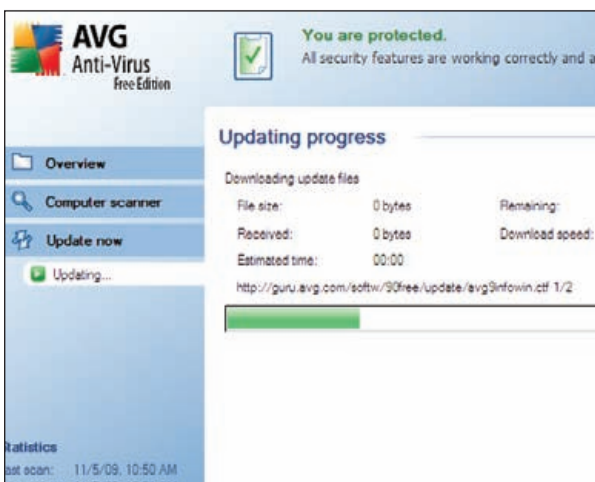
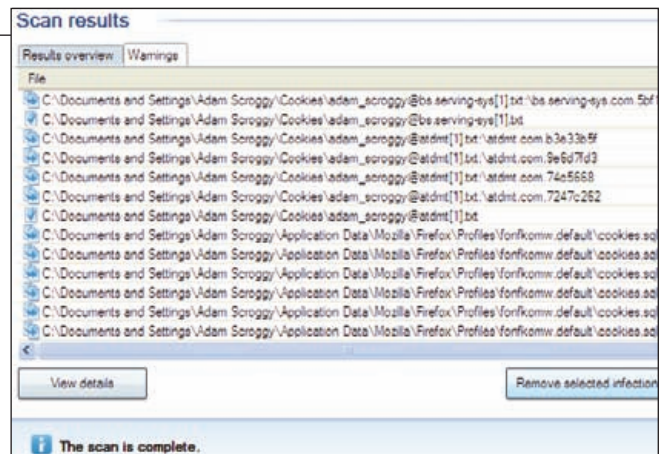


Step 4

When you're finished, the Scan Results Overview page will appear. It is divided into several tabs, including Results Overview, Infections, Spyware, Warnings and Information. Results Overview will be displayed always, but the others will only be displayed if threats were found in that section (note that 'Information' refers to threats that could not be classified. In our scan, for example, AVG Free found 128 warnings, and as such clicking on the 'Warnings' tab will reveal more detailed information about each threat. While we're fortunate to not have any infections or spyware on our PC, Warnings may include hidden files, tracking cookies and suspicious registry keys.

Step 5

Whether your PC has turned up infections, spyware, warnings or information, if you click the appropriate tab not only will you see more information on the topic, but you'll also have access to various control buttons. 'View details' opens a new window with detailed scan result information. 'Remove selected infections' will see the selected findings moved to the Virus Vault, a safe environment for the management of suspect files. 'Remove all unhealed infections' deletes all findings that cannot be healed or moved to the virus vault. Finally, 'Close results' terminates the detailed information overview and returns to the 'Scan results overview' page.



Step 6

Keeping your AVG up-to-date is crucial to ensure that all newly discovered viruses will be detected as soon as possible. Since AVG updates are not released according to any fixed schedule but rather in reaction to amount and severity of new threats, it is recommended to check for new updates at least once a day. Click the 'Update now' tab from the left hand menu on the AVG Free interface to begin scanning for new updates. If AVG finds new update files available, AVG starts downloading and launches the update process itself, during which time you'll get redirected to the Update interface where you can view the process progressing.

Surf safely with **LinkScanner 8.5**

We show you how to set up and use a sophisticated malware detector to protect your PC



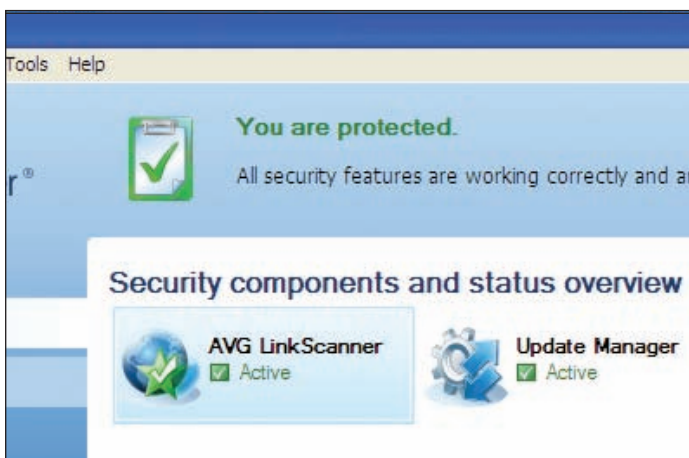
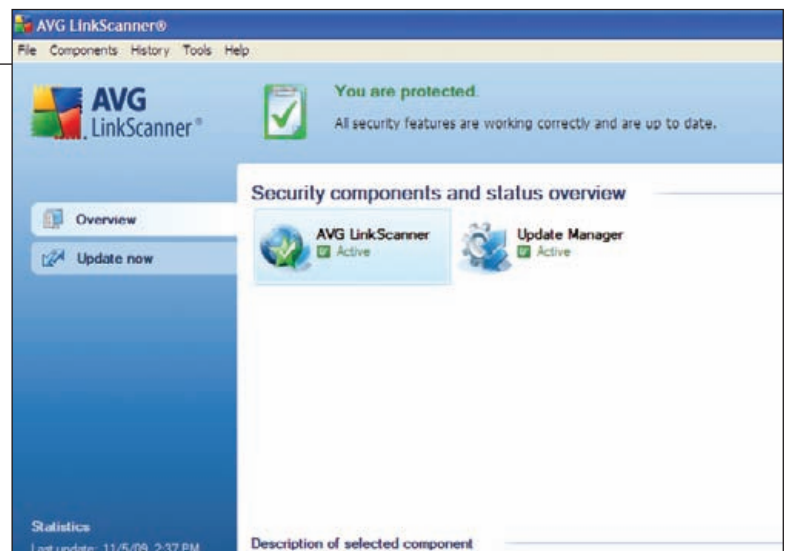
One of the least understood AVG components and the one that causes most confusion is LinkScanner. What does it do? Does it scan webpages, compare URLs against a blacklist, or what? As you may know, there are currently around 30,000 new viruses and other malware hitting antivirus researchers' labs each day. Most spread via the web. This is the aspect of malware that LinkScanner deals with. It scans web page content as that content is deliv-

ered to your computer, and identifies delivery mechanism patterns that indicate potential malware delivery. When it identifies something suspicious, it blocks that page.

LinkScanner is installed on the network layer, intercepting all web traffic regardless of which browser you use and detecting threats before the browser sees anything. It serves as a very strong extra layer in the overall AVG security system.

Step 1

AVG LinkScanner can be installed from our cover CD. Bear in mind that if you've already installed AVG Free or AVG Internet Security then you should have a copy of LinkScanner already running. Once installed, the LinkScanner User Interface can be accessed from the AVG icon in your System Tray. Once it opens, it will look just like the screenshot to our right. The default configuration of AVG LinkScanner is set up to achieve optimum performance, so we don't recommend changing anything unless you're an expert. If you do feel the need to change LinkScanner settings, go to the Tools dropdown menu, select Advanced settings, and you can edit them from there.

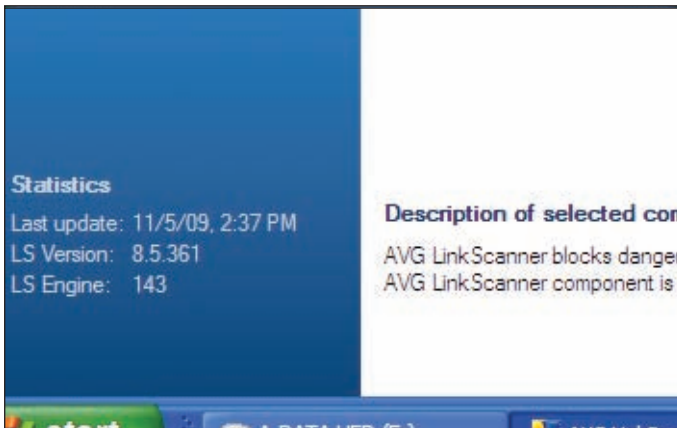
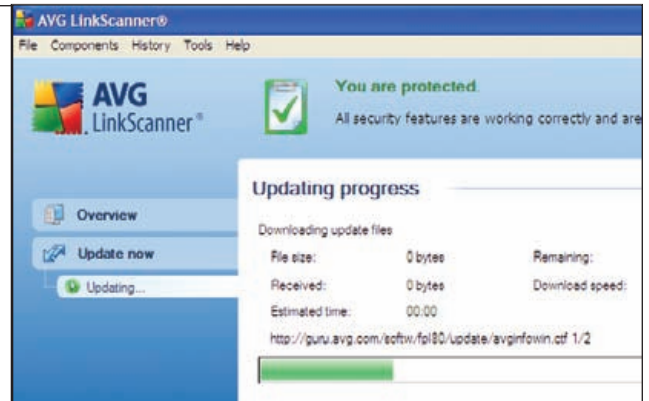


Step 2

At the top of the screen is Security Status Info, where you will find information on the current security status of your AVG 8.5 LinkScanner. If there's a green icon with a tick, it indicates that LinkScanner is fully functional; your computer is completely protected, up to date and all installed components are working properly. If you see the orange tick, you're being warned that one or more components are incorrectly configured and you should pay attention to their setting; there is no critical problem and you have probably decided to switch some component off for some reason. Finally, if there is a red exclamation mark, your AVG 8.5 LinkScanner is in critical status; one or more components do not work properly. This is why we don't recommend changing the settings!

Step 3

On the left hand side of the screen are the Quick Links, which allow you to immediately access the most important and frequently used AVG 8.5 LinkScanner features. Use the Overview link to switch from any currently opened AVG 8.5 LinkScanner interface to the default one that we showed you in Step 1. Select the 'Update now' link to launch the AVG 8.5 LinkScanner update process immediately. It's important that you update regularly in order to stay on top of constantly evolving malware threats. If there are any updates, a small dialog box will appear telling you what you can install. Click OK to continue. When finished, you'll see a message saying 'Update was finished successfully'.

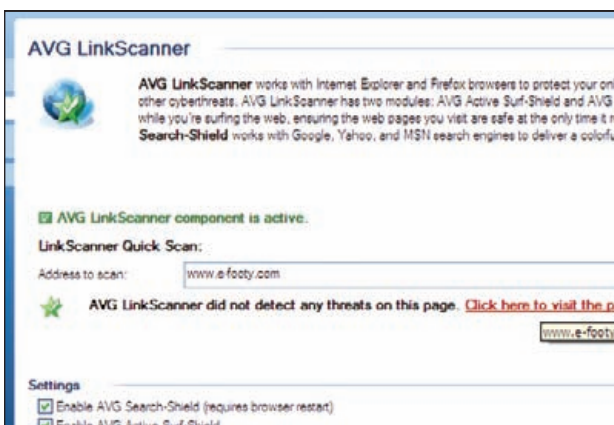
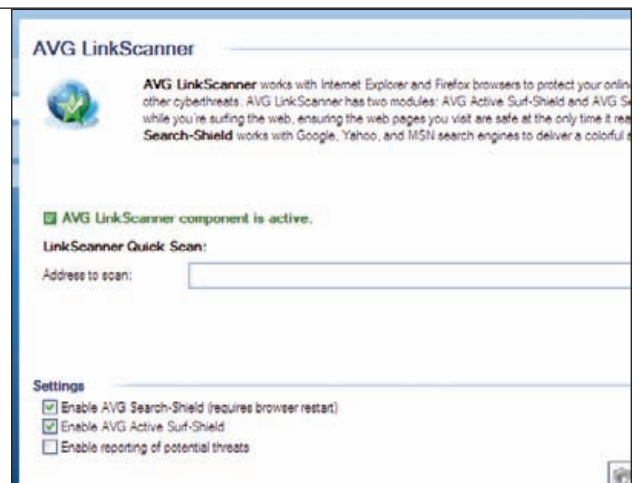


Step 4

At the bottom left corner of your AVG 8.5 LinkScanner interface is the Statistics section, which offers a list of information regarding the program's operation, including when the last update was launched, what version of LinkScanner you currently have installed, and what engine you currently have installed. In particular, you should pay close attention to the 'Last update' section. If you notice that it's been some time since you last checked for updates, you'll need to make sure you're connected to the internet and then click on the 'Update now' link immediately in order to keep your AVG 8.5 LinkScanner software up to date. If you go for too long without an update, you may be putting your PC at risk.

Step 5

Double click the LinkScanner component from the Overview menu. This will take you to the official AVG 8.5 LinkScanner page, which consists of two parts that you can switch on or off. The first is AVG Search-Shield, which activates notifying icons on searches performed in Google, Yahoo! or MSN, with LinkScanner having checked the content of these sites already. It supports both Internet Explorer and Firefox web browsers. The second is AVG Active Surf-Shield, which prevents you from accidentally becoming infected by 'drive-by' downloads and other exploits, ensuring the web pages you visit are safe at the only time that really matters: when you are about to click the link. Once again, both Internet Explorer and Firefox are supported. If for some reason you need to turn either of these components off, you can do so in the Settings menu at the bottom of the screen.



Step 6

You also have the option of manually performing a scan using the LinkScanner Quick Scan bar, also available from the AVG LinkScanner page. Simply type the address that you wish to check out into the data field, and then click Scan. LinkScanner will then scan the page to see if it is safe for you to visit. If it is safe, you'll see a message reading 'AVG LinkScanner did not detect any threats on this page', accompanied with a link that enables you to visit the page immediately. On the other hand, if there is a problem, LinkScanner will display a message saying 'AVG LinkScanner has found potential active threat delivery on that site'. If that is the case, the website may be dangerous and you should probably avoid it wherever possible.

Get full protection with Internet Security 9.0

Complete protection for everything you do online with AVG's excellent security suite



AVG Internet Security 9.0 the crown jewel in a range of AVG products designed to provide you with peace of mind and total security for your PC. It has a streamlined interface combined with more aggressive and faster scanning than ever before. More security features have been automated for your convenience, and new 'intelligent' user options to make security less of a bother for you.

It consists of software aimed at combatting viruses, spyware, spam, rootkits, and more. It also has its own

two-way firewall with advanced features over that which comes included with your Windows operating system, Identity Protection software to protect you from online fraudsters, and an E-mail Scanner to ensure your incoming messages are safe. You can also easily schedule scans so that they run without you having to manually configure them.

Best of all, we've got a 90-day trial of Internet Security 9.0 for you to try free on our cover CD. Simply install and follow this guide to find out how to use it.

Step 1

Once you've installed AVG Internet Security 9.0 on your PC, you can open it at any time using the AVG icon in the System Tray. When open, AVG Internet Security will look something like the screenshot to the right. The user interface itself is very similar to the AVG Free interface (see page 22), but the first thing you'll notice is that there are many more options with the full version. There's also the side menu containing three tabs: Overview, Computer scanner and Update now. Once again, we've discussed the role each of these play on page 22. Additionally, there is the Security Status Info at the top of the page, which will display either a green, orange or red icon depending on your level of protection, and statistics in the bottom left corner.



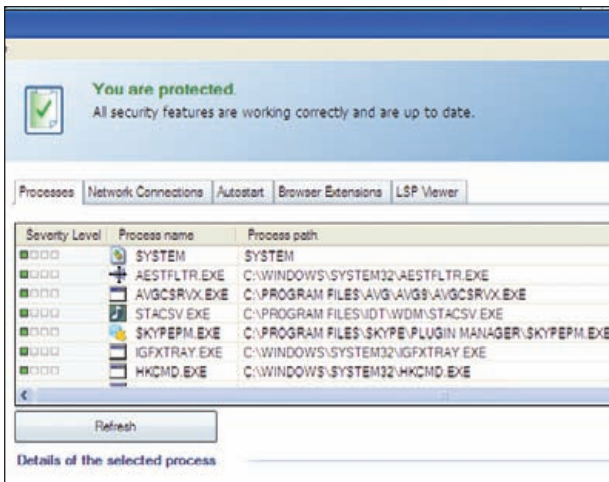
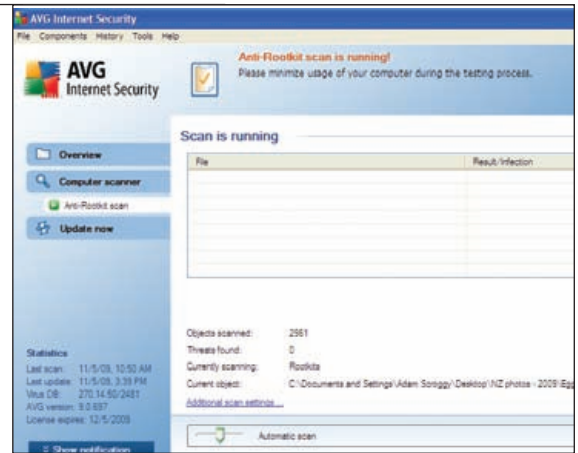
Step 2

The first few options include Anti-Virus, Anti-Spyware and Anti-Spam. The Anti-Virus component in AVG Internet Security 9.0 combines scanning for character strings, heuristic analysis and generic detection in order to ascertain the presence of threats. The Anti-Spyware component protects your computer from all kinds of malware that secretly gathers information from your computer, or adware that generates unwanted advertisements on your computer. The Anti-Spam component checks all incoming email messages and marks unwanted emails as SPAM. All of these components are taken care of during the complete scan which we'll look at in Step 4, but by double clicking each individual component you can ensure they remain up-to-date in order ensure your PC's maximum protection.



Step 3

One option that won't be covered by the complete scan, on the other hand, is Anti-Rootkit. This is a special tool that is only included with paid versions of internet security software. A rootkit is a program designed to take fundamental control of a computer system without authorisation by the system's owners and legitimate managers. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms. To run a rootkit scan, double click the 'Anti-Rootkit' component from the Overview tab and click the 'Search for rootkits' button at the bottom of the screen. The scan should take roughly an hour to complete.

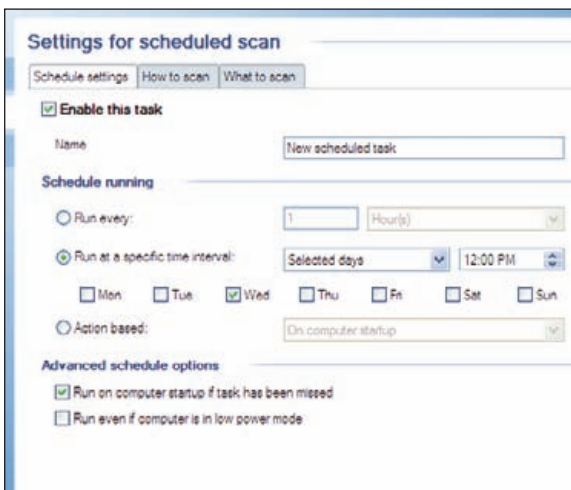
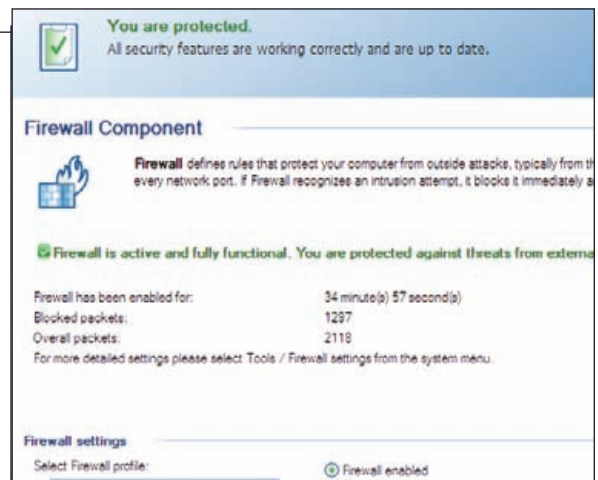


Step 4

Back on the Overview tab, double click the System Tools component to see a detailed summary of the AVG 9 Internet Security environment. The Processes tab displays a list of running applications that are currently on your computer; the Network connections tab shows a list of currently-active connections; the Autostart tab shows a list of applications that are executed during Windows system start-up; the Browser Extensions tab displays a list of plug-ins that are installed on your internet browser; and the LSP Viewer tab shows a list of Layered Service Providers (system drivers linked into the networking services of the Windows operating system).

Step 5

Double click the 'Firewall' button in the Overview menu to be taken to the Firewall component. Firewalls define rules that protect your computer from outside attacks. Your Windows operating system should already have a firewall, but if you're using Windows XP this firewall only controls communication coming in, and not communication going out. For this reason, we recommend the AVG Firewall, which blocks attacks in both directions. However, having both firewalls running at once can cause conflicts, so we recommend switching your Windows Firewall off. You can do this from Windows Security Center (see page 12 for a refresher on this). Once this is done, go back to AVG Internet Security 9.0 and select your Firewall profile.



Step 6

While you can run a scan at any time by clicking the Computer scanner tab and then selecting 'Scan whole computer', you can also schedule scans to save you the trouble of doing everything manually. In the Computer scanner tab, select 'Manage Scheduled Scans', and then select 'Add a scan schedule' on the following screen. The 'Settings for scheduled scan' dialog will open up. After giving your scan a name, you can choose between running a scan at regular intervals (say, every four hours) or running at a specific time interval (for example, every Wednesday at 12pm). You can also make an action-based scan, such as whenever the computer starts. You can further configure the scan by selecting the 'How to scan' and 'What to scan' tabs. When you're done, click Save, and all future scans will run according to the schedule.

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