Safety first

Security is something that all PC users need to think about – but why? We explore the origins of computer viruses and explain exactly why you need to protect your PC

These days it seems that computer security problems are rarely out of the news. Whether it's the latest virus spreading around the world, credit card numbers being stolen and sold or another database full of supposedly private information being leaked, it's easy to think keeping a computer secure is an impossible task. After all, if big companies and Government departments with huge security budgets get caught out, what are everyday users to do?

Fortunately the situation is nowhere near as bleak as it appears. Although the internet poses some very real security threats to home computer users, it is possible to protect your computer, your files and your identity. Better yet, all the tools you need are both simple to use and completely free. We have included some of the best on the CD, and later in this guide we'll explain how to set up and use each one. First, though, you're probably wondering just where these security problems came from in the first place.

Ancient history

When there's a problem, most people naturally want to know what's causing it before they set about finding a solution. In the case of online threats it's tempting to assume that, because they have only hit the headlines in the past few years, these problems are new. In fact, issues relating to computer security date back to a time before the internet itself really existed.

In the early 1970s, computers were enormous, expensive and rare. There was no internet, but a few computers were

▲ Security software has become vital as the threat from viruses has increased

connected together by ARPANET – a system built by the US military. The first ever email was sent over ARPANET in 1971 and, in the same year a programmer created and released the first ever computer **virus**. The Creeper virus transmitted itself across ARPANET and displayed a message on any computers it was able to infect: "I'M THE CREEPER: CATCH ME IF YOU CAN."

Others quickly followed. The second virus, Reaper, had a more noble calling: it leaped around the ARPANET network, checking computers for Creeper and destroying the earlier virus. Some have suggested it might have been created by the same programmer. The Rabbit virus was the first to have a dangerous effect, or 'payload' – after infecting a computer it would multiply and multiply until the computer, no longer able to cope, would crash.

The concept of **hacking** into a computer on a network followed shortly after. In 1984 a group of German hackers called the Chaos Computer Club spotted, and reported, a security flaw in the Deutsche Bundespost's Bildschirmtext computer system. When the Bundespost refused to do anything about the problem the club used the flawed system to illegally transfer over 130,000 Deutschmarks from a bank in Hamburg into its own account, notified the press, then returned the cash.

Not all early hacks were as community-minded. In 1986 Markus Hess, recruited by the KGB, managed to break into the computers of several US military bases through ARPANET. He was only caught after an astronomer, Clifford Stoll, was asked to track down the user who had stolen 75 cents worth of time on his laboratory computer. Hess was eventually jailed for espionage, while Stoll wrote a celebrated book, *The Cuckoo's Egg*, speaking about the incident.

Into the home

Although the hacks and viruses of the 1970s and early 1980s had the potential to cause real harm – at the height of the Cold War, Hess was searching military computers for files related to the word 'nuclear' – they had little impact on ordinary citizens. With the rise of the home computer in the late 1980s, however, this changed.

In 1986 two brothers from Pakistan wrote a virus that could easily spread on the **floppy disks** used by the first IBM PCs running the **DOS operating system**. The virus, known as Brain, did nothing malicious, choosing instead to sit on the disk, taking up valuable space, and the code even included the creator's home address and phone number. It spread around the world, leaving the brothers to fend off angry phone calls until they eventually disconnected the phone line.

The text-only DOS operating system disappeared in favour of Windows, and with the release of Windows 95 and the first common **internet service providers** came the kind of threats we're used to seeing today. In 1995 the Concept virus was the first 'macro' virus – it made use of the **macro** tools built into Microsoft Office to spread itself.

The Melissa (1999) and ILOVEYOU viruses (2000) spread rapidly by email, and produced a load of publicity. Both would examine the email address book on the infected computer and use it to email new copies of the virus to other users. Melissa generated so many emails in such a short space of time that many companies had no alternative but to turn off their email systems. ILOVEYOU did the same, even forcing British Parliament to shut down its besieged **servers** for two hours, while also annoying millions by replacing files on infected computers with copies of itself.

Follow the money

Since the year 2000 the number of Windows computers running both in offices and homes and the popularity of internet connections has vastly increased, but the popularity of viruses designed to cause damage to computers has fallen. This sounds like a good thing, but the truth is far more concerning. From the early days of computing to the end of the 1990s

Jargon buster

DOS Disk Operating System. The standard PC operating system before the dawn of Windows. DOS manages how files are stored on your PC. It is controlled through typed commands.

Encryption The science of scrambling data to hide it from prying eyes.

Floppy disk A small, rigid square of plastic used to store data. Inside the case is a circular magnetic disk (the floppy bit).

Hacking The slang term used to describe illegal access of computer systems by unauthorised users.

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

Internet Service Provider (ISP) A company that provides you with an internet connection, either for a fixed monthly fee or for the cost of local call charges.

Linux An operating system that runs on a variety of computers and can be freely modified and distributed by its users.

It's not just PCs

When we think about online threats many of us assume that only desktop and laptop computers are at risk, but this isn't really true.

Modern **smartphones** are, in effect, tiny internet-connected computers, and mobile viruses such as Cabir have already been discovered. The level of threat to users is currently thought to be low, but products such as Kaspersky's Mobile Security are already available to buy. Some smartphone security programs also allow you to wipe the information on your telephone by sending a text should it be lost or stolen.

Similarly anything attached to a home **network** including network hard disks, your internet connection itself and network cameras, can be at risk if attackers can gain access to the network itself. For this reason it's vital to ensure that any wireless networks are properly secured using **WPA encryption** – turn to page 28 to find out how.

A brief history of security threats

1971 – The Creeper virus spreads across DEC computers. A second virus, Reaper, spreads to destroy it

1974 – The Rabbit virus spreads and multiplies until the infected computer crashes

1982 – The Elk Cloner virus spreads via the floppy disks used by Apple II computers

1986 – The Brain virus does the same thing for IBM PCs running DOS, the text-only precursor to Windows

1988 – First computer firewall protection designed; Dr Solomon's Anti-Virus Toolkit software released

1990 – The first mutating (polymorphic) computer virus released

1992 – The Michelangelo virus causes media panic, but does little damage

1995 – The Concept virus spreads through Microsoft Word

1998 – Netbus tool, which gives complete remote control over an infected computer, released

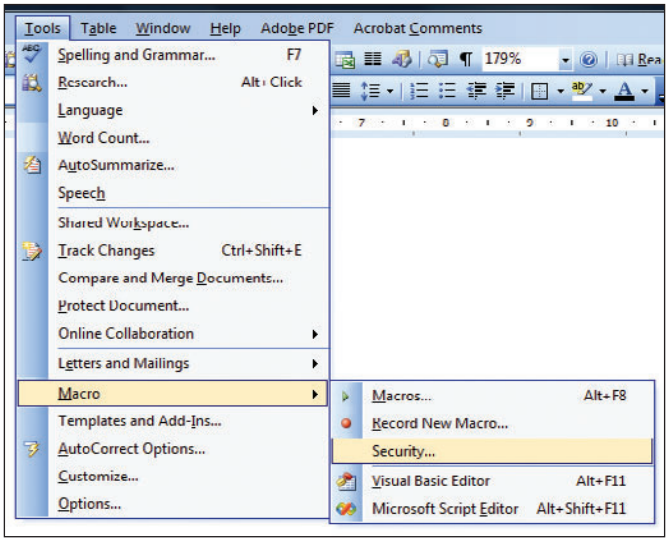
1999 – Subseven allows hackers to view the infected computer using its webcam; Melissa email worm causes significant problems for many email systems

2003 – The Blaster worm spreads rapidly across Windows computers

2004 – Mydoom email worm becomes the fastest spreading virus ever, launching an attack on the **www.sco.com** website

2007 – The Storm worm spreads to more than one million computers, creating a botnet

2008 – The first malicious scam software for Apple Mac OSX computers is found; Sinowal Trojan steals confidential data from computers; Conficker virus infects millions of computers worldwide



▲ The Concept virus spread by exploiting the macro tools in Microsoft Word

most viruses had one of two aims: to do nothing other than spread to more computers, or to annoy the infected computers' users. This annoyance could be a rude message, turning the mouse controls upside down so the computer became hard to use (the Ghost virus) or something more harmful such as deleting files from the **hard disk**. Today most malicious software has a different motivation: making money.

There may still be a few programmers creating viruses for their own perverse entertainment, but the majority of attacks are now focused on your wallet. Many computer infections are designed to take control of the computer behind your back, setting it up as a so-called 'zombie' computer that can be remotely controlled by the attacker. These computers, collected in a group called a 'botnet', are then used to send out junk emails. The Srizbi botnet is estimated to include around 450,000 computers, and at one point last year was sending 60 billion **spam** messages each day. The Conficker virus is believed to have infected between nine and 15 million computers, and uses all manner of clever techniques to hide itself from detection.

Having your computer infected in this way is obviously bad, but there are other infections that are possibly even worse. Some will sit on the computer, examining which websites are being visited and, when they recognise one – your bank, for example – will then monitor and record the password you type. If your bank's security requires the same details to be entered every time, this kind of attack could give criminals access to it. Others watch for credit card numbers then add them to lists that can be purchased by criminals – hundreds of millions of dollars have been lost to 'card not present' fraud, where stolen card details are used to buy goods online or over the telephone. This figure is growing, and remains the most common type of card fraud.Even Card ID theft is recording nowhere near the same amount of damage.

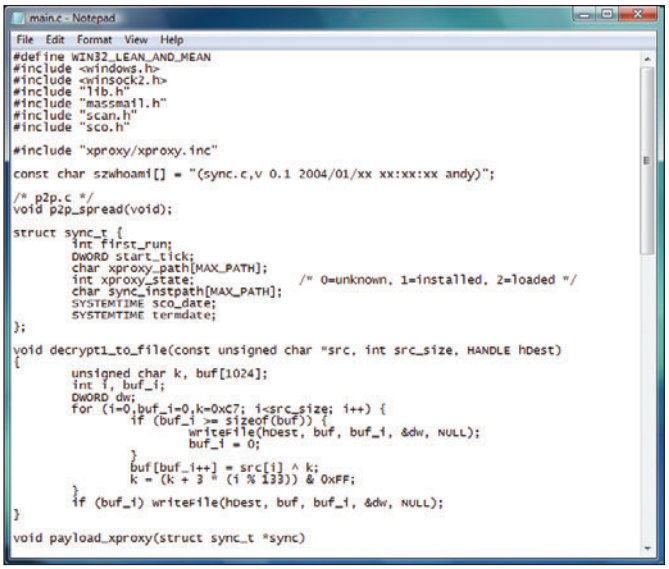
Another common threat comes from programs that claim to be security tools. These often trick users into installing them by claiming that the computer is already infected, then demand money to 'clean' the imaginary threats. A recent report showed that criminals could make more than $10,000 per day over the course of an attack of this kind, with around two per cent of the targeted users coughing up $50 for worthless software.

What's more, new technologies have presented new risks. **Wireless networks** have become common over the past five years, so it's important to remember that the internet isn't the only way for malicious users to gain access to your computers. Of course we'll explain how to protect against all these attacks later on in this Ultimate Guide.

Why Windows?

One question that's often asked is why only Windows computers seem to be at such great risk online when others – Apple Mac computers, for example, and those running versions of **Linux** – seem to be completely immune. Many people assume that Windows is full of security holes and Microsoft simply can't sort it out, but the truth isn't quite as simple.

It is true that other operating systems work in a way that's inherently more secure than Windows. Both Linux and Mac OSX owe much to an old system for computing that separates users into two groups: ordinary users and super-users. With this system, ordinary users are able to perform day-to-day tasks such as running programs and creating documents, but cannot add new programs or change the way the system works. In order to make any



▲ The Mydoom worm was the fastest spreading virus ever

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times

U.S.

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

POLITICS | WASHINGTON | EDUCATION

Computer Users Plot to Evade Virus

By JOHN MARKOFF
Published: Friday, March 6, 1992

SIGN IN TO E-MAIL
PRINT
REPRINTS
SHARE

The nation's personal computer users scurried yesterday to try to escape a malicious computer virus timed to erase data and programs today. But despite a growing level of worldwide concern, computer experts say that until desk-top computer users actually switch on their machines this morning there is no reliable way of telling how widely the virus has spread.

The new virus, which was apparently first detected in Germany last year, was given the name Michelangelo because it was set to erase data on computers made by the International Business Machines Corporation and on compatible computers when the virus program detects the date March 6, the Italian artist's 517th birthday.

The virus has been detected at hundreds of sites before it was able to do any harm. Among them were the New York offices of Drexel Burnham Lambert, where the virus was found in two machines during a precautionary search.

▲ The Michelangelo virus made headlines in 1992 but did little damage

changes to the system the user has to log in using a super-user account or, more usually, temporarily upgrade to the privileges of a super-user by typing in a special password.

This is an inconvenience for the user, but it is effective at limiting the damage any virus can visit: unless it can persuade the user to upgrade to a super-user, the virus will be unable to change any of the operating system files or install more malicious software. By contrast, most Windows user accounts have had complete control over the computer, so any virus that runs in that account has the potential to cause more damage.

Modern versions of Windows have made efforts to reduce this problem, but they haven't been entirely successful. Windows XP allows you to create Limited User accounts, but many people found that using these stopped some software from working. Windows Vista goes one step further with User Account Control. This system pops up a warning box every time an important change to the system was being made, but many Windows users decided to turn it off as they found it annoying.

Weakness in numbers

The weakness of user accounts aside, there's one key reason most current attacks are targeted at Windows computers: despite the increasing popularity of alternatives such as Linux, Windows remains vastly more popular. For example, just under 90 per cent of computers sold in January 2009 came with Windows. Writing a virus for Windows gives it the best possible chance of spreading widely and, if it's designed with financial gain in mind, the best possible chance of making the most money.

What's more, the vast majority of Windows computers run only a handful of versions of Windows, most of which can be attacked in the same way. By contrast, there are dozens of popular versions of Linux, all of which are subtly different, making it a harder system to target effectively.

This is not to say, however, that all other computers are immune from security problems. The Leap virus managed to attack some Mac OSX computers, although its method of spreading via the Apple iChat instant messaging program was fairly limited. More recently criminals attacking Apple users have borrowed a trick from Windows attacks, creating programs that attempt to con Mac users into paying for a worthless security service using exaggerated or fabricated threats.

Similarly, although Linux has few users when compared to Windows, the recent surge in its popularity has led to more threats targeting it. Most notably a virus called Badbunny, which spreads through the popular free office software Openoffice, infected Windows, Mac OSX and Linux. Fortunately Badbunny didn't do anything particularly dangerous, choosing instead to show an obscene photo of a man dressed as a rabbit and a female friend, and appears to have been created more to prove a point than to be released onto the internet.

Be prepared

You now know that computer security threats have been around for almost as long as computers themselves and can impact on any computer, but there's no doubting that Windows computers today are more at risk than they ever have been. The next step is to protect yourself, and in this guide we'll explain how to do just that without paying a penny more. To get started, simply turn the page.

◀ Subseven let hackers view infected computers by hijacking webcams

Jargon buster

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 that they can share data.

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

Server A computer on a network, such as the internet, that distributes information.

Smartphone Generic term for a combined handheld computer and mobile phone.

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.

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.

Wireless network Several computers connected without network cables.

WPA A secure form of protection for wireless networks.

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

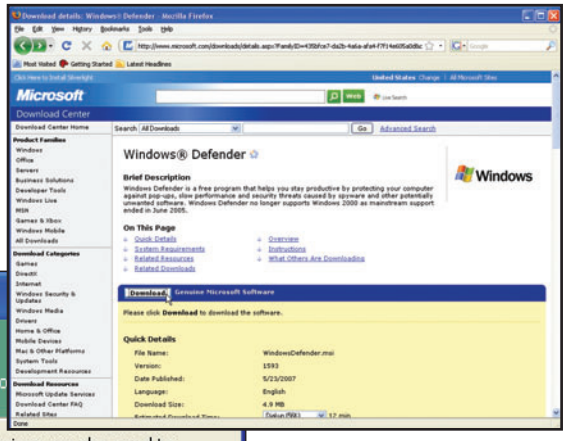
The way in which the dangers of the internet are portrayed by some parts of the media means it's surprising that anyone connects to it at all. From **hackers** to **viruses** and **spyware**, unknown threats and the fear they engender can seem overwhelming. But of course people do access the internet 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.

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 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.



▲ Download Defender online

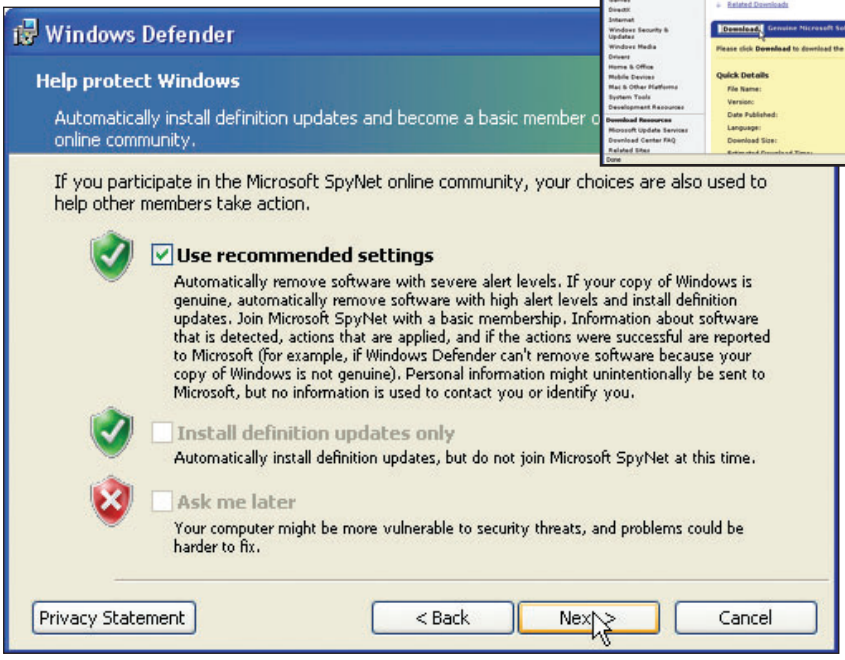
By the release of XP, Microsoft had begun to realise that internet security was a pressing concern for home users. XP included a **firewall** but it was not switched on by default. Given that many home users had no idea what a firewall was, let alone how to activate it, this didn't really help.

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.

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

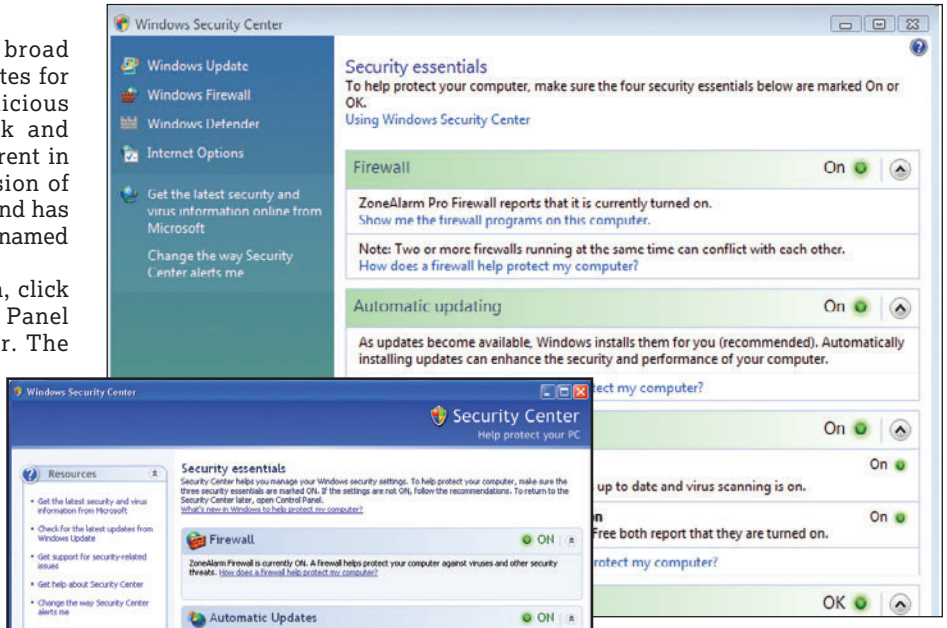


How Security Center works

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.



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

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

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 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

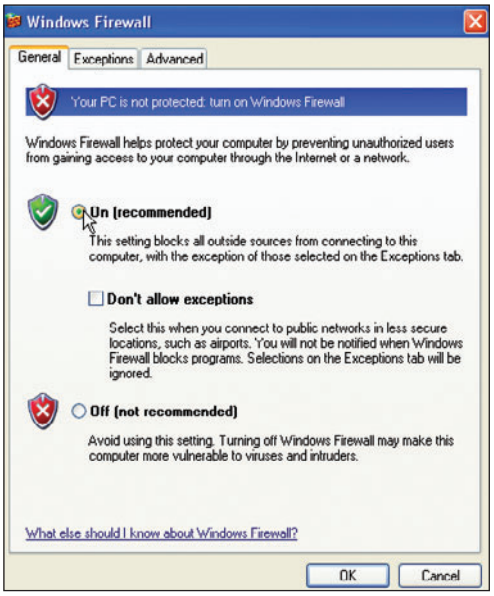
software developers can improve or fix flaws in programs. Windows is the greediest software of all for updates and, while they can be irritating, it's vital to download security updates. Criminals are constantly probing software for vulnerabilities that simply aren't known about. Windows is a tremendously 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 also see the box on page 11 on how to deal with **phishing** emails.



▲ Firewalls check data flowing to your PC

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

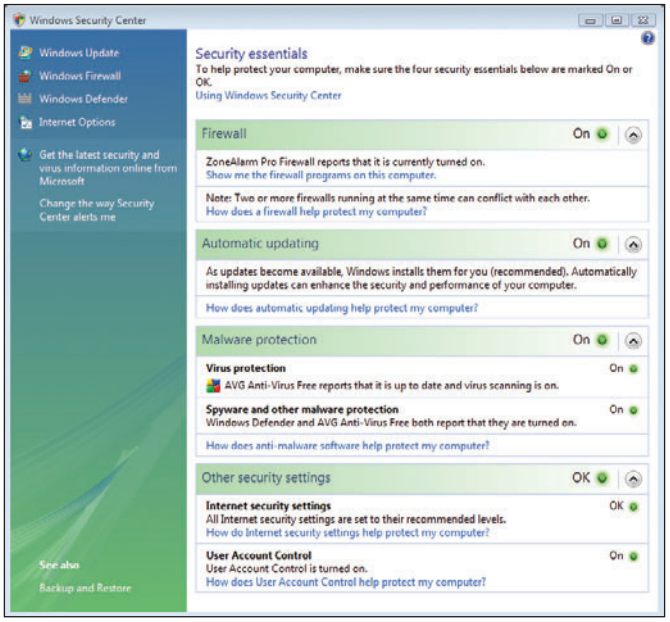
Parental control

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/fvbxl* 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.



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

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.

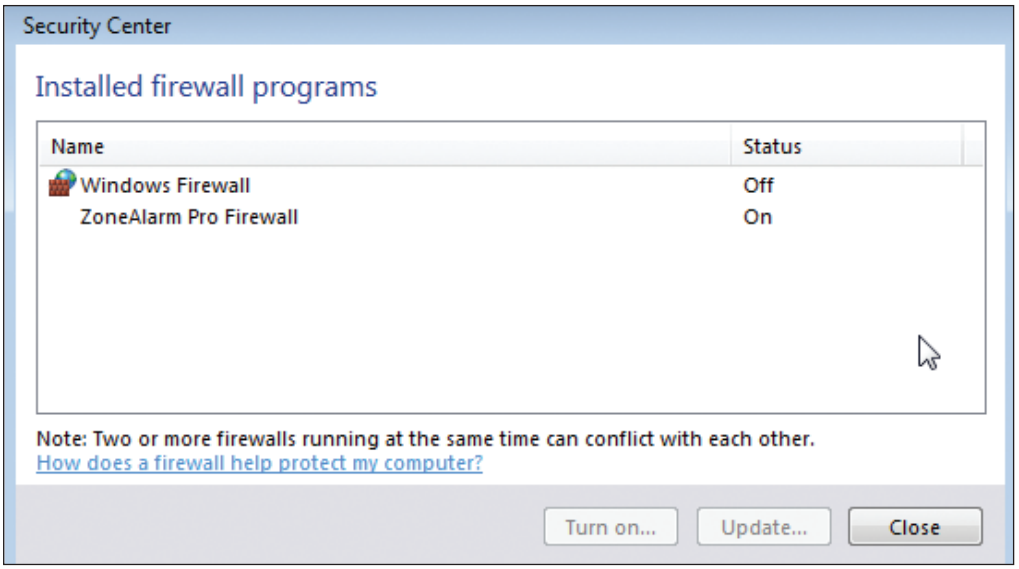
User Account Control is a useful, if controversial, addition to Windows. It's designed to prevent malicious software or other PC users from changing settings for applications but many people find it intrusive, as it requires them to click OK in a **dialogue box** when certain Windows tools are used.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

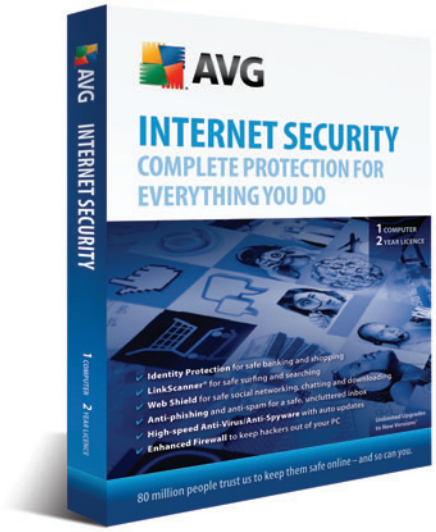
Operating system Governs the way the hardware and software components in a computer work together.

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.



Security software: what do I need?

When it comes to protecting your PC, the built-in tools in Windows aren't enough. We show you what additional software you'll need to stay safe

Software on the CD

You've just read that Windows includes security tools of its own but, unfortunately, these are far from perfect. While Windows Security features have improved over the years – especially with Windows Vista – some vital elements, such as **anti-virus** protection, aren't included at all, and the Windows **firewall**, for example, isn't particularly powerful. In order to make sure your PC is properly protected you will inevitably need to turn to third-party tools and utilities. So what exactly do you need to get hold of in order to stay safe, and how much do you need to pay for protection? In this section we will explain all.

▼ AVG's free anti-virus program provides effective protection

The magic number

There are dozens of different types of security products available on the market, but at the very least you will need to ensure that your computer is protected by three key tools: an anti-virus program, a firewall and an anti-**spyware** tool.

Anti-virus tools are probably the most familiar type of security software to the average user. At their most basic these scan for viruses, examining each and every file on the computer to discover whether or not any infections lurk inside. They do this by looking for a set of known 'definitions' – snippets of virus code that can be used to identify malicious software. Anti-virus tools will require updating on a daily basis to ensure your computer has the definitions for the latest virus threats. Most modern anti-virus tools also use a technique called 'heuristics' to watch out for new and unknown threats; put simply this involves watching out for programs that appear to behave like a virus.

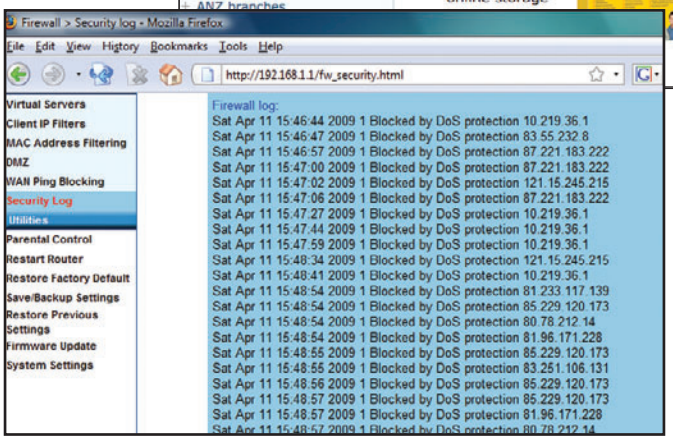
▲ Download Defender for free if you're using XP

While anti-virus programs are designed to find and remove any nasties that have made their way onto your computer, a firewall is meant to stop malicious software or hackers from getting onto it in the first place. It monitors the computer's connection to a **network** (either a home network or the internet itself) and examines information as it passes back and forth. Some of the most dangerous virus attacks of the last decade, including the Sasser

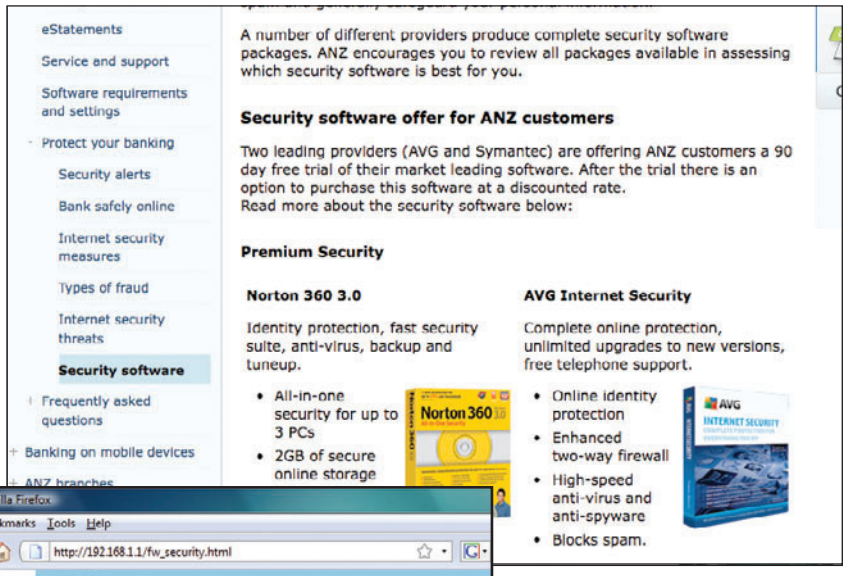
worm that infected high-profile computer systems (such as those of the British Coast Guard and US flight company Delta Airlines) through their network connection, can be easily blocked by a properly installed firewall.

Anti-spyware software works in much the same way as an anti-virus tool does, but with a very specific target. An anti-spyware tool will scan for, and remove, any malicious software that seeks to gather information about your computer use or your personal details. Many anti-spyware tools can also spot and remove **cookies** being used by websites to track your visits. As is also the case with anti-virus programs, anti-spyware tools need regular updates to remain effective at combatting these ever-present threats to your privacy.

As we explained on the previous pages of this Ultimate Guide, Microsoft has provided two of these tools free of charge to every Windows XP and Vista user. Both have a built-in firewall that can be set up to monitor any connection to a network while Windows Defender, which is included in Vista and is a free download for XP, can be used to scan for spyware. If these two tools are running properly you can, therefore, simply add an anti-virus tool. This isn't always the best or easiest way to protect your PC, though.



▲ As well as anti-virus software you'll need a good firewall



▲ Some banks offer free security software to their members

Suite dreams

There are two main problems with adding an anti-virus program to complement the tools already included by Microsoft. For starters, the Microsoft tools just aren't that good: the firewall, for example, is rather limited and somewhat difficult to configure. Second, it leaves you with three separate security tools to keep an eye on, and two different scans to remember to run. For this reason, many people prefer to install one completely new piece of software that covers all the bases: otherwise known as a security suite.

Almost every major security company makes an all-in-one security suite. To confuse matters, though, most of these companies have settled on the same name for this kind of product: AVG (***www.avg.com.au***), Norton (***www.symantec.com)***, Kaspersky Labs (***www.kaspersky.com.au***) and McAfee (***www.mcafee.com***), for example, all sell a product called Internet Security.

At the very least, most security suites include an anti-virus tool, a firewall and anti-spyware protection, although many add much more to the equation. Some include parental control software in order to limit what children can access on the computer or the internet. Many include anti-spam programs to delete annoying junk emails, and some will automatically block the websites used by so-called **phishing** scams. Some even go as far as including a few **gigabytes** of online space for you to store backup copies of your most precious files.

The quality of the tools and services included in these suites varies, but they tend to have several advantages over the security features built into Windows. Most importantly, they usually include a two-way firewall. This monitors not only what information is coming into your computer through the network connection, but also what information is going out to the internet. This allows the software to watch out for programs that are acting suspiciously, and means that even if spyware does get onto the computer it'll have a hard time sending any information back to its criminal owners. The standard firewall built into Windows XP can't do this and, although Vista's firewall can, you'll need to delve deep into its settings to find the necessary options.

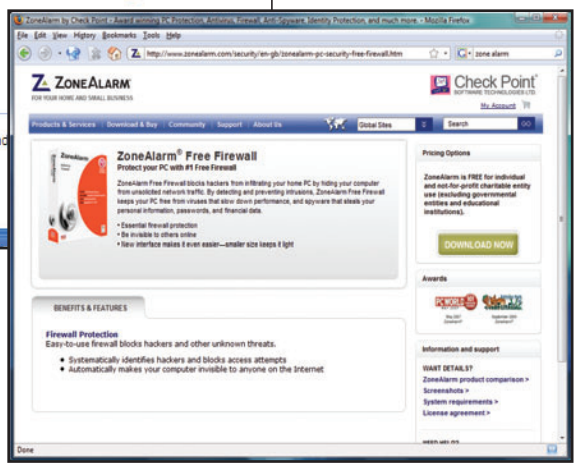
Route to success

If your computer connects to the internet via a **USB** broadband **modem** or **dial-up** connection, you'll need to rely on your computer and software for protection from viruses and other threats. If you connect via a **router**, though, it might be able to help.

Most routers include some sort of internet firewall. This will help to block any intruders or malicious software that attempts to enter your network from the internet. We don't recommend relying on a router's firewall alone – it's best to have a two-way software firewall to prevent any programs passing information out to the internet – but your router firewall can be a useful second line of defence.

Another handy security feature built into some routers is the ability to block Ping messages. A Ping is a message sent across a network to see whether a network address is active, and normally a computer will respond to acknowledge that it is there. These signals are sometimes used by hackers scanning for possible targets, though, so blocking or ignoring them can be useful.

▲ AVG's all-in-one Internet Security package allows you to monitor your protection in one place



▲ Zone Alarm monitors the information going in and out of a PC

Keep it together

Besides having more tools and a better firewall, the key advantage of any security suite should be the convenience that it offers. A good security suite will allow you to manage all the security tools on your computer in one place, and should take care of just about everything for you by updating itself daily and scheduling automatic scans from time to time. It will also allow you to keep an eye on your computer's security by checking just one program window rather than those of three or more different tools.

For most users, then, an all-in-one security suite will provide great protection, but as always there's a price to pay for convenience: most internet security suites cost around $100. Most companies sell products that are valid for use on three computers, and if you have three PCs these work out at a very reasonable $33 per computer per year. If you only have one computer, though, the price can seem annoyingly high. Not to worry, though – if $100 is just too much for you to swallow, all the software you need can be found for free, and much of it has been provided on the CD accompanying this guide.

Free for all

Sadly we're not aware of any completely free security suites for Windows computers. Although many companies make free security products, and some also make security suites, in most cases the full suite is an upgrade that you'll need to pay for. If you want a free security system that's a bit more effective than what Windows has to offer then, you'll need to rely on finding a selection of individual programs that can be found on the web.

We mentioned earlier on in this Ultimate Guide that, at the very least, every single Windows computer needs an anti-virus program to work alongside the firewall and anti-spyware tools built into Windows. Fortunately there are several good anti-virus tools that can be used at no cost.

Perhaps the best known free anti-virus tool is AVG Free. AVG sells its anti-virus tools to both home users and businesses, but for years now it has also given away a basic version of its anti-virus tool for free. It has some limitations compared with the suite software, and doesn't scan for rootkits – nasty infections that hide deep within Windows – but as long as you set up AVG to scan your computer regularly it's an effective prevention against most computer infections. You'll find a copy ready to install on the cover CD included with this Ultimate Guide, as well as a 90-day trial of the AVG Internet Security suite 9.0 software so you can see what a full suite is like.

Great walls of fire

With AVG installed your computer will be protected against viruses, but we recommend going at least one step further by adding a two-way firewall. Like the firewalls included with paid-for security suites, these will monitor any communications from your computer to the internet, as well as any nasties or **hackers** that might attempt to come in from the other direction.

The best-known free firewall is Zone Alarm. This monitors the information going in and out of the computer, keeping a list of which programs are allowed to contact the internet and which shouldn't be talking to anyone. If a new program attempts to contact the outside world, Zone Alarm will ask if you want to stop it.We've shown you how to set up and use Zone Alarm on page 24 of this guide.

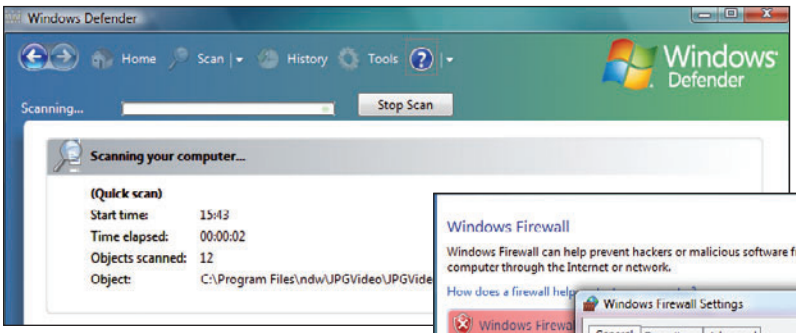
Something for nothing

Before buying or downloading security software, it's worth taking a minute to check that you haven't been offered any for free.

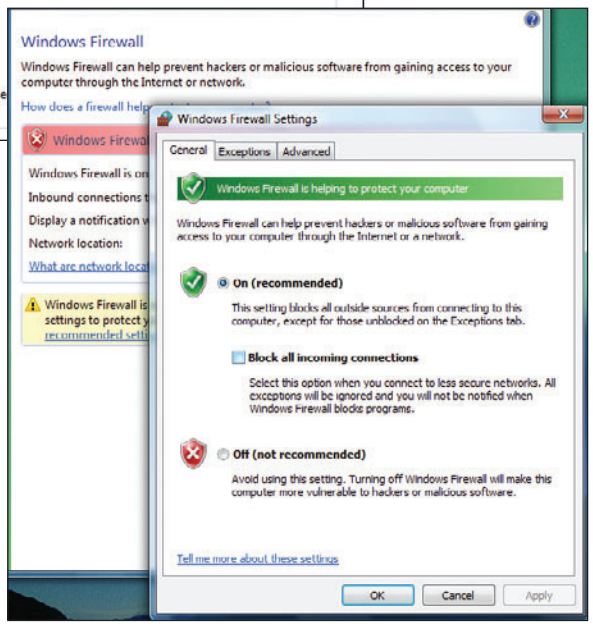
Some **ISPs** offer security software to their customers, so check yours first. Remember that switching from one ISP to another can take a fair bit of time, and if you are on a fixed-term contract you'll be liable for your current fees until the end of that contract, so switching ISP to one that gives you free software won't always be the cheapest option.

Similarly, check your bank and credit card providers to see if they offer anything. With card-not-present (CNP) fraud currently costing financial companies huge sums of money, some may be prepared to pay for software to limit the risk to their customers.

Either way, the best recommendation we can provide is to do a little bit of research online before going out and buying the latest security package. Find out what will suit you best and then go from there!



▲ Windows Defender guards against spyware



▼ The Windows Firewall provides basic one-way protection

Counter intelligence

Finally, don't forget to protect against spyware. Microsoft's own Windows Defender works fairly well, and Vista users should be sure to scan with it every few weeks – click Start and type Defender to find the program. The Windows Update tool will automatically keep Defender up to date with the latest definitions, and a quick scan of your computer will only take a few minutes. Windows XP users can download Defender from the Windows website at ***www.tinyurl.com/dakdan***.

Besides Defender, there are several good free anti-spyware tools. Lavasoft's Ad-Aware is one of the best known, and you'll find a full version of Ad-Aware 2009 on the CD with this Ultimate Guide. We've also included a full version of PC Tools' excellent Spyware Doctor.

Anything else?

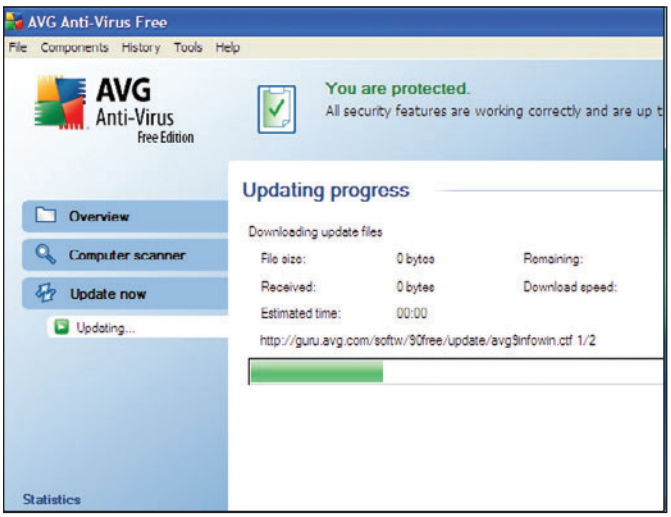
Whether you choose to purchase an all-in-one security suite or install a hand-picked collection of free tools, your PC should be in pretty safe hands with the right mix of third-party applications. There are, however, a couple of other security matters that you might want to consider.

For starters, remember that no matter how good your security software may be, there's still a chance that you might lose files from your PC – a new and particularly virulent attack might bypass your software or – something which is more likely to happen – your **hard disk** itself may simply fail. With this in mind, it's vital to ensure that you have a backup copy of all your most important documents to ensure you don't have to face the heartache of lost files. We've included a copy of Paragon's Drive Backup software on the free CD included with this guide, and you'll find advice on how to use the program starting on page 68.

There may also be occasions when you will want to remove all the files from a hard disk completely – if you're selling a computer, for example, and don't want the new owners to get a glimpse into your private PC world. If that's the case, we've also included Paragon's Disk Wiper tool on the CD to help you delete information permanently.

Finally, remember that your computer is not the only place from which confidential information might be stolen. If you store documents on a portable disk, such as a USB memory key or portable hard disk, it's worth taking precautions to protect them in case the disk is lost or stolen. In our increasingly mobile world, this is becoming more of a problem every day. Truecrypt (***www.truecrypt.org***), a free scrambling software package, can be used to securely **encrypt** all the data stored on a portable disk.

So now that you know exactly what kind of tools you'll need to ensure maximum protection for your computer, you can turn the page to start finding out how to use them.



▲ All-in-one security suites update regularly, saving you the hassle

Jargon buster

Anti-virus Software that detects, repairs, cleans, or removes virus-infected files from a computer.

Cookies Text files generated by websites and stored on your hard disk.

Dial-up A component of Windows that allows PCs to connect to the internet using a modem.

Encrypt To scramble data so it can only be read by the sender and authorised recipient.

Firewall Software or hardware that prevents unauthorised access to a computer over a network.

GB Gigabyte. A measurement of storage.

Hackers People who break into computers.

Hard disk A high-capacity disk fitted in almost all PCs and used to store files.

Internet Service Provider (ISP) A company that provides you with an internet connection.

Modem Device enabling computers to communicate over a phone line.

Network A way of connecting several computers and devices.

Phishing Internet fraud that tries to trick you into revealing personal details.

Router A device used to connect more than one computer to the internet.

Spyware Software installed to monitor and report back on a computer's use.

Universal Serial Bus (USB) A standard that allows quick and easy connection of peripherals.

Worm A program that transmits and copies itself over a network.

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.

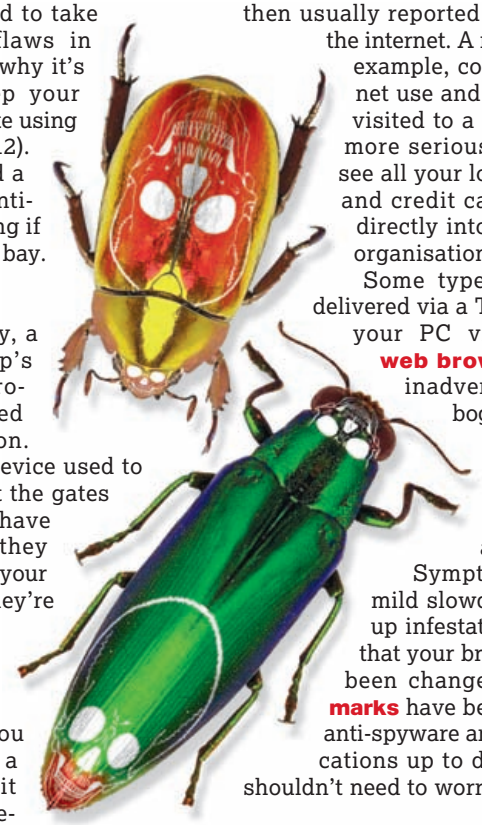
In some cases it's possible to have a virus infection without even knowing it. Only a thorough virus scan will reveal and remove it.

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

Software on the CD

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.

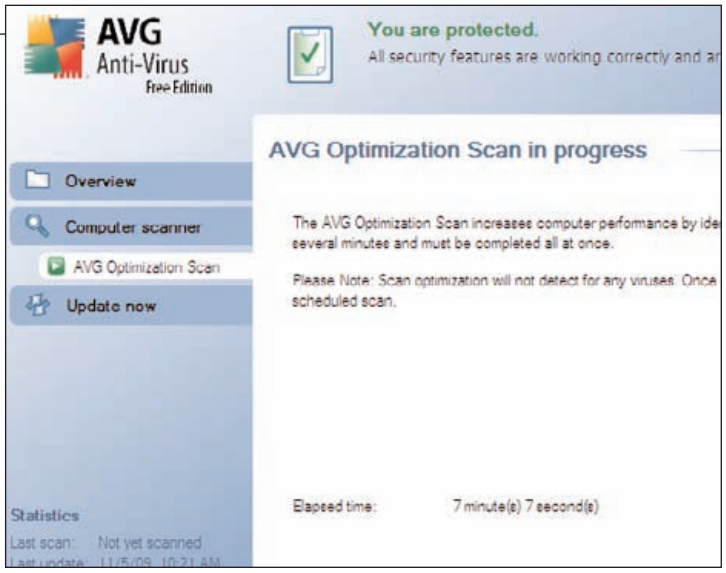
It has always been the philosophy at AVG that everyone should have the right to basic computer security at no cost, and tens of millions of users have taken advantage of AVG Free software since AVG first offered its free protection package back in the year 2000.

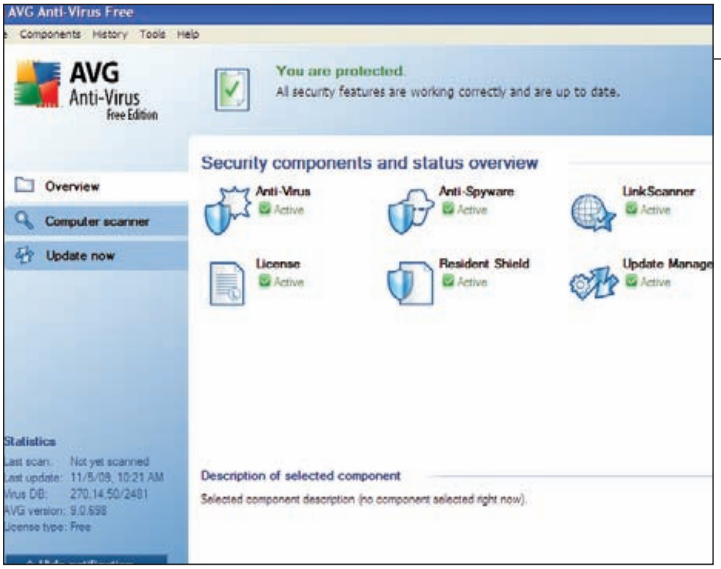
With AVG Free, you can scan your PC for viruses and spyware, as well as scanning websites and incoming emails for signs of danger. Scanning is easy, and we'll show you exactly how in this guide.

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.



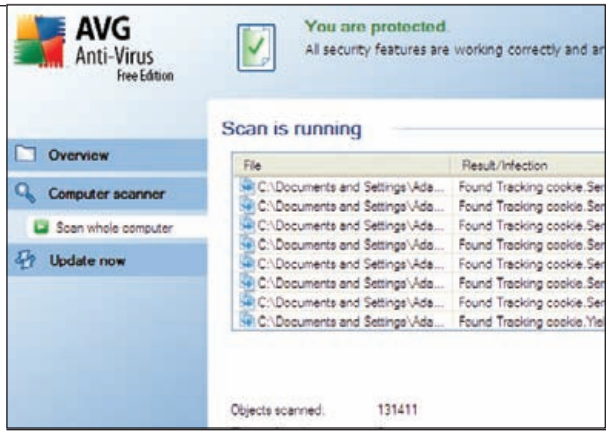


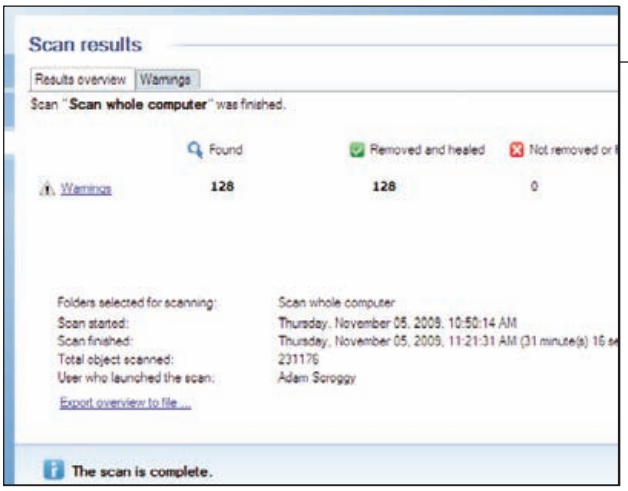
Step 2

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 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.



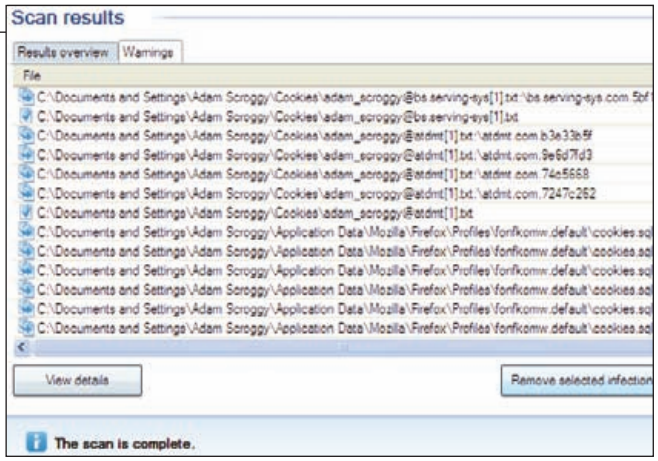


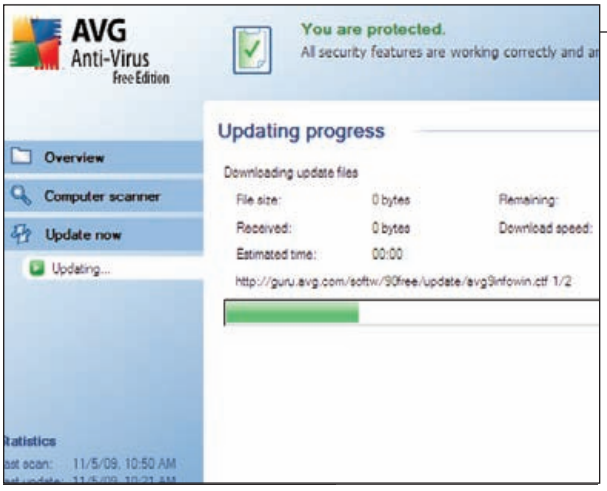
Step 4

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 fault. 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

Software on the CD

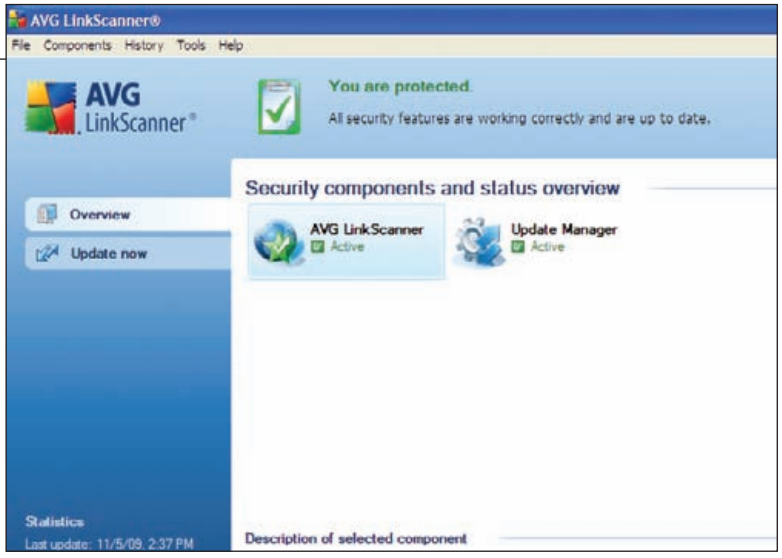
One of the least understood AVG components and the one that causes most confusion is LinkScanner. What does it do? Does it scan webpages, compare URLs against a blacklist, or what?

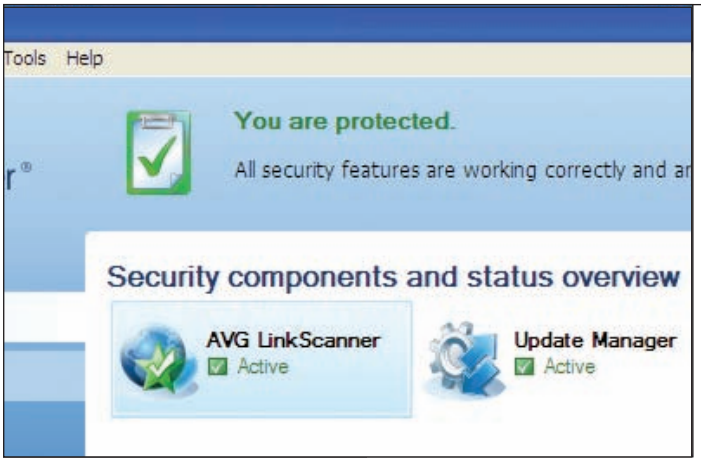
As you may know, there are currently around 30,000 new viruses and other malware hitting antivirus researchers' labs each day. Most spread via the web. This is the aspect of malware that LinkScanner deals with. It scans web page content as that content is delivered to your computer, and identifies delivery 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.



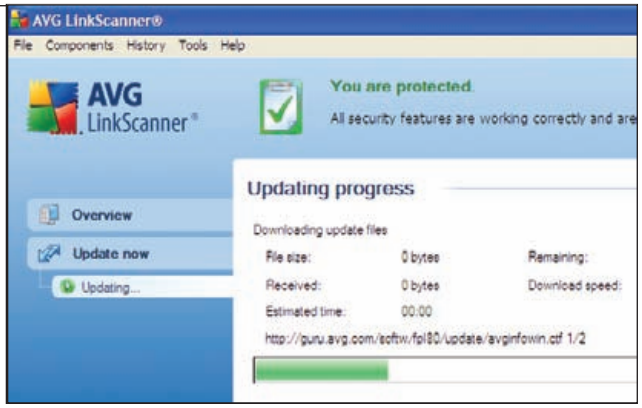


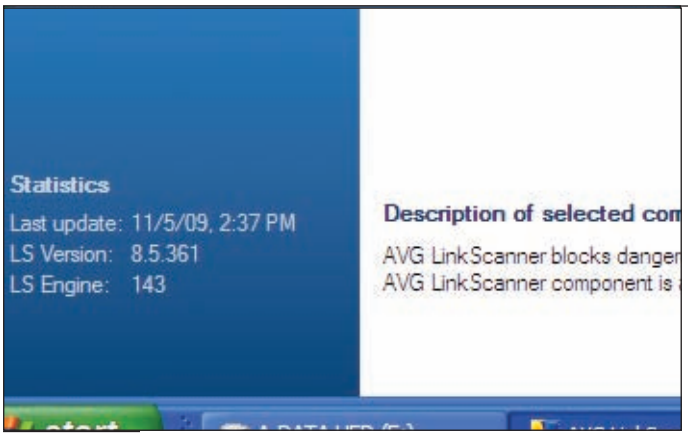
Step 2

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'.



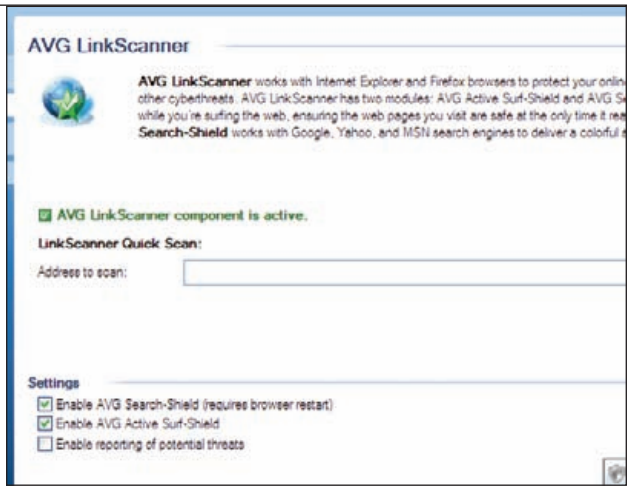


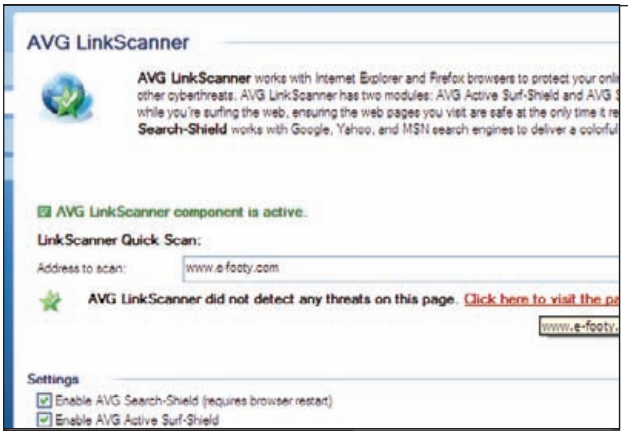
Step 4

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

Software on the CD

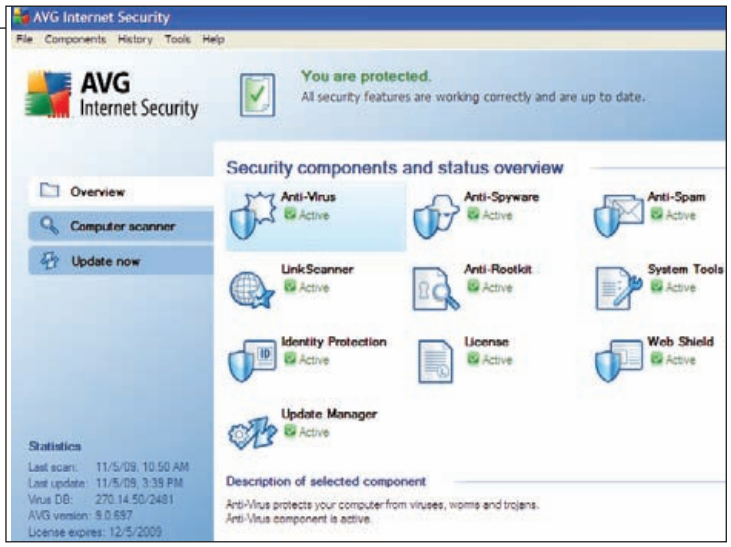
AVG Internet Security 9.0 the crown jewel in a range of AVG products designed to provide you with peace of mind and total security for your PC. It has a streamlined interface combined with more aggressive and faster scanning than ever before. More security features have been automated for your convenience,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

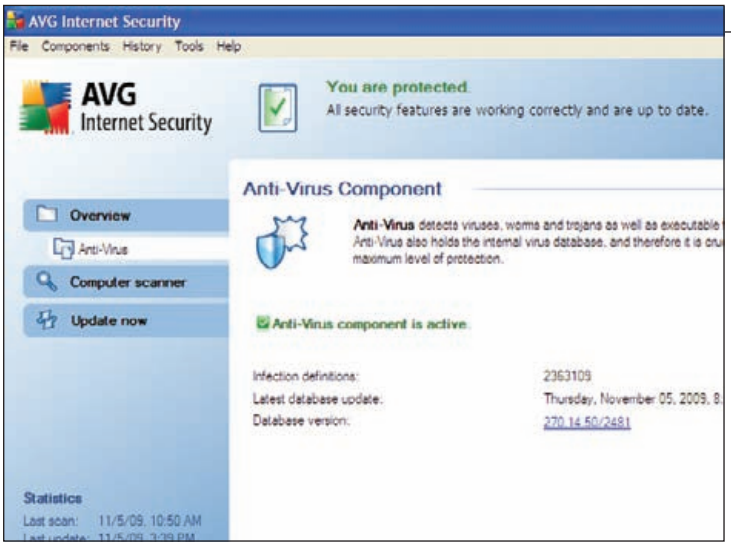
It consists of software aimed at combatting viruses, spyware, spam, rootkits, and more. It also has its own two-way firewall with advanced features over that which comes included with your Windows operating system, Identity Protection software to protect you from online fraudsters, and an E-mail Scanner 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.



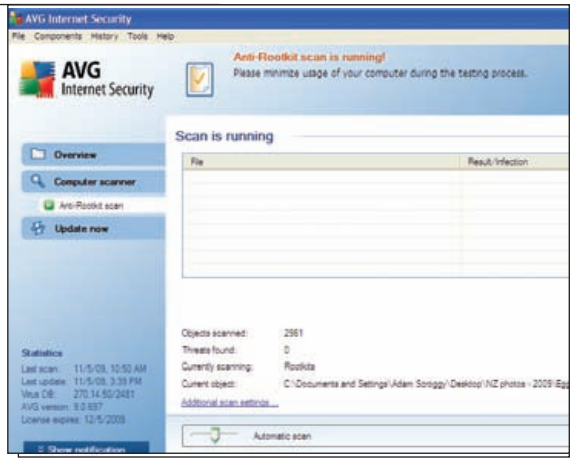


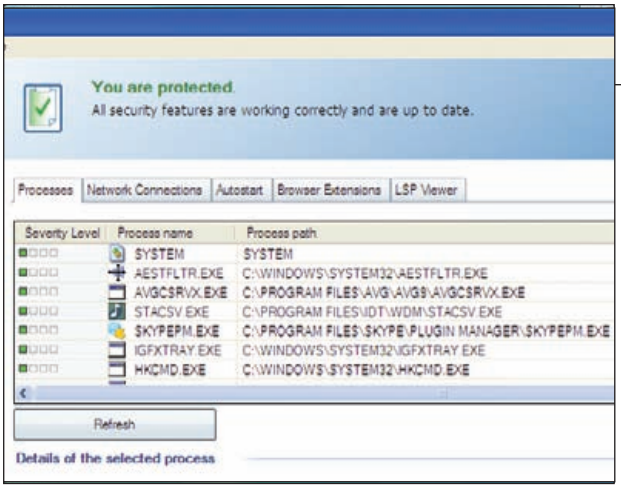
Step 2

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 detention 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.



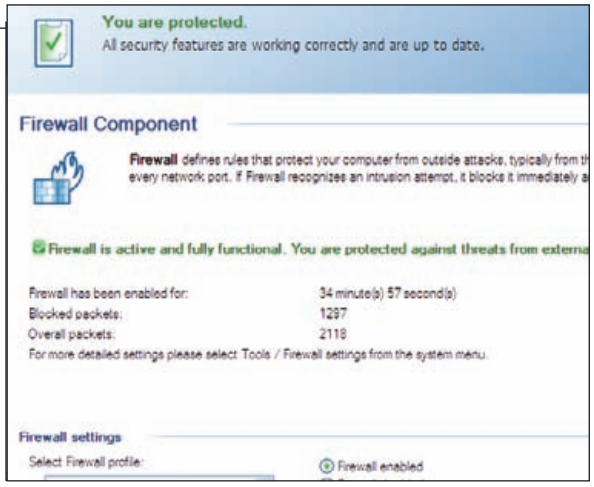


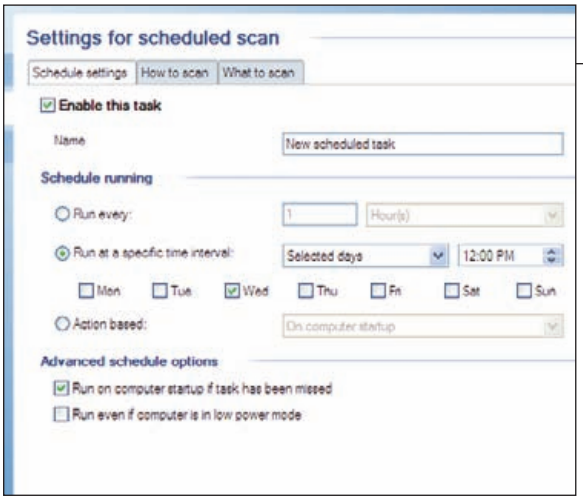
Step 4

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

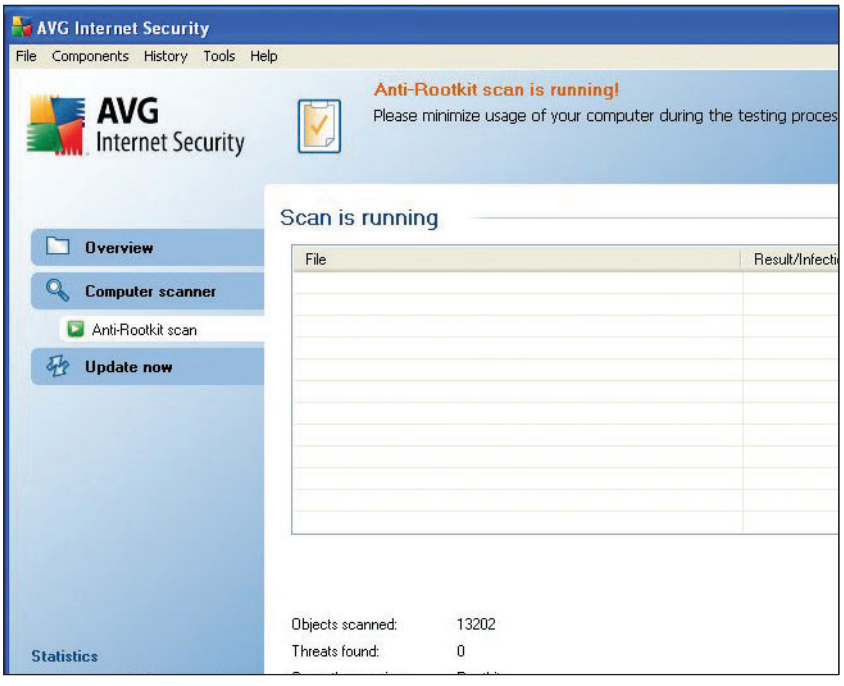
While you can run a scan at any time by clicking the Computer scanner tab and then selecting 'Scan whole computer', you can also schedule scans to save you the trouble of doing everything manually. In the Computer scanner tab, select 'Manage Scheduled Scans', and then select 'Add a scan schedule' on 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.

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

The 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

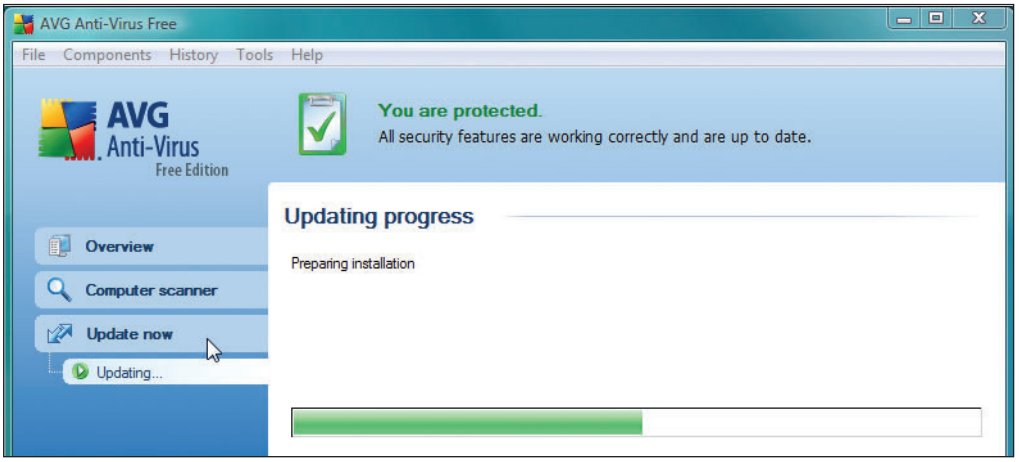
Occasionally, a virus or other form of malware will make it plainly obvious when it has infected your PC – some will even flash up messages proudly claiming your PC as their latest scalp. However, the vast majority will prefer to keep their presence as low-key as possible – the longer they can stay undetected,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

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.

Malicious software removal tool

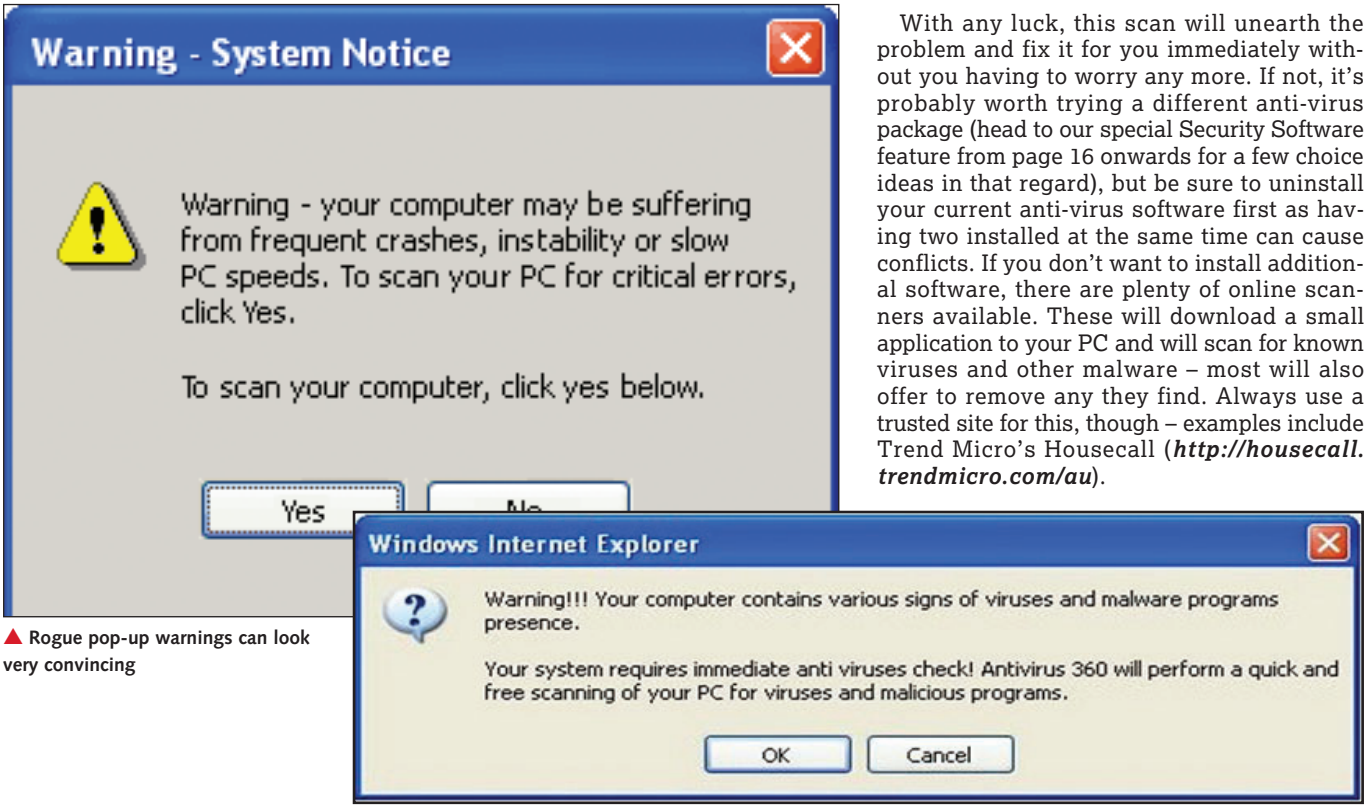
If you are having trouble removing a virus or just want to add an extra level of protection, it's worth installing the Windows Malicious Software Removal Tool from Microsoft.

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/malwareremove**. Once installed, it will then download each month's updates and scan your PC automatically.



▲ Rogue pop-up warnings can look very convincing

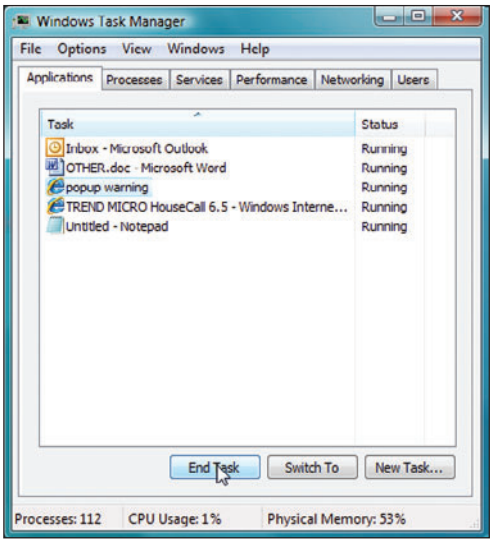
With any luck, this scan will unearth the problem and fix it for you immediately without you having to worry any more. If not, it's probably worth trying a different anti-virus package (head to our special Security Software feature from page 16 onwards for a few choice ideas in that regard), but be sure 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,

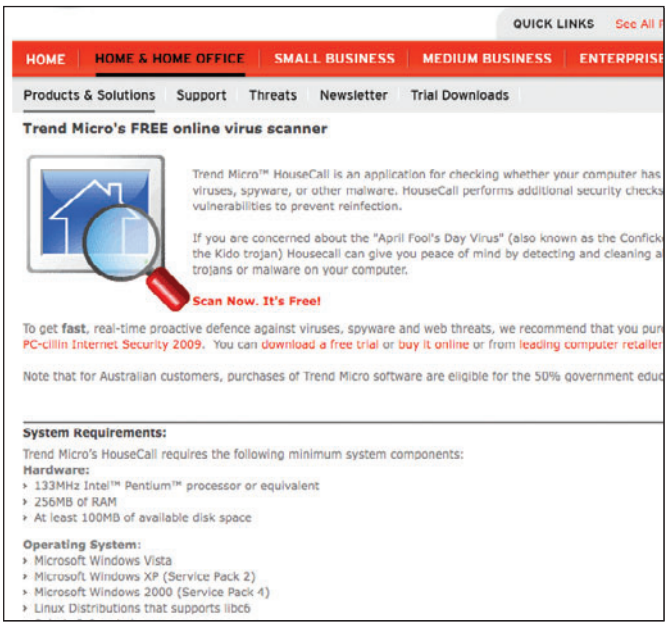


▲ Always use Task Manager to get rid of suspicious pop-up warnings

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.



▲ 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***, 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.

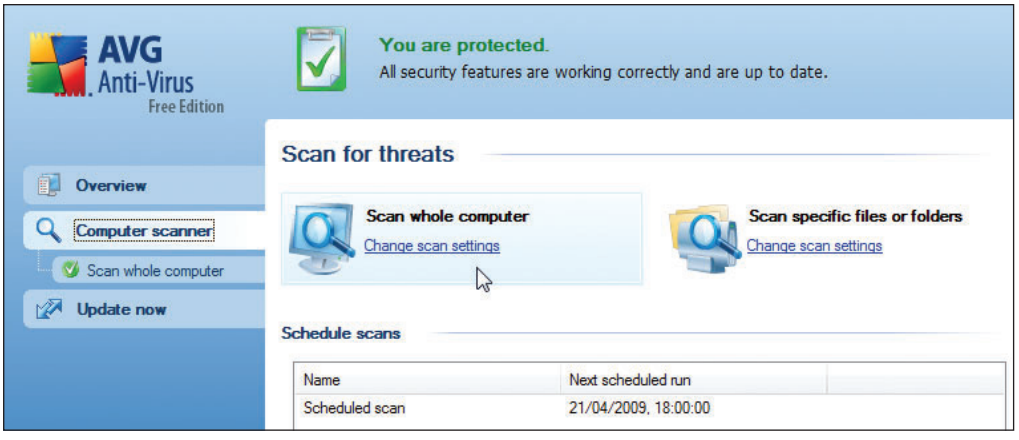
However, it could also be the work of a rootkit. Most free solutions don't include anti-rootkit scanners, and although the paid anti-virus or internet security solutions generally do, they don't include it as part of their scan. With this in mind, you should try a separate scan for rootkits, which is 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.



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

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.

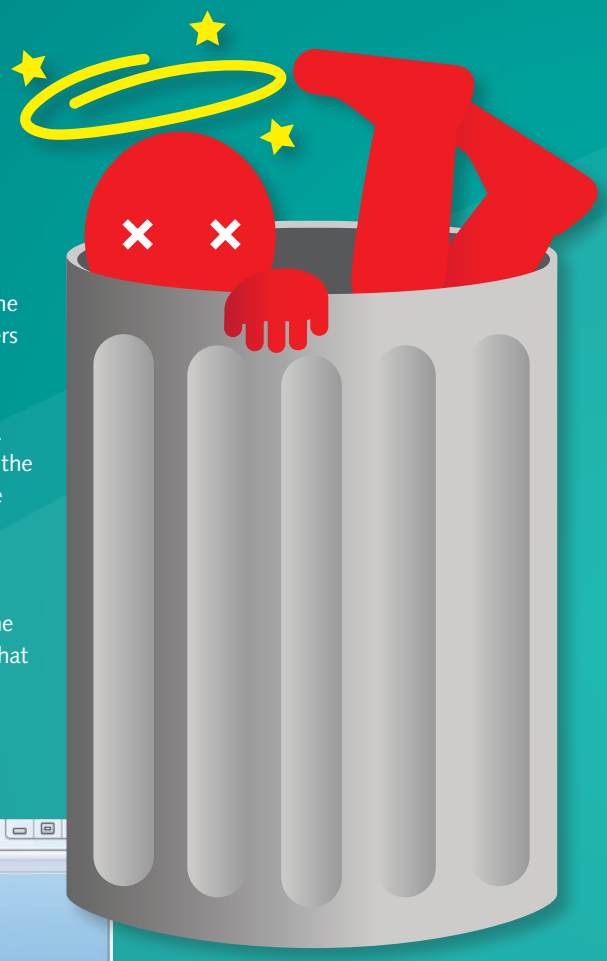
Spyware Software installed (usually surreptitiously) to monitor and report back on a computer's use.

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.

AVG LinkScanner

STAY ONE STEP AHEAD OF THE DATA SNATCHERS

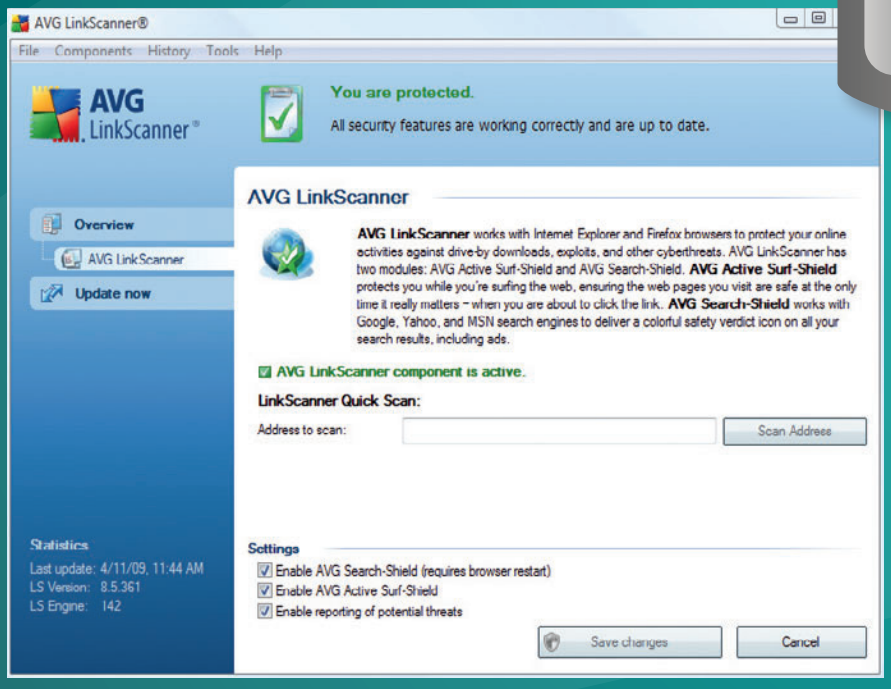


Data Snatchers hide in even the most trusted websites, to steal your personal information: credit card details, private files and your identity. The Data Snatchers move fast - a page that was safe yesterday may not be safe today – and your antivirus and firewall won't help you.

Antivirus? Firewall? LinkScanner®?
Antivirus and firewall software is no longer enough. The threat has evolved. Only **AVG LinkScanner®** can protect you from the Data Snatchers and raise your internet security to the next level.

Look before you click
AVG LinkScanner® puts you one step ahead of the Data Snatchers by analysing every website behind every link you click or type into your internet browser. **LinkScanner®** lets you know if the webpage you are visiting is safe before you even get there.

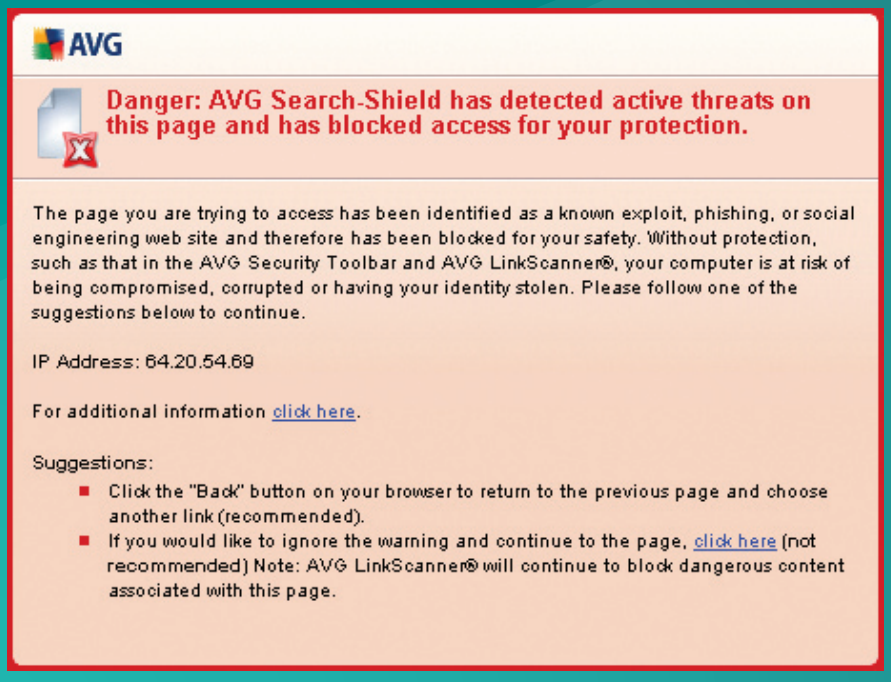
Instant and Real-time
LinkScanner® works in real-time – 24/7/365 – total protection that is one-step ahead of the Data Snatchers. Installation is simple, free, works with your existing antivirus software, and won't slow down your computer.



With AVG LinkScanner you can stay safe wherever you go online, whatever anti-virus you use

Why AVG LinkScanner®
There are millions of poisoned web pages out there. They can live on familiar, big-name sites – and they can come and go within hours. Just clicking on one can get you into trouble. You can end up losing your money, your identity and your most precious digital memories.

AVG LinkScanner® checks each web page in real-time before it opens on your PC. If LinkScanner sees trouble ahead, it stops you. It's quick and easy to install, runs smoothly alongside other major brands of security software and it's free.



AVG LinkScanner won't let you visit web pages it thinks are dangerous

AVG LinkScanner® has a two-fold approach to your safety online:

- LinkScanner Search-Shield scans search results and places a safety rating next to each link, so you know where it's safe to click.
- LinkScanner Active Surf-Shield scans the page behind any link you click on or any web address you type into your browser. If the page is poisoned, it stops you from opening it. (This happens so quickly that you don't even notice it.)

The fact that **AVG LinkScanner®** works in real time makes it unique. The software doesn't rely on "blacklists" of sites that have previously been poisoned, but instead checks for active threats right before you arrive at a page.

The Threat Landscape

If you still haven't downloaded **AVG LinkScanner®**, we'd hate to worry you, but ignorance is not bliss in the current online environment:

- 95% of online threats are web-based and cannot be stopped with anti-virus software alone.
- AVG sees 100,000–150,000 threats a day, 30,000 of these are new each day.
- Online criminals set up their own websites or poison legitimate ones (even just single web pages).
- 60% of all pages hosting web threats are poisoned for less than a day, making the threats difficult to catch unless they are viewed on the actual page in real-time. This makes **AVG LinkScanner®** essential protection.
- One in eight web users will unknowingly come across a poisoned page at least once a month.

Online criminals are getting smarter. But we're always ahead of them. Our real-time **AVG LinkScanner®** software detects threats at the only time it matters – before you arrive. And the software is free, so why not just install the version provided on the cover CD? The Data Snatchers don't hang around, why are you? Install **LinkScanner®** now for complete peace of mind.

QUICK FACTS:

- There are millions of active **AVG LinkScanner®** users.
- **AVG LinkScanner®** is already an essential and standard part of AVG's security software.
- One in eight users has been saved from poisoned web pages with **AVG LinkScanner®**.

How AVG LinkScanner® is tough on threats:

- Scans the pages behind all the links you click or type into your browser.
- Scans the results of web searches in Google, Yahoo! and MSN so you know whether a page is safe before clicking on it.
- Uses the intelligence gathered by a global community of online threat detectors.
- Analyses individual pages rather than entire sites because single pages may be threatened.

How AVG LinkScanner® is easy on you:

- Compatible with current products from other major security brands, so you can continue to use your existing software with **AVG LinkScanner®**.
- Runs silently in the background - you won't notice it until a threat is detected.
- Minimal use of system resources – it won't slow down your computer.
- Easy to install and run.
- Protects you immediately without need of a system scan.
- Automatically updates whenever a new threat is found.

AVG LINKSCANNER IS FREE FOREVER AND INCLUDED ON THE COVER CD!

Easy backup

Here are two quick and easy ways to back up your personal files and keep them safe

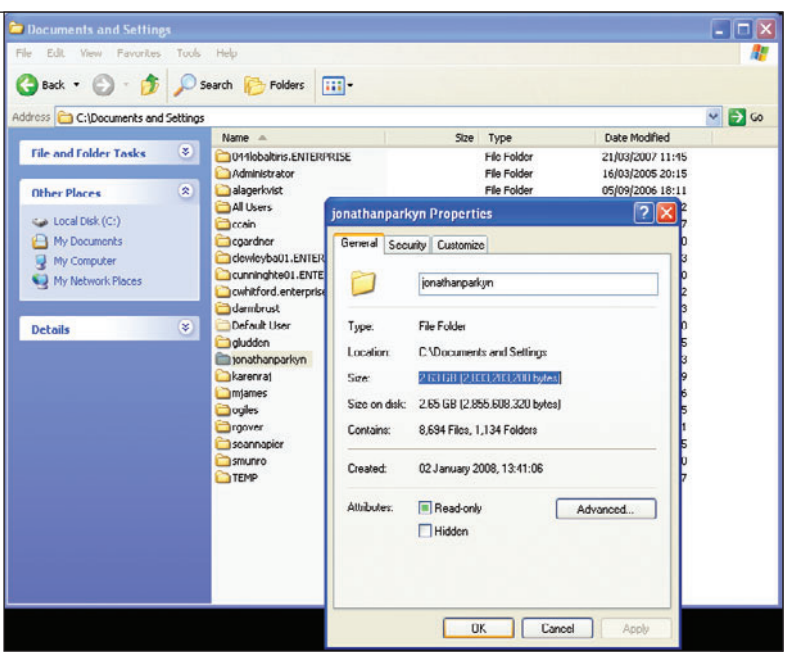
We all know we should back up. Our PCs store valuable documents, files, photos, music and more – but without making regular backup copies of these personal files, they are all at the mercy of a random malware attack or similar disaster.

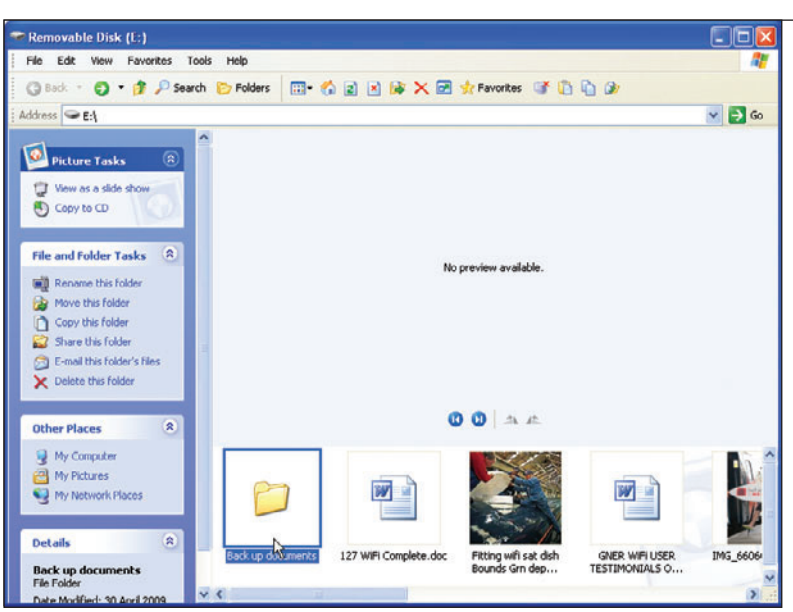
Most of us would like to say we back up regularly, but we don't. So music you downloaded and paid for at an online store, or precious pictures from a family event, could all potentially vanish. If you don't have backup copies, that's it: they're gone forever.

Backing up is a lot simpler than you might think and in some cases it's possible to set it running and never have to think about it again – unless, of course, the worst happens and you need to restore your files. At which point you'll be extremely grateful that you read the following steps and took our advice.

Step 1

The quickest and easiest way of making a basic backup of your files is to copy your Windows User folder onto a **USB memory key**. Your User folder will contain the My Documents folder, along with Windows' default pictures, music and video folders. If you save your files in locations other than the default User folders, you will have to copy these instead. Any make or model of USB key will do, though if you're worried about losing or getting your data stolen, you may want to opt for a device that had security built in, such as Safestick, (**www.safestick.info**). Storage space is the main consideration here, so you'll need to get a rough idea of how big your User folder is. In Windows XP do this by clicking on the Start button then My Computer. Choose Local C Drive and then Documents and Settings. Right-click on the folder that is named after your Windows user name and select Properties. This will tell you how large the contents of your folder is in **megabytes** or **gigabytes**.





Step 2

For Windows Vista owners, go to Start and click on Computer, then double-click the C Drive and open the Users folder. Again you want the folder named after your Windows user name; right-click it and select Properties to see how big it is, to ensure it will fit on your USB key. Put the memory key into a USB port. If it doesn't open in a separate window straight away or offer you an Autorun option to open in a new window, go to Start then My Computer (just Computer in Vista) and double-click on the appropriate drive letter. Right-click on the window, choose New, then Folder and give the folder a name, then open it. Now navigate to the User folder as outlined previously. Right-click on the User folder then choose Copy. Go back to the memory key folder, right-click in the centre of the box and select Paste – this will copy all your files. Depending on the size this may take a bit of time.

Step 3

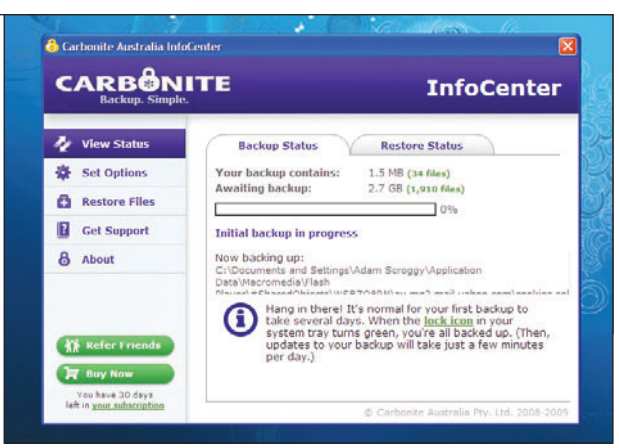
If you don't want to use or don't have a suitable USB memory key, another option is to store your backup copies on a CD or DVD. Most PCs come with a recordable DVD drive, so all you need are some blank discs. DVDs can hold up to 4.3GB, so follow the steps above to work out how much space you need and make the copy. If you have broadband you could consider online backup instead. One such service, Carbonite, offers password-protected storage and comes free with our cover disc. It automatically and securely backs up your files to a remote backup facility. Should you ever lose your files as a result of theft, hard drive failure or other unforeseen disasters, your files can then easily be restored.

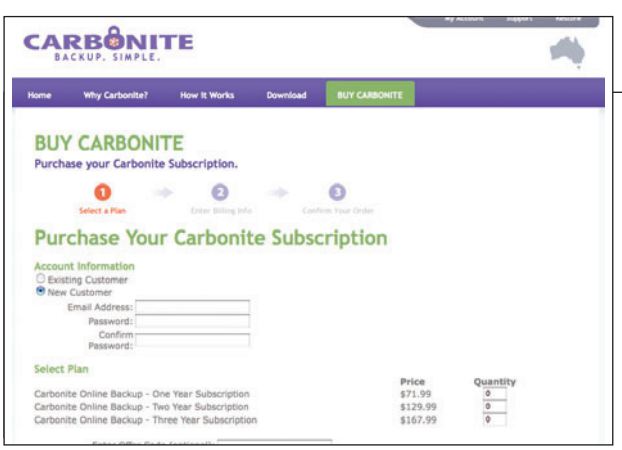
Step 4

To begin installation, click Install on the Carbonite page of our cover disc and then Accept the terms and conditions. The installation will start, and should take about five minutes. Don't worry about changing any of the settings; simply click Next to complete the process. You'll see a message saying that Carbonite has been successfully installed on your PC. There will also be two options: 'Automatically back up "My Documents" and Desktop' and 'I'll manually select what to back up later'. Let's go with the first option to start with, which should already be checked. Keep clicking Next to continue, and then click Done to finish.

Step 5

A popup will now appear welcoming you to Carbonite Online Backup. Click OK and the backup will begin. Now it's time to play the waiting game. It's completely normal for your first backup to take several days. When the lock icon in your system tray turns green (it's currently yellow) you'll be all backed up. From there, updates to your backup will take just a few minutes per day. To check the status of your backup at any time, click the yellow lock icon in your system tray to see the backup in progress.





Step 6

Remember, the version of Carbonite that we've included with our cover disc is a limited 90-day trial, so if you want to continue to use Carbonite's services you'll need to sign up for a licence at $71.99 per year. This works out at a very low $6 per month, which is a very reasonable price to be paid for the security the service offers. To sign up for the licence, head to **www.carbonite.com.au**, click on the BUY CARBONITE link from the top menu, and follow the simple instructions from there.

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.

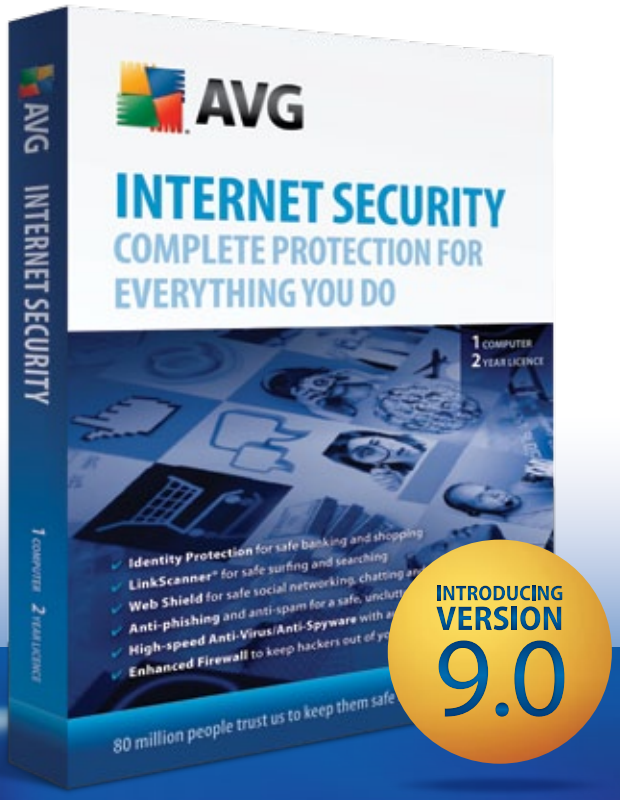
WPA Secure protection for wireless networks.

Zip file A file that has been compressed to save disk space or so it is quicker to email.

AVG

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