# technofile: pc security

**With more and more PC users opting for always-on broadband internet connections, computer security has never been so important. Robin Morris looks at the latest antivirus and firewall packages to help protect your system against web crime**

Internet saboteurs are becoming more sophisticated by the minute, and it's impossible to protect yourself against every conceivable danger. However, with the help of the latest security software, you can make your PC inaccessible to all but the most determined intruders.

Happily, the cost of protection is anything but prohibitive. Read on and we'll tell you how to secure your PC from the worst excesses of web crime.

## Viruses and worms

In their most basic form, viruses and worms are programs that replicate themselves. Spreading from computer to computer, they have often been programmed to carry out a task.

This could be as simple as deleting files, slowing down your PC or playing a message or tune. Alternatively, they could be waiting for a particular date before showing their party trick.

The Chernobyl virus, for example, is triggered on the 26 April and can hoax the PC into thinking the hard drive is empty. The SirCam worm can steal random documents from your hard drive and email them to other users, while the Klez worm can infect your PC with the ElKern virus.

Traditionally, viruses attach themselves to program files. When the file is loaded the virus may lodge itself in the PC's memory, infecting other files from there. Other viruses copy themselves to the boot sector of hard and floppy drives at startup.

## Reading from the script

Since its introduction in Windows 98, Microsoft's WSH (Windows Scripting Host) has allowed users to go underneath the surface of the Windows desktop using scripting languages like VBScript (Visual Basic Script) and JavaScript. With them, onerous tasks can be easily automated while web page designers often use scripting languages to add extra features to their products.

But this level of programmability also allows virus writers to exploit the power of the Windows operating system. Typically, the virus will pose as an innocuous text document and will be sent through normal email systems. In reality, though, the file will actually be a script virus and clicking on it will bring the virus to life.

Melissa is a famous virus that used VBScript, although the BubbleBoy virus offers a more potent warning about the dangers of script viruses. Exploiting a security deficiency in older versions of Microsoft Outlook, this virus was able to activate itself as the user read the email that delivered it.

## Email invasion

Macro viruses are extremely similar to their script-based siblings, using the built-in scripting languages of programs like Microsoft Word, Excel and Access. By copying themselves into the template files, they are activated whenever a document is edited or created. And because email clients tend to load certain programs automatically when email is viewed, macro viruses can be very hard to get rid of.

## Free as a worm

The majority of today's so-called viruses are actually 'worms'. Both viruses and worms replicate themselves, but the two differ in their means of replication. Whereas viruses must attach themselves to something (like a file or the boot sector of a hard drive), worms are free-floating and can reproduce themselves.

In the majority of cases, worms resemble script viruses (generally using VBScript), and use email systems to travel and replicate across the internet. These virulent infections can mail themselves to all the names in an address book. The famous SirCam worm is one of the most prolific. As well as scanning address books, it can extract email details from files on the hard drive and send itself out to a whole new list of recipients.

## Internet privacy

**When you download packages such as the popular file-transfer program Kazaa, you might think that you're getting something for nothing.**

**However, there's a good chance that third parties are also getting something back from you. Spyware is similar to a backdoor program – it sits on your hard drive relaying your activities to interested parties.**

**The spyware could be telling them what web pages you visit, how often you click on adverts or how you used a particular application. By recording your keystrokes and mouse clicks, the spyware knows exactly what you did on your computer.**

**Unless you read the license agreement before installing software, you won't realise that you could be consenting to having your private life recorded. Tools like SpyBot (http://security.kolla.de) and Ad-aware (www.lavasoft.de) can clean systems of most forms of spyware.**

**These utilities can also keep an eye on cookies – small text files installed on your PC by many websites. Cookies record information about you for future reference. Usually the information will be harmless identification details allowing the website to determine who you are.**

**Sometimes, however, the cookies will be recording information about your habits – for example, how many times you visit sites featuring adverts belonging to that company.**

**Though in general it's best to leave cookies alone, if you want to be sure nobody's collating information on you, you'll probably want to control the number of cookies on your system.**

**For more on spyware and keeping your PC safe, see *Security check* on page 98 and *Fight back against spyware* on page 124.**

Unsure of a technical term? Find out exactly what it means in our searchable Glossary which is on the cover disc

## Antivirus packages

Letting your PC roam the internet without protection is inviting trouble. The solution? Install antivirus software. Most packages use two different methods to detect viruses. The first of these is to look through definition files – a record of all virus 'fingerprints' known at that time. It is this file that an antivirus package refers to when it scans for viruses. It's important to download up-to-date definition files as frequently as possible. Better still, set your program to download them automatically.

### New threats

But while a database of fingerprints may be very well for families that have already been identified, what if a brand-new virus should come out? By the time antivirus companies have identified the offender, worked out a solution and posted an updated definition file on their sites, the virus could have swept through the internet community. This is where heuristics can excel.

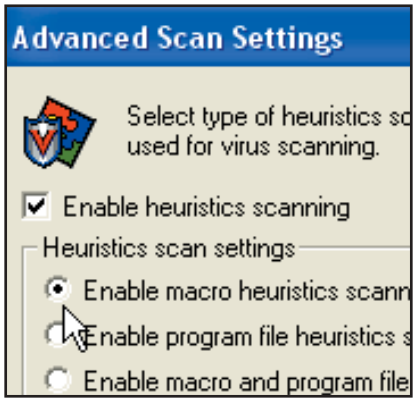
Heuristics techniques involve monitoring files for signs of virus activity. For example, a typical virus might install itself as a resident program, try to access your address book or write to the Windows Registry. But while this approach stops plenty of unknown viruses, heuristics often wrongly identifies a perfectly innocent file as containing a virus. As a result, many antivirus packages allow you to alter the sensitivity of the heuristics.

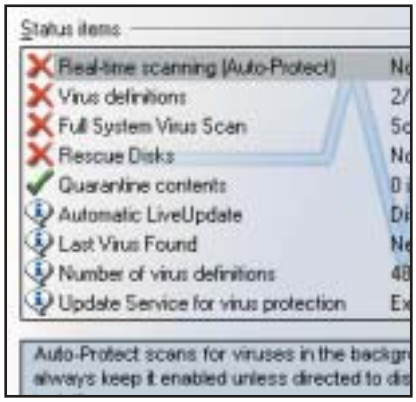
### Static vs dynamic

Most existing heuristics techniques are static in nature. But a new breed of virus program is harnessing the potential of 'dynamic heuristics' or, as it's more commonly known, sandboxing. In sandboxing, suspicious files are executed within a controlled virtual environment.

The antivirus program observes the behaviour of the file to assess its threat. For polymorphic or metamorphic viruses – those that can encrypt themselves or change the structure of their bodies to fool standard detection techniques – this virtual environment is likely to be the most effective mode of detection.

A good example of an antivirus program that uses sandboxing is Finjan's SurfinGuard Pro package. Because it can theoretically detect all virus activity, you won't need to keep downloading updates. However, sandboxing features are still relatively rare in the home and small office markets and only time will tell exactly how effective this solution is.


### What to look for

Viruses can slip into your PC through a variety of routes. For instance, not all packages will check Instant Messaging attachments, while only certain antivirus packages such as McAfee VirusScan extend protection to wireless devices.

When a package claims that it combs email software for viruses, make sure your

program is supported – many packages will check Microsoft Outlook and Exchange but ignore other popular email titles like Pegasus and Eudora.

Nowadays, detecting and removing worms and script viruses should be a formality for any good antivirus package. And when a program says it searches for worms and script viruses, check that this extends to the heuristics – some packages only uncover worms and script viruses they can identify through the definition files.

Once you've installed an antivirus program, you should see very little of it with alerts kept to a minimum. Be wary of antivirus programs that consume a lot of machine resources. If the speed of your Windows sessions slow to a crawl every time the antivirus program bursts into life, you're probably going to be switching it off at vital moments.

Some antivirus programs use shortcuts to speed up scans. For example, Panda Antivirus concentrates on files that have been modified rather than running through everything on the PC.

## Firewalls

As growing numbers of broadband users leave their machines connected for long periods, the internet is the perfect hunting ground for hackers searching for PCs to rape and pillage.

To find a victim, hackers simply have to run a port scan. When a PC wants to send or receive information, it will open up a port and dispatch or accept the relevant packets of data. Ideally, you only want these ports to be open when you're making contact with other computers on the internet.

Unfortunately computer programs frequently forget to close the relevant ports and hackers are well aware of this. Each PC connected to the internet has an unique identifying IP (internet protocol) address consisting of four sets of numbers – for example, 158.152.25.65.

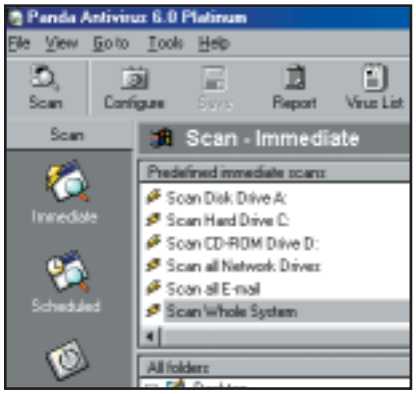
A hacker feeds long lists of IP addresses into a port scanning program to locate a vulnerable PC. Then they can slip inside and browse its contents.

In truth, most port scanners are merely curious and will probably leave without taking anything. But some may sift through your files looking for credit card details or passwords. They could also turn your PC into a mail server, hitting other internet users with a barrage of spam.

Alternatively, hackers may hide a backdoor program on your PC – a piece of code designed to make your PC perform particular tasks. For instance, the program may send the hacker lists of all the files on your system or tell them when your PC is switched on.

It could open ports on your PC at a set time allowing the hacker back into your system. The backdoor program may even command your PC to initiate a DOS attack, where a targeted internet server is hit by a deluge of data packets, possibly making it break down under the strain. It's hard to bring down an internet server using one PC, but in a DDOS (Distributed Denial of Service) attack your PC could be one of an army of machines directed to hit a certain internet server at the same time.






## Should you pay for security software?

**You can download ZoneAlarm and AVG Anti-Virus Free Edition (see *Antivirus software* on page 70) and enjoy the benefits of protection without having to spend a penny. So why would you ever want to pay?**

**Well, many antivirus packages are all about definition files. If a new virus or worm hits the internet community, you want to know that you're going to be protected. The fact that you're paying for a high-quality antivirus solution puts you in the driving seat when it comes to getting updates.**

**You should also get much better technical support, and some antivirus companies – Panda, for example – promise that, if you should be hit by an unidentified virus, you can send the infected file to the company and it'll get you a cure within 24 hours. A fullscale virus attack on your PC system is exactly the time when you'll be glad you've got the support of an entire technical department behind you.**

**In the case of firewalls, you can expect to get more in-depth information on the other machines trying to connect to your PC. ZoneAlarm Pro 4.0, for example, not only gives you a geographical location of the offending machine, but periodically reports this information to the sender's ISP. Some firewalls offer extra features like spyware and pop-up blockers, and email privacy. The removal of Trojan horses is often handled better as well.**

Backdoor programs can also be installed through worms, viruses and Trojan horses. The latter are programs that usually arrive in email attachments disguised as new games, applications or utilities. But their real purpose is to smuggle a backdoor program on to your PC.

While some of these problems will be solved by installing an antivirus package, anyone connecting to the internet (particularly through broadband, which is geared up to keep users connected for long periods) needs additional security.

## Barbed wire fence

Installing a firewall effectively surrounds a PC with protective fencing so that no data can go in or out of your machine without your permission. Hardware solutions are available, but most home and small office users will be fine with a software solution.

The firewall keeps a list of trusted IP addresses. When a system on the internet or an application tries to send data to or from your PC, you'll be given the option of placing it on the list. Obvious candidates would be your email package, security utilities or Windows updates. Less obvious would be the obscure IP address from Eastern Europe.

But it's not just other computers on the internet that you should regard with caution. Programs installed on your PC may be broadcasting information about your system and it's the ability to stop data getting out that distinguishes the best firewalls.

Windows XP has built-in firewall facilities that stop incoming but not outgoing data. ZoneAlarm Pro, on the other hand, not only notifies you when a program tries to connect to the internet, but can give you a list of all programs connecting at any one time.

Look for a firewall package that uses 'stateful inspection'. This increases the

## Firewalls

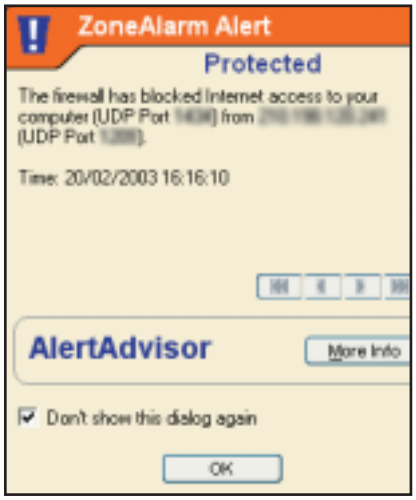
| Product | Website | Price (ex VAT) | Support |
|---|---|---|---|
| ZoneAlarm 3.7 | www.zonelabs.com | free for personal use | online forum/FAQs, virtual agent |
| ZoneAlarm Pro 4.0 | www.zonelabs.com | £26 | online forum/FAQs, virtual agent four-day email support |
| Norton Personal Firewall 2003 | www.symantec.co.uk | £34 | searchable knowledgebase, UK phone support charged at £18 per incident |
| Sygate Personal Firewall 5.0 | soho.sygate.com | free for personal use | online forum/FAQs |
| Sygate Personal Firewall 5.1 | soho.sygate.com | £25 | online forum/FAQs, email support, only phone support in US and Canada |
| BlackICE PC Protection 3.6 | blackice.iss.net | annual subscription £21 per user (£10.50 to renew) | searchable knowledgebase, email support |
| SmoothWall Corporate Server 3.0 | www.smoothwall.co.uk | £180 for unlimited users | online forum/FAQs, email support, more advanced options available through resellers |

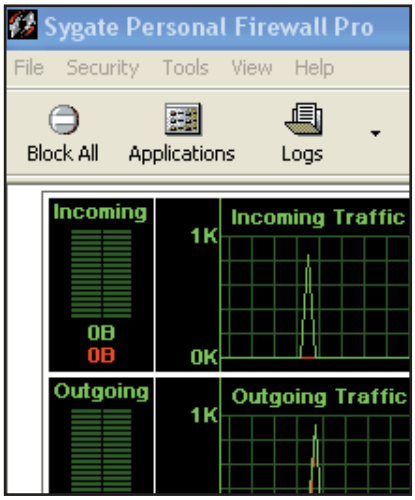
## Antivirus software

| Product | Website | Price (ex VAT) | Support |
|---|---|---|---|
| Norton AntiVirus 2003 | www.symantec.co.uk | £40 | knowledgebase, UK telephone support charged at £18 per incident |
| McAfee VirusScan | uk.mcafee.com | £26 | hot topics, extensive FAQs, free email/chat, occasional free telephone support |
| Panda AntiVirus Titanium | www.pandasoftware.co.uk | £20 | free email, one-year 24-hour phone support cure for new viruses within 24 hours |
| Trend Micro PC-cillin 2003 | uk.trendmicro-europe.com | £34 | knowledgebase, online agent support |
| AVG Anti-Virus Free Edition | www.grisoft.com | free for personal use | none with free version |
| Sophos AntiVirus | www.sophos.co.uk | varies according to number of users. Starts at approx £100 | extensive FAQs, UK email/phone cure for unidentified viruses |
| Finjan SurfinGuard Pro | www.finjan.com | £19 | knowledgebase, extensive FAQs range of support options available at extra cost |

detection rate by thoroughly filtering the data and uses past experience to catch intruders. The internet is full of tools for testing the security of your firewall connection; http://grc.com/default.htm is a particularly good starting point.

Some antivirus packages now come with built-in firewall facilities and home users can download powerful firewall programs free of charge. But perhaps the best solution is to buy a security suite such as McAfee Internet Security 5.0 or Norton Internet Security 2003 which combine antivirus and firewall programs. The perfect way to make your PC a no-go zone for hackers and crackers. ■




| Advanced features | Summary |
|---|---|
| basic firewall features | still one of the best individual firewalls and free for home users |
| location tracker, email monitor, ad blocking, expert-level rules | strong firewall but email/phone support rather patchy |
| email privacy, visual world map tracking, ad blocking | good package offers value for money when bought with Norton AntiVirus 2003 |
| free but not as user-friendly or efficient as ZoneAlarm | reasonably priced all-in-one solution |
| large array of configuration options backtrace feature, anti-IP spoofing | powerful firewall that offers plenty for experienced users |
| standard firewall features | difficult interface and not enough features to raise this above the competition |
| strong network features, huge range of optional add-ons | for multiple users, this offers a cost-effective and versatile solution |

| Advanced features | Summary |
|---|---|
| automatic updates, instant message scanning, automatic virus removal | not cheap but probably the most comprehensive package here |
| automatic updates, wireless device protection, x-ray tool for email | fast, powerful and extremely effective. An excellent choice |
| automatic updates, damage repair advanced heuristics | cheap, easy to use and not feature-heavy |
| Wi-Fi/PDA protection, firewall, internet access control | reasonably priced all-in-one solution |
| automatic updates, automatic healing | no technical support, but this powerful antivirus program comes free |
| advanced workstation and network facilities | plenty of features makes this a decent office solution |
| sandbox antivirus package, no updates needed | sandbox feature still fairly unusual. One to watch |