Anti-virus software

- AVG AntiVirus
- Dr Solomon's AntiVirus Toolkit
- Dr Solomon's HomeGuard
- IBM AntiVirus
- Inoculan AntiVirus
- McAfee VirusScan
- Norton AntiVirus
- PC-cillin
- VDS Pro

Although there's a plethora of viruses that can bring your PC low, a little preventive medicine can keep it healthy. We compare and evaluate nine anti-virus software packages

Health service

Illustration: Susie Louis

Computers have a long way to go before they take on human characteristics. But in one respect they already have: they can catch viruses. As with human viruses, a sick PC can display a range of symptoms. Some are like a mild cold and hardly noticeable, but others can be fatal. Although a computer virus can't actually kill a PC, it can damage or wipe out software and data on the hard disk, which is almost the same thing.

How do you catch a virus?

Just as you pick up bugs from other people, so your PC gets viruses from other PCs. Internet downloads and e-mail attachments are among the most common carriers of computer viruses, along with floppy disks. Shrinkwrapped software is pretty safe, as it is usually checked by the manufacturer. If you have kids who swap games with their friends at school, not only could they be breaking the software author's copyright, they are doing exactly what's needed to enable viruses to spread.

You can take preventive measures to keep your PC healthy. Just install and use anti-virus software. Better than cod liver oil – and without the unpleasant taste – anti-virus software will stop your PC getting a virus in the first place. And if it already has one, or you get lax about taking the medicine, it will get rid of the infection swifter than a course of antibiotics. Anti-virus software is more expensive than the medicine you buy at the chemist's – though the way prescription charges are going, not for long! – but if you value your data it's a price worth paying.

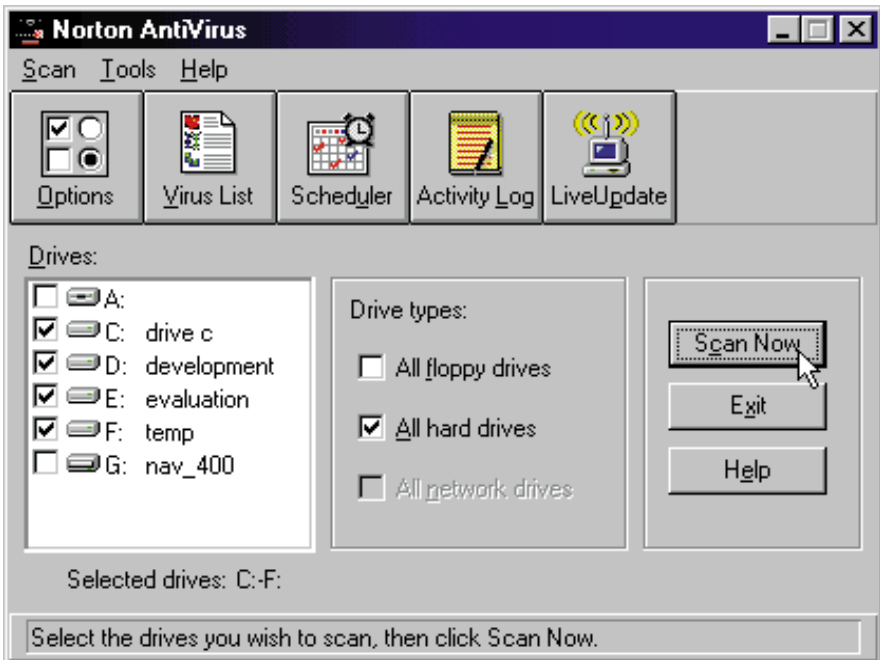
The first attack

Only 12 years ago there were no PC viruses. The first virus was reportedly the wrath of two brothers who owned a store called Brain Computer Services. They were angry about people who made illegal copies of software. The virus infected any floppy disk that was used after someone had booted from one of their disks, and changed the disk volume label to '(c) Brain'.

Unfortunately the virus wasn't fussy about whose software was on the disks it infected. It spread widely – so much so that, eventually, press reports predicted that it would result in the end of computing as we know it. Although those apocalyptic predictions failed to come true, they did have two effects. One of these was to alert malicious people to the idea of computer viruses, with the result that new ones began to appear. The other effect was to prompt people like John McAfee in the United States and Dr Alan Solomon here in the UK to write software that could detect and remove viruses.

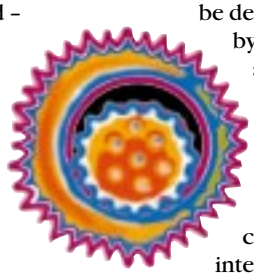
Computer viruses are so called because they spread in much the same way as biological viruses. They are carried on disks or in files and the computer 'catches' the virus when you load a file or run a program. Once the computer is infected the virus spreads to other disks or files. When these disks or files are used by someone else, their computer becomes infected too. And so on.

Viruses usually have an incubation



To use an on-demand scanner, select the drives to be checked and click Scan.

period during which they just spread. If they didn't, and just started destroying files or displaying rude messages straight away, they would be signing their own death warrants. The most common viruses are those that only do something noticeable – called the payload – quite rarely, like after the PC has been started up 400 times or only if it's Friday 13th.



Prevention is better than cure

There could be a virus incubating on your computer right now. If you don't use an anti-virus product you would have no way of knowing about it until the payload triggers. So let's look at anti-virus products and what they do.

The first anti-virus products were scanners, so called because you used them to scan your hard disk for infected files. In the early years the number of different viruses was small, and programs were written to look for each known virus in turn. As new viruses appeared, scanners got out of date because they couldn't identify them. So the software needed to be regularly updated.

McAfee's VirusScan became popular because it was released as shareware on bulletin boards – yesterday's equivalent of the Internet. To get an update, you downloaded the latest version. There is still a shareware version of VirusScan, though most people now buy it as a boxed package.

Conventional software publishers didn't like the idea of software that was obsolete by the time it reached the dealer's shelves, so they looked for other ways to detect viruses. One was the integrity checker. This works by taking a snapshot of every file, storing information about it so any changes to a file can be detected. When a file is infected by a virus it grows in size, which an integrity check will detect.

Many products that used integrity checking made bold claims like 'detects all known and unknown viruses'.

Unfortunately, some files change for valid reasons. An integrity checker can't tell the difference between a legitimate change and one caused by a virus. The result is false alarms. Not only that, but virus writers got clever and started writing 'stealth viruses' that hid changes from any program that was looking for them. Anti-virus software producers had to develop 'anti-stealth' techniques to combat this.

Up until mid-1995, PC viruses affected only program files and disk boot sectors (small programs that are run when you boot the computer from a disk). Then someone at Microsoft decided to find out if it was possible to create viruses using the Microsoft Word macro language. It was, and unfortunately the experimental virus infected a document which was shipped to customers on a CD. The Word Concept macro virus spread rapidly and spawned a host of imitators, with the result that macro viruses are now the most common type affecting PCs.

The advent of macro viruses sounded the death knell for integrity checkers. Word processor documents change frequently, so you need a program that looks at the macros to determine if they are infected. Integrity checking, however, is still used by some products to help protect other types of file. Norton AntiVirus, which calls its integrity check 'inoculation', offers it as an optional extra layer of protection. IBM AntiVirus uses it to speed up the file scan: if a file appears to have changed it is checked in full looking for specific viruses.

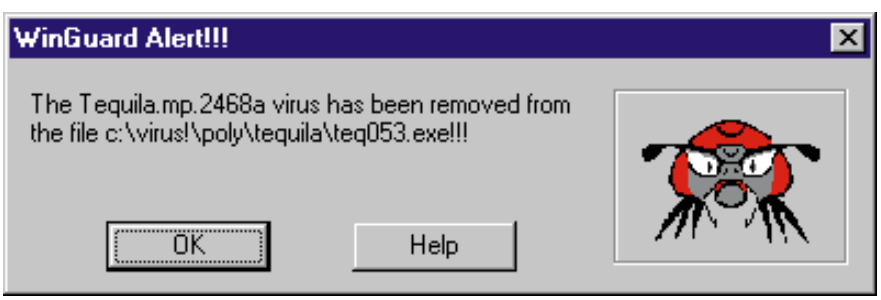
False alarms

Another technique that anti-virus products used to try to avoid the necessity of updates was the virus monitor. This watched for things that viruses do, like modifying application files and writing to the system files and boot sectors of a disk. The trouble with this is that there is hardly anything that viruses do that no ordinary application does, so virus monitors can give false alarms too.

Norton AntiVirus has a virus monitor called Virus Sensor. To avoid false alarms, the checks most likely to give trouble are turned off by default. You can also nominate 'trusted' programs that are allowed to perform the monitored activities. If you are prepared to take the trouble to set up the software to eliminate false alarms, Virus Sensor will give you a chance of catching a virus that eludes other detection methods.

There are more than 15,000 viruses, and the number is increasing at a couple

An on-access scanner checks files as you access them and can remove viruses at the same time.

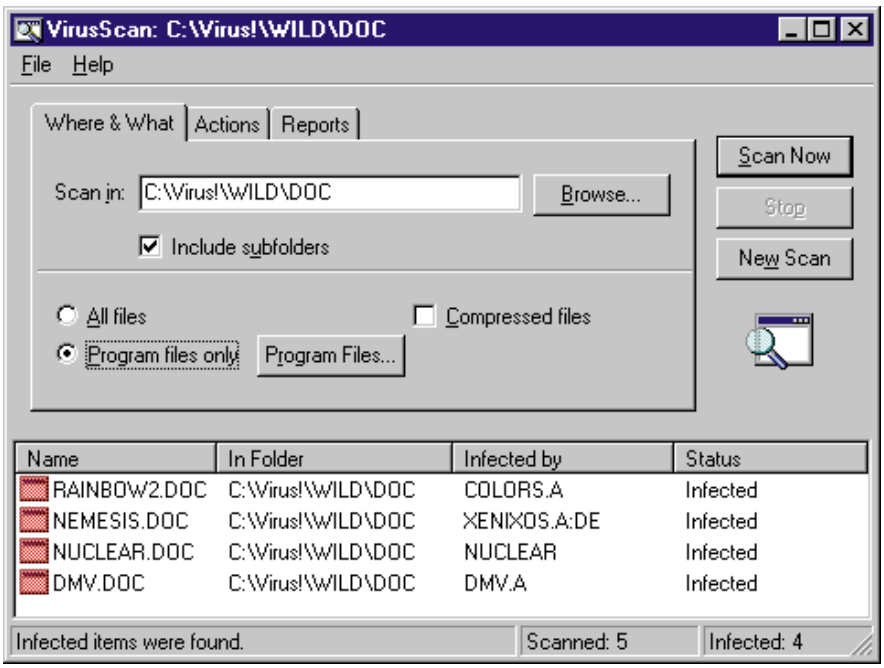


of hundred a month. Today's anti-virus products have a difficult job to do checking every file that is capable of carrying a virus without taking all day. Some programs are quicker than others. Inoculan AntiVirus and PC-cillin are among the quickest. But speed isn't a benefit if it comes with poor detection rates or frequent false alarms, and neither of these products scores highly here.

The most effective products are also the best sellers from companies like Dr Solomon's, IBM, McAfee and Symantec. This reflects the fact that keeping up with the flow of new viruses and developing new detection methods is technically demanding work. Smaller companies can't afford the development costs. Inexpensive products like Finson's VDS Pro may provide some protection, but there are many viruses that they fail to catch. They can also give false alarms causing unnecessary panic.

Even the best-performing products have gaps in their armoury simply because new viruses will have appeared since the last update was released. To counter this, products analyse each file heuristically to see if they contain program instructions that look suspicious. Most products claim a heuristic capability, but in the poorer ones it doesn't work that well and false alarms occur quite often.

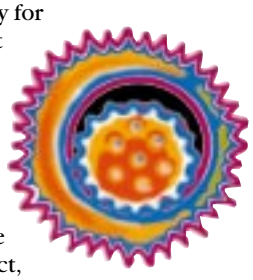
Anti-virus companies make great claims for the capabilities of their detection engines. McAfee claims that its Hunter engine is best at detecting Word and Excel macro viruses. Dr Solomon's Anti-Virus Toolkit boasts Advanced Macro Heuristic Analysis that can detect over 80 per cent of unknown macro viruses with no false alarms. Symantec claims the Bloodhound detection engine in Norton AntiVirus detects over 90 per cent of new and unknown macro viruses and 80 per cent of other new viruses. This means if you don't update your anti-virus software you won't be completely unprotected from new viruses.



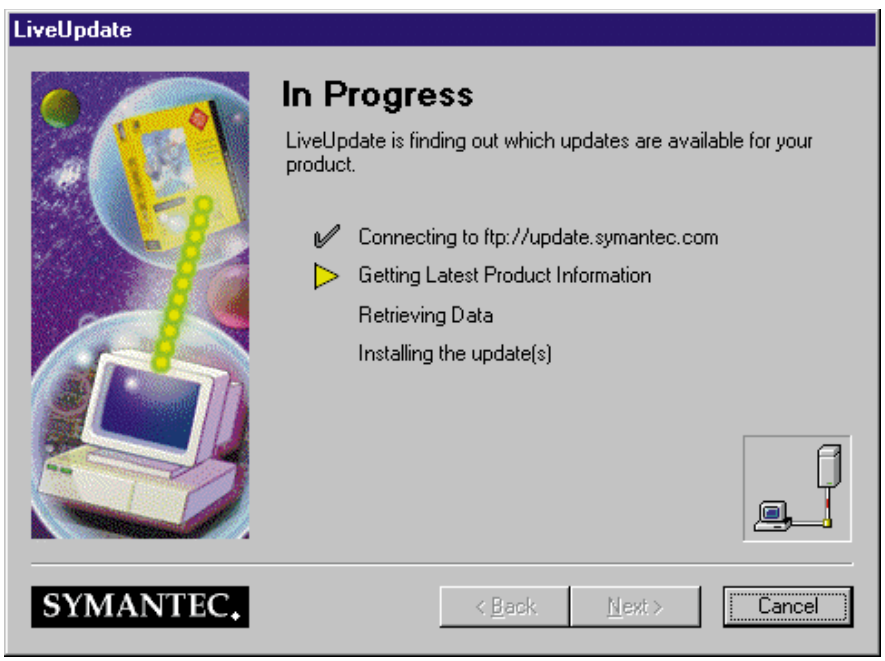
Macro viruses are now the most prevalent type of computer virus.

Updates are still a good idea, though, and how they are obtained is an important consideration when buying a product. If you're on the Internet, you can usually download updates using tools like Norton's LiveUpdate, which is cheap and quick.

If you want updates on disk you'll pay extra. Packages could have sat on a dealer's shelf for months and will be out of date when you get them, but some products still make you pay for even one update. Two that don't are IBM AntiVirus and Dr Solomon's HomeGuard, which both include a voucher for one free update. Dr Solomon's AntiVirus Toolkit, which seems to be the most expensive product, includes four quarterly updates in the price.



Most products let you download updates over the Internet.



When to check

No matter how good your anti-virus software and how diligently you update it, it's ineffective if you don't use it. Products offer various ways to ensure your system is regularly checked. Norton Anti-Virus and Dr Solomon's Toolkit both include separate schedulers, while IBM AntiVirus lets you schedule a check when your PC starts up. McAfee expects you to use the Windows 95 Plus Pack System Agent, but includes ScreenScan which checks your PC while the screen saver is running.

A better solution still is to use an on-access virus scanner. This is one that sits permanently in memory and checks files as you access them, so you can't run an unchecked file. On-access scanners are great for Internet users, because they

⇨

Anti-virus software compared

		AVG AntiVirus	Dr Solomon's AntiVirus Toolkit	Dr Solomon's HomeGuard	IBM AntiVirus
Contacts	Company	Grisoft	Dr Solomon's	Dr Solomon's	IBM
	Telephone	01732 746636	01296 318800	01296 318800	01329 242728
	Typical price (inc VAT)	£79	£80	£29	£39
Systems	MS-DOS	●	●	❍	●
	Windows 3.1	●	●	●	●
	Windows 95	●	●	●	●
	Windows NT	●	●	❍	●
Features	On-demand scanner	●	●	❍	●
	On-access scanner	●	●	●	●
	Automatic disinfect	❍	●	●	❍
	Emergency boot disk	❍	●	●	●
	Scheduler	❍	●	❍	●
	Disk updates included	❍	4	1	1
	Online updates	●	❍	❍	●
Ratings	Ease of use	★★★	★★★★	★★★★★	★★★★★
	Value for money	★★	★★★★	★★★★★	★★★★
	Performance	★★★	★★★★★	★★★★★	★★★★
	Overall	★★★	★★★★★	★★★★★	★★★★

❍ No ● Yes

★ = Poor ★★ = Below average ★★★ = Average ★★★★ = Good ★★★★★ = Excellent

Preventing infection

- Install anti-virus software, and use it regularly.
- Back up your files to protect them from loss.
- Update your scanner regularly.
- Check files and disks from outside sources before using them.
- Enable the virus protection for your hard disk's boot sector in your PC's Setup.
- Don't swap copies of programs with friends.
- Remove floppy disks from the drive after use to avoid accidentally booting from them.
- Use Rich Text Format to exchange documents created in Microsoft Word.
- Use WordPad or the Microsoft Word Viewer to open Word documents that might contain viruses.
- Encourage friends and colleagues to take anti-virus precautions.

Viruses and the law

Writing viruses isn't illegal. The Computer Misuse Act makes it a crime to cause 'unauthorised modification' to a system or data. This covers everything from malicious software to hacking. Virus writers have only committed a crime if it can be proved that their virus ran on someone's computer without permission.

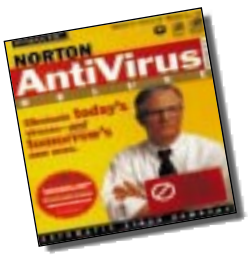
Catching virus writers is easier said than done, since it isn't an activity that draws attention to itself. Viruses don't often include copyright notices or other traceable information, and in many cases the identity of the virus writer isn't known. To date, just one British virus writer has been caught and convicted.

warn you about infected downloads and e-mail attachments the instant they are saved to your hard disk. Either a dialog box will appear or you'll see a blue text mode screen telling you what has happened, with buttons for you to choose how to continue.

A good on-access scanner makes scheduled scans almost redundant. In fact Dr Solomon's HomeGuard consists solely of an on-access scanner, making it the easiest to use anti-virus product of all.

Once your software has found a virus, the next step is removing it. Products offer various ways to do this. McAfee, Norton and Dr Solomon's on-access scanners allow you to disinfect files on the fly, causing little interruption to your work. Others make you stop and run the standalone scanner to check and clean the hard disk. If Norton AntiVirus detects a virus during a scan, its Repair Wizard guides you through the steps needed to thoroughly remove it.

If a virus is already active on your PC, removing it is harder than if the virus is merely present in a file. Some products provide an easy solution to this problem. Dr Solomon's products include the



Inoculan AntiVirus	McAfee VirusScan	Norton AntiVirus	PC-cillin	VDS Pro
Computer Associates	McAfee	Symantec	TouchStone	Finson
01753 577733	01344 304730	0171 616 5600	0181 875 4458	0171 723 4003
£39	£29	£49	£25	£20
●	●	●	●	●
❍	❍	●	●	❍
●	●	●	●	●
●	❍	●	❍	❍
●	●	●	●	●
●	●	●	●	●
❍	●	●	❍	❍
❍	❍	●	❍	❍
●	❍	●	❍	●
❍	❍	❍	❍	❍
●	●	●	●	●
★★★★★	★★★★★	★★★★	★★★★★	★★★
★★★	★★★★★	★★★★★	★★★★	★★★
★★★	★★★★★	★★★★★	★★★	★★
★★★★	★★★★★	★★★★★	★★★	★★

Magic Bullet, a disk that you use to boot your PC, scan for viruses and clean any infections. IBM and Norton AntiVirus also have emergency boot disks that let you disinfect a PC without having to run software from the hard disk that might itself be infected.

For home and small office users, McAfee's VirusScan is the best buy. It's inexpensive, easy to use and well integrated into Windows 95. The memory-resident Vshield checks files as you access them. You also get a standalone scanner to check disks and files whenever you want. ScreenScan checks your system while it's idle and the screen saver is running, so there's little chance for a virus to escape unnoticed. The cost of updates on disk is reasonable. They're also available free over the Internet or from a UK-based bulletin board.

For complete, all-round protection, Norton AntiVirus 4.0 is highly recommended. It includes both on-demand and on-access protection. Norton's latest scanner is highly effective. The product is the most customisable of all virus detectors, and its optional Inoculation and Virus Sensor options provide extra levels of detection that the others don't have. You also get an emergency boot disk to rescue already infected PCs. If you're on the Internet, getting updates for Norton AntiVirus is easy: just click one button and wait. Otherwise, updates are only available on disk on a monthly basis which makes the subscription fee rather expensive. Julian Moss

Malicious software

Macro virus: The most common type of virus – written in the macro language of an application. They mostly affect Microsoft Word, though Excel viruses have been found.

Boot sector virus: This virus type infects the system areas of disks and is activated when you start up the PC. They are quite widespread. Some are also quite destructive.

File or parasitic virus: This type of virus spreads by adding itself to program files so it is activated when you run the infected program. They are not as common as the other viruses, though there are many different examples because they are fairly easy to write.

Trojan: Named after the mythological Trojan Horse, this is a destructive program which pretends to be something useful. Trojans are not viruses at all, and since they don't spread by themselves, you aren't very likely to encounter one.

Logic bomb: A destructive payload built into some software with a specific trigger, like 'if my name is not on the payroll, delete the data files'. Logic bombs are a form of revenge taken by wronged programmers. If you employ programmers, be nice to them.