

# 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

**T**hese 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 fire-wall 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

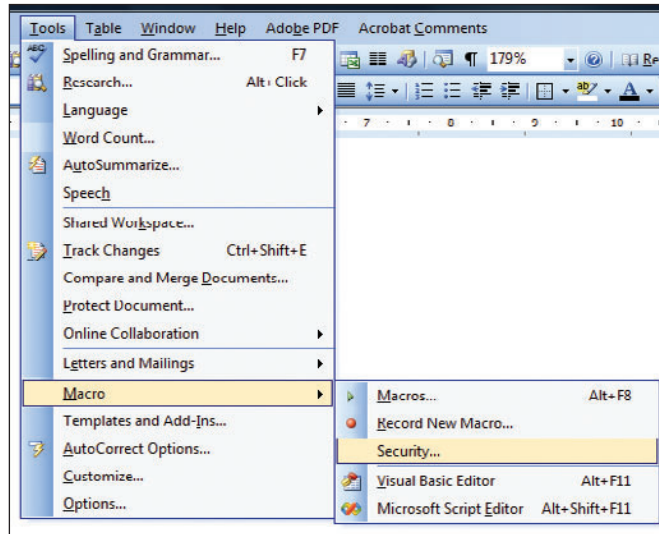
**1999** – Subseven allows hackers to view the infected computer using its webcam; Melissa email worm causes significant problems for many email systems

**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](http://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.

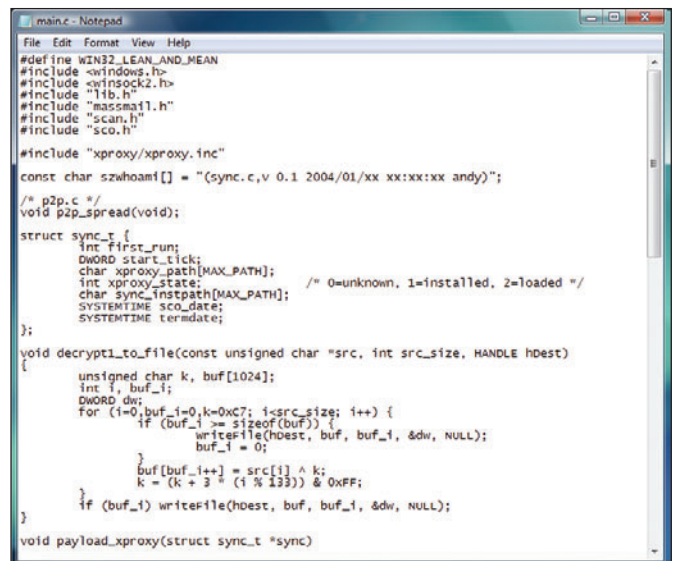
What's more, new technologies have presented new risks. **Wireless networks** have

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

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.

SIGN IN TO E-MAIL  
PRINT  
REPRINTS  
SHARE

▲ 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.



## 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.

▶ Subseven let hackers view infected computers by hijacking webcams

# Glossary

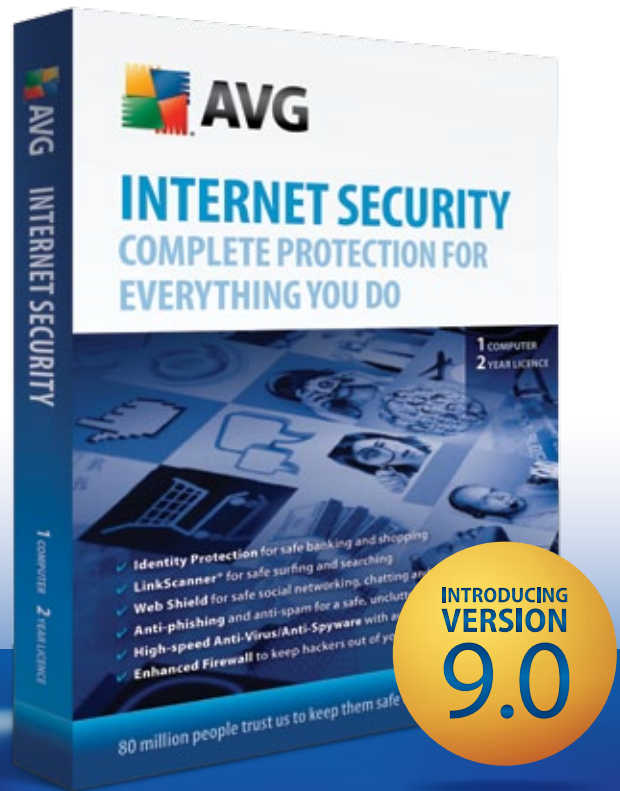
## Jargon buster

- ▶ **Add-on** Program that adds features to a web browser or applications, and is loaded only when needed.
- ▶ **Adware** Advert-supported software. Often installed surreptitiously on a PC and can compromise privacy.
- ▶ **Anti-virus** Software that detects repairs, cleans, or removes virus-infected files.
- ▶ **Bandwidth** The maximum amount of data that can be transferred over a connection at one time.
- ▶ **Beta** Version of software still in development.
- ▶ **Bios** Basic Input Output System. Software built into all PCs to control the basic operation of devices.
- ▶ **Bittorrent** File sharing software that enables users to download data from PCs anywhere in the world.
- ▶ **Boot** The process a PC goes through after it is switched on.
- ▶ **Broadband** A fast internet connection, such as ADSL.
- ▶ **Cache** Store for frequently used data or files.
- ▶ **Compression** The process of reducing a file's size by encoding the data.
- ▶ **Cookies** Text files generated by websites and stored on your hard disk.
- ▶ **CPU** Central processing unit. The brain of a PC.
- ▶ **Cursor** A moving pointer indicating a user's position on the screen
- ▶ **Dialogue box** A window that pops up to display or request information.
- ▶ **Disk image** A file containing all the contents of a floppy disk CD or DVD.
- ▶ **DNS** Domain name service. Translates website addresses into a language computers understand.
- ▶ **Domain name** The name used to identify a site on the internet.
- ▶ **Dropdown menu** A list of options that appears beneath a menu bar when you select a menu option.
- ▶ **Encryption** The science of scrambling data to hide it from prying eyes.
- ▶ **Firewall** Software or hardware that prevents unauthorised access to a computer over a network.
- ▶ **Floppy disk** A small, rigid square of plastic used to store data.
- ▶ **Format** To prepare a disk for use.
- ▶ **GB** Gigabyte. A measurement of storage capacity.
- ▶ **Hackers** People who break into computers, often in an attempt to steal information.
- ▶ **Hard disk** A high-capacity disk in almost all PCs, used to store data.
- ▶ **Icon** Image used by Windows to identify a file.
- ▶ **Internet Service Provider (ISP)** A company that provides you with an internet connection.
- ▶ **Internet Protocol (IP) address** An identifying number of a computer attached to a network.
- ▶ **JPEG** A common format for image files.
- ▶ **Keylogger** A malicious program that tracks your key presses and then sends them back to criminals, allowing them to commit fraud.
- ▶ **Malware** Software that performs harmful or surreptitious acts.
- ▶ **MB** Megabytes. A measurement of storage capacity, usually for computer memory.
- ▶ **Memory key** A thumb-sized USB storage device.
- ▶ **Modem** A device that enables two computers to communicate with each other over a telephone line.
- ▶ **Network** A way of connecting several computers and devices so they can share data.
- ▶ **Network Adapter** A socket for connecting a PC to an office network or some broadband internet connections.
- ▶ **Optical drive** Disc drive that uses a laser light to read and write data.
- ▶ **Partition** A large hard disk can be split into partitions or 'virtual' drives, which are treated by Windows as separate, smaller hard disks.
- ▶ **Phishing** A type of internet fraud that has the aim of tricking you into revealing your personal details to cyber criminals.
- ▶ **Plug-in** A program that adds extra features to your web browser or to other applications, and is loaded only when it's needed.
- ▶ **Reboot** To restart a computer.
- ▶ **Registry** A file in Windows that stores information on all hardware and software installed on your PC.
- ▶ **Rootkit** Software that gives a malicious user administration rights and access to a computer.
- ▶ **Router** A device used to connect more than one device to the internet.
- ▶ **Server** A computer on a network that distributes information.
- ▶ **Spyware** Software installed to monitor a computer's use.
- ▶ **SSID** Service Set Identifier. A naming convention for wireless networks.
- ▶ **Trojan** A malicious program disguised as a harmless one.
- ▶ **Universal Serial Bus (USB)** A standard that allows quick and easy connection of external peripherals to your PC.
- ▶ **URL** Uniform Resource Locator. The unique address of a web page.
- ▶ **Virus** A malicious computer program designed to cause damage to computer data.
- ▶ **Web browser** A program developed for navigating the internet.
- ▶ **Webmail** An email account accessed via a website.
- ▶ **Wep** Wired Equivalent Privacy. A security standard for wireless networks.
- ▶ **Wifi** An umbrella term for various standards for wireless networking.
- ▶ **Wireless network** Several computers connected without network cables.
- ▶ **Wizard** A step-by-step process that helps you choose settings.
- ▶ **WPA** Secure protection for wireless networks.
- ▶ **Zip file** A file that has been compressed to save disk space or so it is quicker to email.



# SAY HELLO TO AVG 9.0

Faster, Safer, Easier to Use.



## HOME SECURITY

**Complete protection for everything you do**  
AVG Internet Security with Identity Protection

**Surf the web with confidence**  
AVG Anti-Virus & Firewall

**Essential protection that won't get in your way**  
AVG Anti-Virus

**Up-to-the-minute protection for online banking and shopping**  
AVG Identity Protection

- 1-year and 2-year licence options available
- Free updates and product upgrades for the licence duration
- Fast, automated scanning and updates
- Free local telephone support, plus 24/7 e-mail support

AND MUCH MORE...

## TOUGH ON THREATS.

- ✓ Total protection against the latest threats
- ✓ Virus-free chat and instant messaging
- ✓ Anti-spam and phishing prevention
- ✓ Blocks hacker attacks
- ✓ Blocks poisoned web pages in real-time

## EASY ON YOU.

- ✓ Won't slow your PC down
- ✓ Easy to use — install and forget
- ✓ Simple set-up and automatic free updates
- ✓ Works in the background
- ✓ Free local telephone support

110 million people trust us to keep them safe online – and so can you.

NZ 0800 284 000  
**avg.co.nz**

AU 1300 284 000  
**avg.com.au**