workshop

INDEX

Protect your PC

Most PC users worry about the possibility of viral infection, but don't necessarily do much to prevent it. Simon Alveranga shows you how simple it is to beef up security and keep your data safe

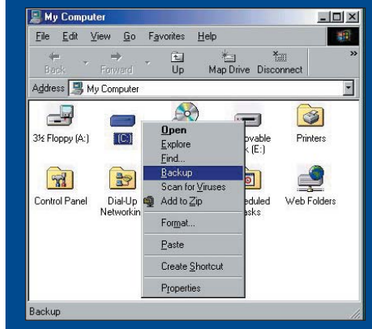
As the PC has become more powerful, so too have many of its peripherals, software and connections. However, it's not all good news for the modern computer – along with greater complexity comes greater vulnerability.

In the 80s most viruses were spread via floppy disk. The virus would be hidden alongside a program and, once the application was running, the virus could replicate itself and infect other programs. Nowadays, with better connectivity, viruses can be spread via the internet, downloads or email. Even worse, as programming advances so do viruses, incorporating auto-executable functions. This means that simply viewing an innocent-looking email may infect your machine. Despite being aware of the possibility of infection, home users in particular tend to assume security is built in to a system and therefore works automatically. This is not the case. However, with a few quick and easy steps, you can address your PC's security needs.

Over the following pages we'll lead you through the basics of PC protection, showing you how to ward off viral attacks with a more secure operating system, antivirus software and personal firewalls. And because the worst still might happen, we've tips on automatically backing up your PC and restoring lost files.

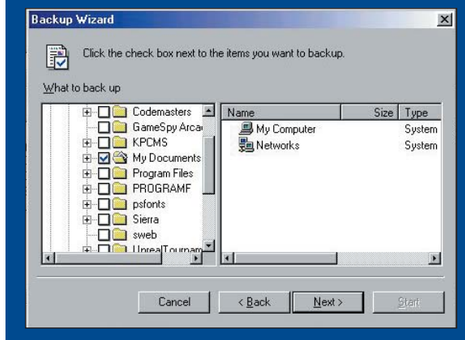
Backing up your hard drive

If you don't want to invest in a third-party utility, you can use Windows' own Backup program. As always, if you intend to take our advice and install antivirus and other security software, it's wise to make a copy of your files first.



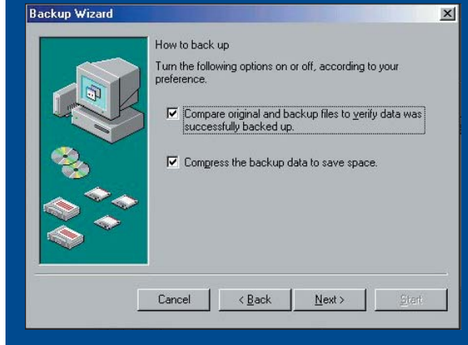
1 Double-click the My Computer icon on your desktop, then right-click the hard drive icon, usually named C. Select Backup from the menu. If right-clicking the hard drive icon doesn't bring up the Backup option, choose Sharing from the menu that appears and then Tools, Backup status

2 Select Create new backup job then choose whether you want to back up selected files, folders and drives or back up your entire hard disk

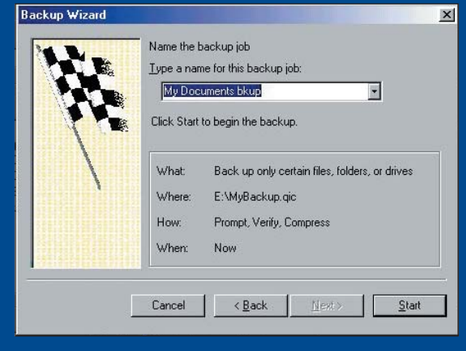


3 Assuming you chose to back up specific files, select the required files by ticking the appropriate boxes. Click Next and choose All selected files

4 Designate the drive that you want your data backed up to, ensuring there is sufficient free disk space to do so



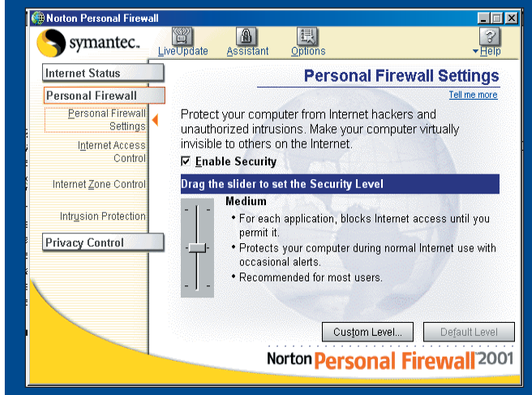
5 Click Next and ensure that both the checkboxes are selected. The first option verifies your data has been backed up correctly, while the second one compresses the backup data to save space



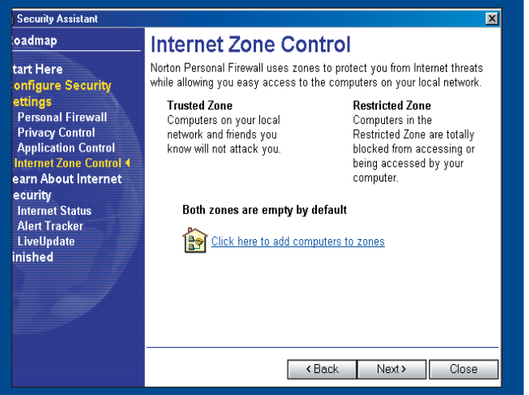
6 Give your backup job a name – such as My Documents.bkup – and hit Start. Your selected files (or entire disk, if you chose that option) will now be copied to your selected drive or removable media

Installing a personal firewall

Norton Personal Firewall 2001 is ideal for home and small business users who take security seriously but don't have a huge budget. It ring-fences your network, providing defence against intrusion and prevents your personal data being broadcast without your knowledge. Experiment with our trial version of Norton Personal Firewall on this month's cover disc.



1 Norton Personal Firewall 2001 acts as a software barrier between your PC and any nasties trying to gain access to your data. Under Personal Firewall settings you can specify the level of security you require, ranging from Low to High, so going online is less of a worry



2 In order to continue using network file and printer sharing facilities once the firewall software is installed, use the Security Assistant to edit the Internet Zone Control settings. This will allow known computers, such as those on your company network, to see your PC while blocking all others

Viruses: what are we up against?

The purpose of a virus varies from mischievous to malicious. Some viruses will simply display a message on your screen alerting you to the fact you've been infected; others can devastate your entire system causing irreversible data loss. Certain viruses have a much more insidious purpose, alerting hackers when you are online.

• Virus This is the original infectious agent and is generally a small piece of software that hitches a ride with a real program. Once the application is run the virus is activated, allowing it to either replicate by attaching itself to other programs or cause damage to your system.

• Email virus This is a relatively new strain of virus that has developed as email has become more widespread. Email viruses are very infectious as many of them, once opened (they usually arrive as an attached file), will scan the recipient's address book and send copies of themselves to a designated number of people. One of the best-known email viruses was Melissa, also known as the I Love You virus.

• Worms These are small programs that have the ability to copy themselves from computer to computer via a network connection. They will seek out specific security loopholes and send a copy of themselves through to the new PC where the cycle will continue. A particularly well-publicised worm was Code Red, which clogged networks and slowed internet traffic in 2001.

• Trojan horses These devious viruses are actually programs that are non-replicating and work by purporting to do one thing while also performing hidden tasks. They are commonly used by hackers as a means of alerting them when you are online, providing them with backdoor access to your computer.

Avoiding viral threats

Fortunately, there's a number of steps that you can take to combat these threats. Businesses will find their data less vulnerable to attack if they run a secure operating system like Windows NT or Unix. These are designed for networks and have built-in antivirus and security features that detect and block viruses and protect the hard drive.

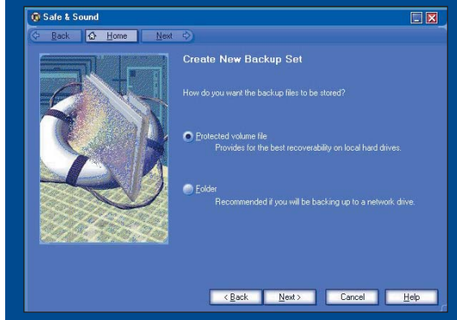
Home users and those running Microsoft's standalone products are less fortunate. If you are use an unsecured operating system such as Windows 98 or Me, make sure you install a virus-scanning program and visit the product's home page regularly to check for software updates. Failing that, use an online scanner such as Trend Micro (http://housecall.antivirus.com), which is on this month's cover disc.

Another tip is to upgrade Microsoft Internet Explorer to the latest version. This should protect you from Nimda and older worms, as version 6.0 plugs a number of loopholes that these viruses took advantage of. To upgrade Internet Explorer 6.0, go to Start and click on Windows Update. Once the web page has opened, go to the Products Update page where you should find the latest version of Internet Explorer.

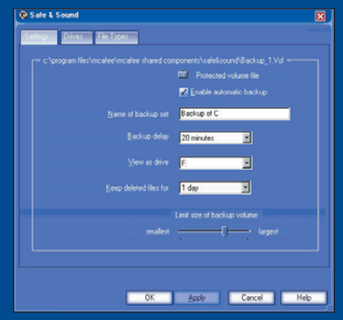
Also remember to back up your data regularly and create a Startup disk. To do this simply insert a blank floppy disk into your A drive. Click the Start button, Settings, Control Panel and Add/Remove programs. Here you will find a tab for the Startup disk – click on Create Startup disk and follow the onscreen instructions.

Securing data with Safe & Sound

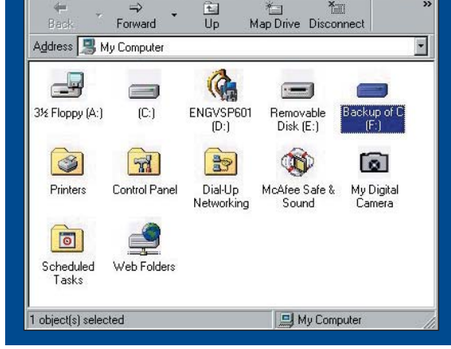
McAfee's antivirus package, VirusScan 6.0, features a useful tool for backing up and recovering your lost data. Safe & Sound lets you back up your entire hard drive or selected data. You can choose to back up to a network or have Safe & Sound create a secure area within your existing hard drive. A trial version of VirusScan 6.0 is on this month's CD.



1 The program is easy to use – simply select Safe & Sound from the VirusScan Start page, then click New. You will be asked to select a protected volume file or a folder



2 Choose a location for your backup job (we've chosen our second hard drive, F) and click Next. You can configure your backup job, manipulating options such as how often your data is automatically backed up and how long files marked for deletion should be kept for. Click Next, give your job a name and click on Next again. Safe & Sound will now begin backing up your data



3 Once the backup is complete, click Finish. Your backup can be revisited at any time by opening Safe & Sound, selecting the backup job and clicking Edit. The backup is also visible in My Computer. In our case it's called 'Backup of C'. Now if our PC loses data, we know where to find another copy of the file

Password protection

It makes sense to assign a password to prevent or restrict access to your PC's data. The easiest way of preventing access is to set a Windows boot password. To do this, enter Setup before Windows starts up by pressing the key shown during startup (usually delete, but sometimes F2).

Here's how to set Windows 98's password protection. Once you have entered Setup mode, use the right arrow key to move through the menus at the top of the screen to the Security menu. Now use the down arrow key to choose Set User Password. Press Return and the password box will appear; type in your password and press Return again, then confirm your password.

Now you need to scroll (using the down arrow key) to the Password on Boot option. Press Return and you'll see it's set to Disabled. Use the relevant arrow key to select Enabled, then press Return. And that's it. Choose the Exit menu at the top of the screen and, when prompted, press Return to exit Setup.

Next time you boot, Windows will ask for your password and won't load without it. While this is a great way to protect your system, it does mean that no one can access *any* part of your PC, and anyone with PC knowledge will easily bypass it by entering Setup and simply switching the Password on Boot option to Disabled. So think about investing in a password-protection program. There are many packages available, including Boot Guard Plus (www.bootguard.com) and Access Manager for Windows (www.softstack.com), both of which are available on this month's cover disc. DeskPass 2000 3.0 (www.beets.org) lets you restrict access to certain programs, files or your entire PC and can also record keystrokes made on your system. This will allow you to monitor what your PC is being used for – it's not uncommon for hackers to hijack your processing power or bandwidth for their own means. A trial version of DeskPass 2000 3.0 is on this month's cover disc. ■

ON THE COVER DISC See this month's cover disc to trial some useful protection utilities