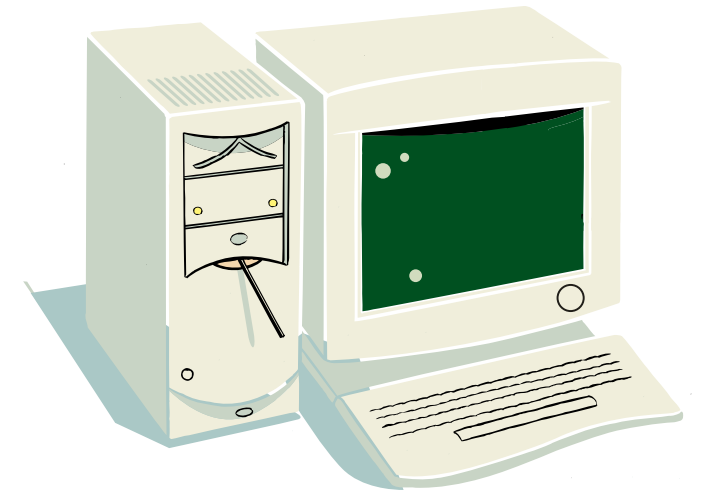


Trouble-free computing

Losing your data could be the same as losing your head when it comes to business. Jason Whittaker guides you through what to do when disaster strikes – and how to prevent it in the first place



It could never happen to me. That's what Isabel Robertson, a freelance writer who lives on one of the islands of the Inner Hebrides, thought. Having spent days researching and writing an article for a key client, four hours before the deadline she tried to open the file from a floppy disk to send it by email. Her computer refused to read the drive.

After trying a number of basic steps, it became obvious that there were serious problems and she was in danger of losing her client. Because of the deadline, as well as the fact that she was a day's travel from the nearest centre that could help her, Robertson used the internet to find an emergency service that could help. She accessed the remote data recovery service offered by Ontrack and was able to save her files – and her contract.

"Without Ontrack's help I would have let the client down badly. The Ontrack engineer was brilliant and I was so impressed that I could retrieve the data without leaving the house. I would recommend the remote data recovery service to anyone," she said.

The consequences of data loss can be catastrophic. In 2000, the DTI (Department of Trade and Industry) estimated that some 70 percent of companies which suffered a data disaster simply could not recover and stopped trading within 18 months. The question to ask is whether your business would survive the event, or would it become another fatality?

Your data lifeline

According to Todd Johnson, general manager at Ontrack Europe: "Electronic information is the most valuable asset a

company owns – data is the lifeblood of any company." Protecting that information is not just about restoring data in the event of a crash, but also ensuring that you have plans in place to keep it safe.

Central to this is having a proper procedure for backup, but the sort of surgery required for full recovery of your PC should also be complemented with regular checkups that include virus protection, computer security, risk assessment and insurance.

For André Post, senior researcher at Symantec Security Response, it is all about safe computing, which is not just software but a way of thinking: "Make sure you have antivirus software installed and kept up to date, and preferably a firewall as well. Also, keep all your software patched with the latest security fixes to keep your system as safe as possible. Last, but not least, use common sense – for example, when receiving emails from sources you don't know."

When is data disaster most likely to strike? Most of us probably think of a catastrophe of the type we've already outlined, or an actual drive failure when the hard disk we trust to preserve our precious data suffers a fatal attack. Such events, however, are relatively rare.

More common are those incidents where, after upgrading a piece of hardware or installing new software, a conflict occurs and a carefully balanced house of cards comes tumbling down. Many people will perform a major operation, such as changing to a new operating system, without checking their backup systems only to find that a vital piece of hardware or software, such as a tape drive or backup application, no longer works.

While most users are familiar with the scenario of a server holding this important data, more and more users are working remotely with mission-critical data stored on notebooks and even computers at home. We also rely increasingly on web and other remote servers to protect valuable data for sharing with colleagues.

If you host a website with a third party, or use them to provide file space online to store personal data, make sure that you check what course of action they will take in the event of something going wrong.

Computer rehab

The most important step for recovering from a computer crash is to ensure that you have backups of all your important data and applications. Simply copying to tape or disk, however, is rarely enough. As Todd Johnson remarks: "People assume

Top five recovery tips

1. Don't panic.
2. Don't run utilities until you have spoken to an expert. Companies such as Ontrack offer free telephone consultations with skilled technicians.
3. Question any company you use.
4. Be wary of companies that promise no charge for an evaluation: costs will either be hidden later down the line, or they will attempt a quick fix rather than full data recovery.
5. There's a range of options, from using utilities to onsite or remote recovery and even sending your hard drive back to the lab. Check out all the alternatives.



The most common form of backup, now that the humble floppy has had its day, is the CD: cheap enough and, with the latest CD-writers, fast enough not to deter even the most recalcitrant data savers

that they will never need data recovery because they have backups. We constantly receive calls from customers who have gone to their backups and found that the tape is corrupt or there is nothing there." A backup strategy for storing data is not enough – you also need to validate that data to ensure that it will be recoverable.

Backup strategies are divided into three main parts: hardware, software and procedure. If you do not have backup software on your PC, the chances are you already own a backup program on your Windows CD, though it is rarely installed by default. For Windows NT, 2000 and XP, NTBackup is included in the Valueadd/MSFT folder, while 95 and 98 users can access it from the Windows Setup tab in the Add/Remove Software dialog box from the Control Panel.

Windows Backup can back up and restore files, as well as perform an automated system recovery: simply save system files to a floppy disk and, when you boot up, the program retrieves files from your backup media. Backups can be scheduled and the whole process has

been simplified by means of a number of Wizards for every process.

While Windows Backup will perform most tasks required by the majority of users, alternatives are available that provide more control and support for a wider range of media, such as Dantz Retrospect Express (starting at £33 for individual licences) or, for enterprise services, Backup Exec from Veritas (from £319). While an option such as that provided by Veritas seems expensive compared to a free utility from Windows, it is capable of performing centralised backups from a server, simplifying the whole operation across a network.

Disks and images

An alternative to this type of backup software is to use disk imaging programs such as Norton Ghost or PowerQuest's Drive Image. These applications create a compressed image of your drive that stores all application, user and system files and can be copied to CD. Should your computer fail, simply boot from your drive image to restore your system as it was before the crash.

Hardware options are more varied, and we can only deal with them briefly here

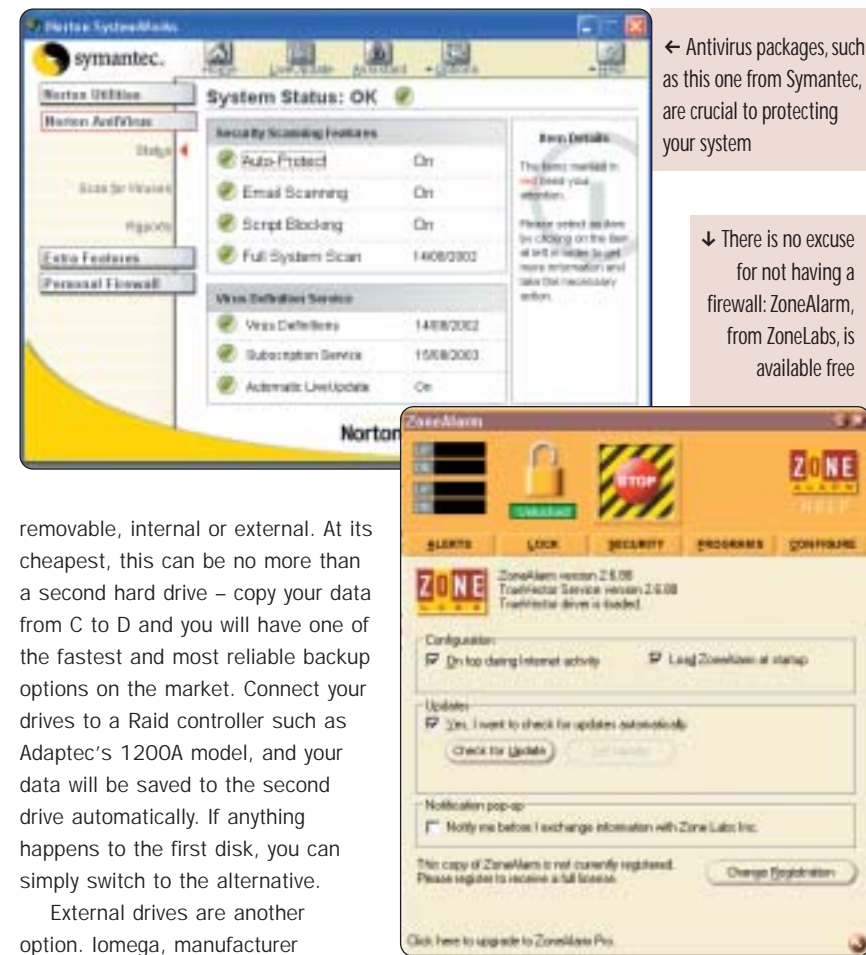
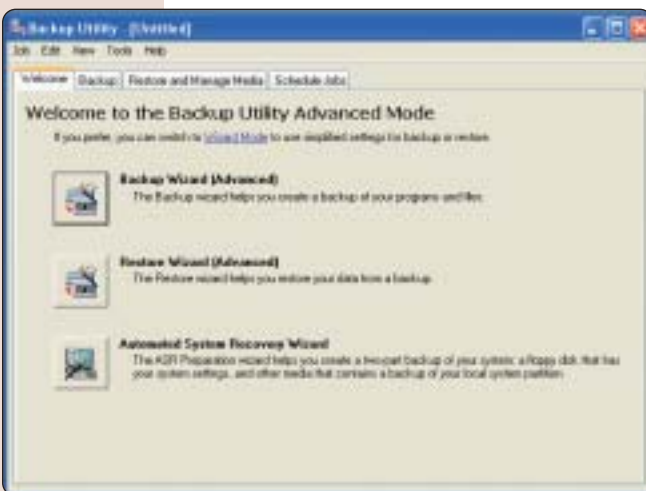
although the Emergency Contacts panel includes lists of suppliers. Probably the most common form of backup, now that the humble floppy has had its day, is the CD: cheap enough and, with the latest CD-writers, fast enough not to deter even the most recalcitrant data savers.

But CD-Rs are not without their problems. Because data is burnt rather than stamped into the recording layer, apparently indestructible CDs can deteriorate fairly rapidly and even the best are rarely guaranteed for more than 10 years.

In addition, the 650-700MB limit of CDs makes them unsuitable for backing up today's multi-gigabyte hard drives. Writable DVDs are becoming more popular, but backup is one area where tape comes into its own. Tape can, in the right conditions, have a shelf life of up to 30 years. Though slow, drives such as the Seagate TapeStor or HP Surestore can accommodate up to 40GB of data – more than enough room for a complete backup.

Increasingly popular, however, are drive alternatives: fixed or

↓ Norton Utilities provides a trusted set of tools for optimising and protecting your disk



← Antivirus packages, such as this one from Symantec, are crucial to protecting your system

↓ There is no excuse for not having a firewall: ZoneAlarm, from ZoneLabs, is available free

removable, internal or external. At its cheapest, this can be no more than a second hard drive – copy your data from C to D and you will have one of the fastest and most reliable backup options on the market. Connect your drives to a Raid controller such as Adaptec's 1200A model, and your data will be saved to the second drive automatically. If anything happens to the first disk, you can simply switch to the alternative.

External drives are another option. Iomega, manufacturer of the ubiquitous Zip disk (not recommended for serious backups itself, if only because of its limited capacity), has recently released the Peerless cartridge drive, with capacities of 10-20GB.

FireWire or USB drives are even better priced alternatives, offering capacities of anything up to 160GB, often for the price of a Peerless cartridge. Like the Peerless system, external drives also have the advantage that they and your data can easily be taken off site.

Planned recovery

Simply possessing the right application and drive is not enough: what happens if storage medium is faulty, for example, or

data is lost to a fire or water damage affects your media?

As we have already suggested with external drives (though the same is also true of tapes, CDs and other removable media), there are options for taking your data off site. If the worst comes to the worst and you lose your equipment, at least you can recover valuable information.

This is assuming, of course, that the tape, CD or hard drive is still readable. Even in the best environmental conditions storage media can fail, meaning that if data is not verified all your information can be lost. What is more, rewriting data

to the same tape or rewritable CD is more likely to result in information becoming corrupted. The alternative, however – to use a clean tape, disc or drive for each backup – quickly becomes expensive.

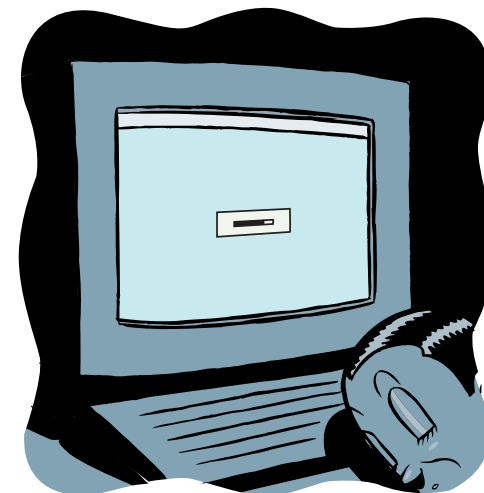
The best compromise is what is known as the GFS (grandfather, father, son) system, where backups are rotated and media slowly recycled. A full backup can be made at the end of the working week (the grandfather tape), with incremental backups at the end of each day (father and son), preserving only recent changes. At the end of the month, a complete backup is taken and stored on a new tape, while the others are used again.

The backup strategies and applications that we have considered so far, though, assume that you can access your PC. What happens, however, if the worst has occurred and your disk is down completely, or you did not back up your data in the first place?

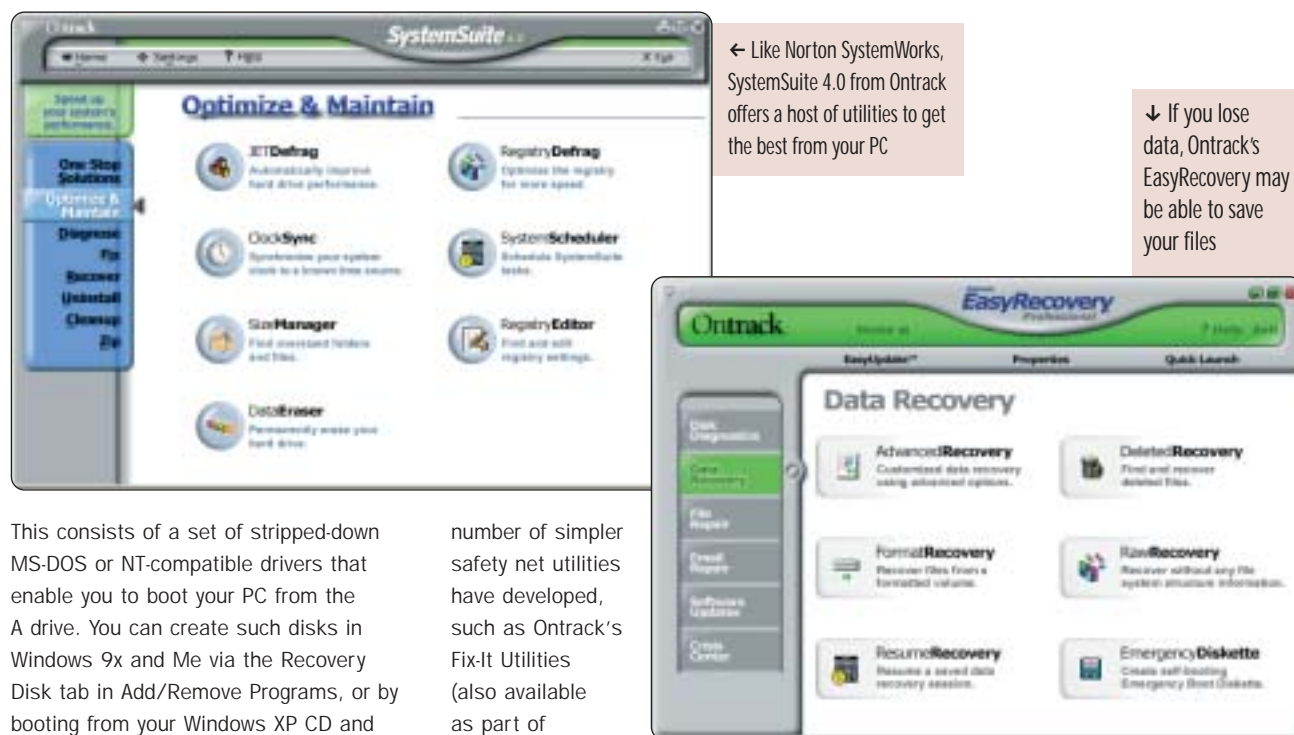
Crash team

True hard drive crashes, where the drive mechanism fails – for example, when the read/write head collides with a platter – are fortunately very rare, but there are plenty of other reasons why you may not be able to access your data. A virus, for example, could delete files or, more seriously, wipe essential Bios data: alternatively, a poorly configured machine could go down, corrupting information that points to the files on your disk.

Such events need not be entirely catastrophic, but you do need to prepare for them in advance. First and foremost, you need to prepare a recovery disk.



Simply possessing the right application and drive is not enough: what happens if storage medium is faulty, for example, or data is lost to a fire or water damage affects your media?



This consists of a set of stripped-down MS-DOS or NT-compatible drivers that enable you to boot your PC from the A drive. You can create such disks in Windows 9x and Me via the Recovery Disk tab in Add/Remove Programs, or by booting from your Windows XP CD and using the Recovery Console by typing `d:/i386/winnt32.exe /cmdcons`, where D is the letter of your CD drive.

A startup disk or Recovery Console provides a few basic command tools to diagnose and repair your system. Typing `Chkdsk /f`, for example, checks the status of a disk and can repair some errors, while `Fixboot` writes a new partition boot sector to your disk and `Expand` extracts a file – useful if you need to replace a device driver, for example, from your Windows disk.

These are powerful tools, but also difficult to use, and it is no surprise that a

number of simpler safety net utilities have developed, such as Ontrack's Fix-It Utilities (also available as part of SystemSuite 4.0), McAfee Utilities 4.0 and Norton Utilities 2002 (included in Symantec's SystemWorks 2002). These programs all work in a similar fashion, and include most of the tools you will ever need to protect and optimise your PC – SystemWorks and SystemSuite in particular – including antivirus and even firewall protection as well as diagnostics and repair tools.

If you have SystemWorks or SystemSuite installed, each program offers a one-stop solution for beginners that will analyse and fix most faults on

a system. If you require a more detailed repair, both also offer expert tools, such as Norton Disk Doctor and PCDiagnosics, and DiskFixer as part of SystemSuite.

The road to data recovery

Tools such as SystemWorks and SystemSuite can help you work out where problems are occurring on your PC, and they even provide unerase tools that can help recover files that have been deleted accidentally.

When recovering lost data, there are a number of options open to most users. In the first instance, a Windows crash may have made your system unstable – what is less important here than the issue of your data going missing is the fact that your PC is becoming unworkable.

Windows Me and XP have built-in System Restore tools that you can access from the Programs, Accessories, System Tools menu, returning Windows to a previous, more stable state. For users of earlier versions of Windows, GoBack from Roxio provides a similar service.

If you have lost important data, as mentioned previously, utility suites from McAfee, Ontrack and Symantec include tools for unerasing data, while Ontrack also provides a more robust data recovery application, EasyRecovery Professional, which performs similar diagnostics tests

Emergency contacts

Backup

- Retrospect Express 6.0 +33 1 55 33 02 00; www.dantz.com; £33
- Backup Exec 8.6 0870 243 1000; www.veritas.com/uk; from £319
- Norton Ghost 2002 020 761 65600; www.symantec.co.uk; £33
- Drive Image 2002 0118 9522 600; www.powerquest.com; £32
- Surestore DAT 24i 08705 474 747; www.hp.com/uk; from £500
- TapeStor Travan 7.0 www.seagate.com; from £270
- Adaptec ATA RAID 1200A www.adaptec.com; from £65
- Iomega Peerless www.iomega.com; from £225

Data recovery and drive diagnostics software

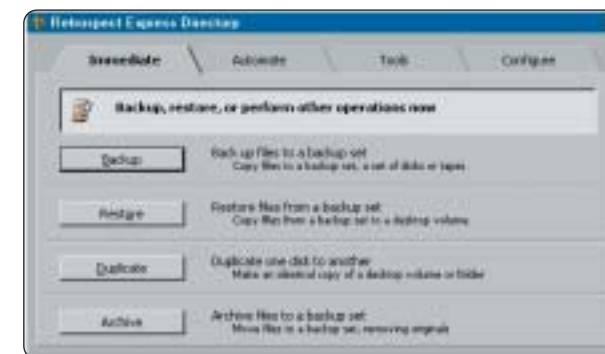
- EasyRecovery Pro 6.0 01372 741 999; www.ontrack.co.uk; £59
- SystemWorks 2002 020 761 65600; www.symantec.co.uk; £49
- SystemSuite 4.0 01372 741 999; www.ontrack.co.uk; £33

Data recovery services

- MJM Data Recovery 0800 072 3282; <http://datarecovery.mjm.co.uk>
- Ontrack Data Recovery 01372 744 422; www.ontrack.co.uk/datarecovery
- Vagon 0800 581 263; www.vagon-data-recovery.com

Antivirus

- McAfee VirusScan 6.0 ; www.mcafee.com; £22.99
- Norton AntiVirus 2002 www.symantec.co.uk; £24.99
- PC-cillin 2002 01628 400 500; www.trendmicro.com; £24.99
- Sophos AntiVirus 01235 559 933; www.sophos.com; £99
- Kaspersky AntiVirus 01223 576 001; www.kaspersky.co.uk; £23.50



↑ Dantz's Retrospect Express offers fast, easy backup to removable media drives as well as restoration, duplication and archiving facilities. Other features include compression, scripting and automatic backups

Firewalls

- Norton Personal Firewall 2002 www.symantec.co.uk; £27.99
- BlackICE Defender 3.5 www.networkice.com; £28.99
- McAfee Personal Firewall www.mcafee.com; £23
- Zone Labs ZoneAlarm www.zonelabs.com; free Personal Edition, £32 for Pro version

Uninterruptible power supplies

- Belkin SurgeMaster www.belkin.com; from £19.99
- Belkin Gold Series UPS www.belkin.com; from £55.99
- APC Back-UPS 0870 845 8520; www.apc.com; from £52.99
- Liebert PowerSure www.smartups.com; from £95

Top five safe computing tips

1. Antivirus software is key: keep it up to date. Set the update feature to do it automatically.
2. Install a firewall, not merely to keep intruders out but to prevent malicious code on your computer affecting others
3. Patch your applications regularly to cover security gaps.
4. Use your common sense: if an email offer seems too good to be true, then it probably is.
5. Safe computing equals responsible computing: if your PC is properly protected, you are less likely to cause damage to other users by passing on viruses, for example.



Prevention is better than cure

It is an unfortunate fact of life that the virtues of the internet are accompanied by a number of vices that make your data less secure. "There are plenty of people who wish to attack you and run malicious code on your PC. To prevent a computer being compromised, we always advise people to implement safe computing, which means both using the right software and maintaining a certain way of thinking," says Symantec's André Post.

For Post, antivirus software is "super-mandatory" on any system. "It's the core of safe computing practices," he says. "Why do I think that? We see many viruses that are so poorly written that, in many cases, they do not simply infect files but destroy the host. If that happens, the chances are that you won't be able to recover all your data if you try to clean a virus after the event."

to SystemSuite but also offers a host of tools for retrieving data from your system.

Such tools are not always sufficient, however. Installing them after you have experienced data loss is likely to do more harm than good. This is because when data is deleted the operating system does not actually remove it, it simply gets rid of the file headers that point to where the data is on disk. Installing more files will subsequently overwrite that data, making it unrecoverable.

Such tools are also less useful when a disk has suffered some form of physical damage. But even if you do not have data recovery software installed or your drive is harmed in some way, you may still be able to retrieve information via a data recovery service, such as Vagon (www.vagon-data-recovery.co.uk), MJM Data Recovery (datarecovery.mjm.co.uk) or Ontrack (www.ontrack.co.uk).

Ontrack, which first supplied its Disk Manager in 1985 and began data recovery services in 1987, is the best known of these companies. It offers data recovery both in the lab and remotely over the net.

In either case the first service provided is an estimate of the projected time and cost of retrieval. "The time it takes to get data back is critical," points out Ontrack Europe's Todd Johnson. "With remote data recovery we can get the customer up and running in a couple of hours."

When using a firm such as Ontrack for data recovery, the disk is first diagnosed, either remotely by sending it to the company, or by a visit to your home or office from a technician. Some companies offer free diagnosis, but this will probably be recouped at a later date. In any event, be prepared to pay. As Ontrack's Johnson remarks, "You only have one chance to get back your data."



“Safe computing is like providing your immune system with a vaccine to protect it at certain entry points”

André Post, senior researcher, Symantec

As well as Norton AntiVirus from Symantec (www.symantec.com), recommended packages include McAfee VirusScan (www.mcafee.com), PC-Cillin (www.antivirus.com), Kaspersky AntiVirus (www.kaspersky.com) and, for network protection, Sophos AntiVirus (www.sophos.com). Installing antivirus software is not enough, however: new viruses are released all the time, so your program must be kept up to date.

In addition, as Symantec's Post points out, major virus threats over the past year or more, such as Code Red or Nimda, have exploited loopholes in the host software, such as a web server. For this reason, it is vitally important not just to look after your antivirus applications, but also to install a firewall and patch all programs running on your computer.

While hardware firewalls are available even for individual users, most people increasingly run software versions such

as Norton Personal Firewall (www.symantec.com), BlackICE Defender (www.networkice.com), McAfee Personal Firewall (www.mcafee.com), or ZoneAlarm (www.zonelabs.com). The latter is even available as a free version, so there really is no excuse not to run a firewall.

Finally, another external threat – arguably a less malicious one, even though its consequences can be equally devastating – comes from the electricity supply that powers your PC. While surges, spikes, blackouts and brownouts are less of a problem in the UK than the USA, it still remains that rapid variations in electricity can cause data loss.

And never underestimate the ability of lightning to knock out a modem at the very least if it strikes a telephone cable. Cheap surge protectors are available from Belkin, although these only protect your computer from a power spike; an uninterruptible power supply (UPS), such as the Back-UPS range from APC, also provides emergency power in the event of failure.

Safety first

How, then, do you prevent your PC from crashing in the first place? Ontrack's Johnson believes that safe computing is relatively easy: “Protecting your computer is like maintaining your car. Today's PCs are built so well that the thing you need to pay most attention to is the environment it is running in – whether there is air conditioning to cool it down. Also, check your backup is up to date and validated,

and that you're running antivirus software. Those are the three main things. It's pretty simple really.”

Symantec's Post agrees: “Safe computing is like providing your immune system with a vaccine to protect it at certain entry points.” More than users simply protecting their own PCs, however, Post argues that we should be aware of the implications of unsafe computing for other users.

“I would love to see people having a raised awareness of what it means not merely to own a computer, but to be responsible for it as well, particularly when connected to the internet. If your computer is used as part of a distributed denial of service against, say, the White House, that will make you an accomplice.”

Knock-on effects

Protecting your own data has consequences for other users: installing firewalls and antivirus software does not automatically prevent your PC from ever being compromised, but they are important steps that will protect not only your own data but help minimise the risk of other computers being affected.

In addition to such software, invest in a UPS or at the very least a surge protector to guard your hardware. Attempting to recover information after a disaster is less likely to be effective if you have to install software following the event. As such, ensure that you have suitable diagnostics applications such as Norton Utilities or SystemSuite to help you to recover from a crash – or even prevent it in the first place.

Finally, even if your data world comes crashing down and you haven't prepared, don't give up. “If you experience data loss, there are solutions out there,” advises Ontrack's Johnson. “Do your research and ask for help.” ■



← Viruses are increasingly stealthy, and can knock out entire servers as well as individual PCs on the network