

# Keep your data safe

**For many businesses, their data *is* their business. Learn how to keep your data in and the viruses out.**

Your customer details, your accounts... for many businesses these exist in electronic format.

You don't want to lose that information – but you could: burglary and theft are not unknown. Accidents happen – there's fires and flood.

Then there's human error: people press delete, forget to back up...

Worse than that – there are people out there whose sole purpose in life is to write viruses that systematically destroy your business, and will laugh gleefully if you're not protected. You wouldn't

leave your building unlocked at night and it's the same with information security. It's common sense, and a few simple steps can make you a lot less vulnerable.

You don't need to be a techno-wiz to put in place some basic precautions. However, this is an area where you may benefit from professional help.

## 10 steps to security

### 1 Install virus protection

Viruses are malicious programs that spread from computer to computer, often deleting documents or programs. Many viruses spread simply because people don't keep their operating systems up to date or use anti-virus software. Prevent virus infections by installing anti-virus software and updating it regularly. Don't open files if you don't know who they're from.

### 2 Set up a firewall

A firewall is a program that stops unauthorised users accessing your computer. Hackers use tools that scan the internet looking for vulnerable systems. Stop outsiders from hacking into your network by installing a commercial firewall product and switching on the Internet Connection Firewall.

### 3 Keep your software up to date

Think of your software like a car: you have to take it to the garage for a service every once in a while. It's like that with software, system updates and service packs will fix bugs and patch security issues, keeping your system running smoothly. Download and install the latest patches and updates for all your software so you can stay up to date.

### 4 Use strong passwords

A password is a way to authenticate your identity. Don't make it easy for people to access secure systems by using easily guessed passwords. Educate your people to use complex passwords that include numbers and letters, and ensure they are changed regularly.

### 5 Ensure physical security

Keeping your office computers safe and preventing physical access to PCs and documents is a vital component

of information security. Sometimes a casual break-in can be more damaging than someone hacking into your system from outside. Locks, alarms, visitor logging, and asset tagging are all ways to improve physical security.

### 6 Protect sensitive files

Having interconnected information systems means that you risk your important data being viewed or tampered with by unwelcome parties. Protecting areas and documents with passwords is a good first step.

### 7 Get staff on your side

For your network security to be effective, you need everybody's co-operation. Technology only does what people tell it to do. Let staff know the reasons why you don't want them to download software, or use their work address in chatrooms. Include your policies in your staff handbook (see page 94) and train people in security awareness. You may also want to consider measures that prevent access to potentially harmful applications or websites deemed inappropriate or non-business related.

### 8 Put in place robust policies and procedures

Good security isn't just about having the right hardware or software: it's about making sure people use the

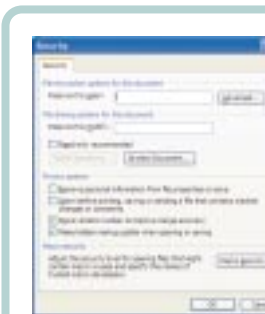
right processes. It can be a good idea to give someone the responsibility for overseeing security issues. Consider writing a plan that covers the technology, people, policies and processes – and revisit regularly.

### 9 Beware spyware and adware

According to a recent report that surveyed over a million internet-connected computers, your PC is likely to be infested with around 28 programs that have been installed without your knowledge. Spyware monitors the websites you visit; Adware displays pop-up advertisements, interrupting your work. Programs such as SpyBot and AdAware can find these programs and eliminate them and are freely available to download from the internet.

### 10 Back up

Backups are the last line of defence against hardware failure, floods, fires or the damage caused by a security breach. Decide what information



#### Tech tip

You can add a password to a **Microsoft Word, Excel** or **Microsoft® PowerPoint® 2003** file by choosing General Options from the Tools button in the Save As dialog box.

you want to back up and how often, and identify someone who will be responsible. You should also test the integrity of your backup by restoring the information occasionally.

For more information about how to secure your business, visit [www.bcentral.co.uk/security](http://www.bcentral.co.uk/security).



#### Tech tip

**Windows XP** has a backup utility. To find it, go to the Start menu, and choose All Programs > Accessories > System Tools > Backup. You can then work through the wizard to back up your data.