

Security tools

What they are and what they can do

Connecting PCs to the Internet has major advantages for the way in which you do business. However, it also opens a doorway through which people outside your company can access or damage your data. It is therefore essential to have good security tools in place.

Computer viruses can be a major problem. These are malicious bits of code that will enter a system without your knowledge and will often completely destroy your data. They can come hidden in e-mails or on disks with other software. They spread themselves by hiding in e-mails you send, sending themselves to everybody in your address book, or by attaching themselves to other files that you are putting on to a disk. However, there are a number of very good **anti-virus products** on the market that continually monitor the files that you are working with and the e-mails you receive and warn when they detect a virus. Most of them can either repair the file to neutralise the virus or will destroy any infected files. Because new variants of viruses appear on an almost daily basis, it is important to keep anti-virus software up-to-date. The better products allow you to download updates from the Internet at frequent intervals.

Whenever you are connected to the Internet, it is possible for somebody with malicious intentions to use the same route to get in to your system and read or destroy your files. **Firewall** systems (which consist of software and, sometimes, dedicated hardware) monitor the connection and block any unauthorised access to your system.

Once e-mails have left you, there is little you can do to protect them from prying eyes although, in reality, they are no more vulnerable to interception than a normal phone call or fax message. If you need to send sensitive information, **encryption** software will encode the message so that only the sender and a person who has the key to decrypt it can read it.



Physical PC security

There is no point in taking great care of the electronic security of data if it can be removed by somebody stealing a PC. It is therefore important to take care of the **physical security** of your PCs by locking them to fixed objects and by not keeping them where they can easily be taken. This is especially important for laptop PCs and PDAs. A number of products are on the market that are specifically designed for physically securing PCs. Encryption software can also be used to make it very difficult for anybody to read the files on your PC if they do manage to steal it.

Somebody working in or visiting your office could read or modify files that they should not have access to. If you are concerned about this, use passwords to control access to your PCs and don't leave them switched on when you are not there. Higher levels of security can be achieved by using computers that need you to insert a smart card or that check your fingerprint before they allow you to access files.

Advantages and Disadvantages

Good security tools will protect systems and data from 99.9% of attempts to attack them, but they have to be kept up-to-date.

Security tools can sometimes be oversensitive and detect problems that don't exist. This can be annoying. Security procedures can also be annoying. If you make them too annoying, people will find ways of bypassing them¹.

Key messages for SMEs

- Security tools are not an option, they are an essential. The loss or corruption of data held on your computers could literally put your company out of business. It is comparable to losing **all** of your paper records in a major fire.
- Security tools are worthless unless they are kept up-to-date.



Typical Internet security product

¹ If passwords must consist of 10 or more characters and must be changed every month, people will be unable to remember them and will write them down – probably on Post-It notes stuck to their PCs.

What to buy

Before buying security tools, read the PC magazines that are available in your country for reviews of what is available. Many of these also have websites that contain archives of earlier reviews. Two useful English language sites are <http://www.pcpro.co.uk> and <http://www.zdnet.com>. You can find links to reviews in some other languages in the FlexWork briefing on 'Equipment reviews'.

Typical prices are:

- Anti-virus software from about €30 for a single user
- Firewall software from about €40 for a single user
- Physical locking devices from about €25

Questions to ask suppliers

For any security product you should ask what, if any, insurance is included to cover your losses if it fails. In addition, for virus and firewall software, you will want to know:

- Can I save money by buying a multiple licence to cover all of the computers in my company?
- Does the software come with inbuilt help and/or paper reference manuals?
- What maintenance, support and upgrading service do you offer?