ProActive Resolutions

Websites & Internet Security

The basics of Internet security

Firewalls

Almost all businesses utilise the Internet in some way, whether it's for research, e-commerce or email. Yet many of them leave themselves vulnerable to security breaches, a hazard when computers often contain sensitive information like customer details. If your computer system was hacked, how would you cope?

One of the best ways to avoid unwanted, undetected intruders is to install a firewall. A firewall is an invisible shield which filters the information going out of and coming in to your computer via the Internet. It's not infallible, so you will still need to employ common sense and avoid suspicious websites, but an Internet connection without a firewall is like a wallet left on a dashboard. Why take the risk?

Hackers use sophisticated systems to scan for unprotected machines and steal valuable data, hijack hard drives and cause damage that you may well be liable for – for example a breach of confidential customer information or the loss of a credit card number.

Windows has a firewall option which you can switch on from Internet Explorer>Tools>Internet Options, but you should also consider purchasing additional firewall software to protect yourself. You should configure your firewall so that it won't send any information out without your express permission on each occasion. You set up automatic permissions for trusted sources so you aren't constantly bothered by messages.

Viruses

A virus is a self-replicating computer program that is designed to damage your computer and the data it holds. It can also tie up your system by sending emails to everyone in your address book (thereby spreading the virus) and in some cases, deleted Windows or the contents of your hard drive. Imagine the cost to your business if that happened!

Viruses are spread by emails, from the Internet, or via documents. You should install a virus scanner to automatically scan anything you receive. Run a regular virus scan of your hard drive and ensure you update the software daily. New viruses are made every day so you should keep your database updated.

Spyware

Another type of malicious download is spyware or adware. This is a self-installing program that hides on your PC and monitors your activity, reporting back to an individual or exposing you to unwanted advertising. You should installed a separate spyware scanner and run it alongside your virus software.

A common sense approach is best when dealing with Internet security. Only install legitimate copies of software for which you own the licence, don't open chain emails or anything that looks suspicious, and virus scan any incoming documents before opening. You should also implement a policy to ensure your staff adhere to safe and sensible web surfing and make regular backups of all data.

Top tips for IT security

No business is safe from hackers, but you can take some simple steps to reduce your risk.

1. Keep passwords un-guessable

Don't use the same password for everything, and avoid obvious things like names or birthdays. Instead, pick a combination of letters and numbers, for example a favourite holday destination and the year you were there.

2. Update your software

If you are using any standard software such as Microsoft Windows you should look for software updates online. Most new versions of Windows, such as XP, will automatically prompt you when an update is available. These are called patches and fix any known bugs or holes in the software which might allow hackers access.

3. Build a fortress

Invest in anti-virus and anti-spyware software and update it regularly to ensure it can detect even the newest nasties. It is not expensive but could save you a fortune in lost data, customers and hardware.

4. Make regular backups

In the unfortunate event of a security breach, the theft of a laptop or even a fire, your business will not be able to operate without the contents of your hard drives. Make backups to CD ROM daily or weekly and keep them offsite, or use a backup service for a small fee.

5. Emails are not always friendly

If you receive an unsolicited email and you are unsure, delete it immediately. Emails are the most popular way of spreading viruses, but you can install anti-virus software to scan incoming mail for viruses and spam. However, you should regularly check your spam folder for legitimate emails which may have slipped through.

6. Install a firewall

A firewall build a barrier between you and potential hackers while you are online. Use the Windows standard one or install a bought package.

7. Don’t input private data on public machines

Internet cafes or other public machines are a handy way of surfing the web while out and about, but are also vulnerable to hackers who can log and steal your passwords or credit card details. Avoid using data like that on a public machine and stick to simple surfing.

8. Use the latest versions of operating systems

Older versions of Windows are very vulnerable to attack, so you should consider upgrading to Windows Vista to ensure you have the most up-to-date protection.

9. Encrypt your files

You can encrypt files through Windows or through specially-purchased software, which makes sensitive data safe from prying eyes.

10. Call the professionals

If in doubt, get a professional out. It’s always better to be safe than sorry, and there are many highly-skilled IT consultants who can help you set up and maintain a secure online working environment.