



What you can do to manage network security

Thanks to the continued presence of internet worms, viruses and other threats to computers, network security consistently ranks as a top concern of business owners – even for those operating simple networks.

The good news is that you and your employees can manage many of these security measures yourself without help from an IT professional. The network security steps listed below are ranked by degree of difficulty. Start with the easy jobs and work your way through the others as your time, resources and skill level permit.

Easy jobs

If you have ever completed tasks such as installing a program or setting up a printer for your computer, you should have little trouble performing these jobs.

- **Install and update antivirus software.** Antivirus software is easy to install and, once running, constantly checks to prevent infections that could damage or destroy your data across your network. But know that hackers constantly write new viruses and that your antivirus software is effective only if it knows how to find the latest threats. So when you install antivirus software, set it to automatically download updates to catch new viruses. If you bought a new PC that included antivirus software for a trial period, sign-up when the free period expires to continue getting updates – or invest in another product.
- **Use software update tools.** Software companies like Microsoft have free tools you can use to update your software so it's more secure. For instance, it only requires a few mouse clicks to set Windows XP or Windows Small Business Server to use the Automatic Updates feature. This tool allows Windows to go online automatically to look for and install the latest updates to squelch security threats. Once you turn on Automatic Updates, it requires no further effort on your part. The software will update itself. The Microsoft Office System also has an automatic updating tool.
- **Install spyware protection.** Install and regularly update anti-spyware software, which looks for secretive programs that try to collect your passwords and account numbers. Microsoft has a free Windows AntiSpyware (US link) program and a Malicious Software Removal Tool (US link) you can use to rid your PCs of unwanted software.
- **Install a software firewall.** A firewall examines data passing into your network and discards it when it fails to meet certain criteria. Software firewalls, such as the Windows Firewall built into Windows XP Professional, protect only the computer they are running on, but provide a good back-up defense to hardware firewalls. It's easy to turn on the Windows Firewall.
- **Install spam filtering software.** Spam is unsolicited commercial e-mail that infiltrates inboxes and can force employees to waste time sorting it. While primarily a nuisance, junk e-mail does carry a risk when it contains attachments that, if opened, could release a virus. Also, some spam falls into the category of "phishing," or tricking recipients into giving away passwords and other valuable information that could put a business at risk. Installing a spam filtering product, or configuring built-in Outlook 2003 junk e-mail filters, can help to significantly reduce spam.

Harder tasks

This set of tasks can be more difficult. They require more technical expertise or ongoing management of your security policies and processes.

- **Restrict equipment access.** You can improve security by restricting physical access to your servers and networking equipment such as routers and switches. If possible, move these machines into a locked room and ensure only those designated to work on the equipment have keys. This minimises the chance that someone unqualified can tamper with your server or try to "fix" a problem.

- **Set permission levels.** You can assign users different permission levels on a network using Windows Small Business Server 2003. Rather than giving all users "Administrator" access, give individual users access to specific programs only, and define which user privileges are allowed to access the server. For example, you can grant permission to some users to read certain files stored on the server, but not to change them. Only your network administrators should be able to access all your system files and services.
- **Remove network access for former employees.** Eliminate the ability of former employees to log onto your network. It is easy to delete their access and user privileges, but if you wait too long, you may give disgruntled ex-employees an opportunity to damage or steal files.
- **Create an e-mail and internet use policy.** A recent study reported that 6 percent of all e-mail messages are infected with viruses or other programs that can damage your computers. Create a company-wide internet use policy that includes instructions to employees to not open e-mail attachments they do not expect. The policy should also address risky online activities and forbid such practices as downloading free utilities and other programs from the web. Instruct employees to not share passwords or account information if they receive an e-mail asking for them.
- **Require employees to use strong passwords.** Passwords that are easy to guess can enable unauthorized people to gain access to your network. To prevent this, your security policy should require that passwords contain both letters and numbers. And, while passwords should be changed regularly, avoid requiring employees to change them too often. If they struggle to remember their passwords, they may write them down and post them on their monitors, making it easy for others to break into your computer system.

Hire help

These tasks are not extremely technical, but you may want to consider hiring a computer or network consultant to handle them. Consult a Microsoft partner that has the proven expertise to help you plan and implement projects requiring more advanced skills.

- **Install a perimeter firewall.** While a software firewall protects the PC it is installed on, a perimeter firewall is a hardware device that plugs into and protects your entire computer network. A notable feature is that it enables you to close down network ports. Because network ports enable communication between client computers and servers, you can strengthen your network's security and thwart unauthorized access by closing unused ports. This step is more difficult to implement and you may want an expert to help set up your firewall functions correctly.
- **Secure a Virtual Private Network.** Linking offsite users to your company's network over the internet enables them to check e-mail and access shared files. A Virtual Private Network (VPN) lets you do this more securely. However, there's a significant security risk any time you make your network accessible to outsiders. You will want to bring in a security consultant because getting a VPN working properly can be tricky.
- **Configure wireless security features.** Anyone within radio range of a wireless network has the potential to listen in or transmit data on the network. If you plan to use wireless networking, bring in an IT professional to ensure security features are activated and that wireless encryption and access control features are properly configured.
- **Create back-up and restore procedures.** This task can be as simple as burning a CD with your data files on it and then storing it in a safe place. Windows XP includes a tool to back up and restore data to your PC. However, you may want to look at a more sophisticated solution. If you need your data to be available at all times, you should work with an IT expert who can add hardware to your system that builds in redundancy, making duplicate copies of files on a different hard drive every time you save them. That way if one hard drive dies, the back-up system can step in and keep your data flowing. You should back up files at least weekly, and practise restoring data periodically just to verify

that you can.

- **Configure database security.** If you have a database that stores customer, sales, inventory or other types of critical information for line-of-business applications, hire IT professionals to ensure that this information is well protected. For instance, a database expert can shield Microsoft SQL Server from most internet-based attacks by only allowing authorised users to connect to the database. They can also create back-up systems to restore your data if it is lost.

For more advanced assistance, call PC Pal today on 01603 766716

From <http://www.microsoft.com/uk/smallbusiness/starting/technology-in-business/security/managing-network-security.msp>