Secure your network

Making your home network as safe as possible is important, yet many people don't know all the potential pitfalls of unsecure networks. Our handy guide is here to help

What puts some people off setting up a home network is the fear that anything stored on their hard disk could be accessed by neighbours or **hackers**, and that the speed of a **broadband** connection could be whittled away by unauthorised users tapping in from outside.

While no network is ever immune to attack, provided you take a few simple precautions there's no reason a wireless network shouldn't be as secure as one where all the devices are connected by cables. Armed with the information presented here, your network will be safe.

What's the problem?

When it comes to network security, the main concern is making sure that any wireless connections are protected against unauthorised access. If you use a wired-only network, then you needn't worry quite so much, although internet-borne security problems, such as hackers, **viruses** and **spyware**, will always have to be taken into account. Even the most secure network will not block these types of web threats. For that you'll need to know some basic rules about how to deal with email and web pages, and you'll need some useful tools, such as Windows Firewall and Windows Defender, to fend off malicious software.

The main problem with Wi-fi is that, because it is a form of radio the signals can be intercepted and unauthorised signals can be sent to the radio receivers in your network: the wireless **router** and all wireless-enabled computers, storage devices, printers and so on.

A network that has not been secured by an **encrypted** password can be detected by anyone with a Wi-fi-enabled computer. In doing research for this this feature, we detected four wireless networks with no protection. If we were inclined to break the law, we could log into any of those networks and use that person's broadband account to visit websites, download illegal copies of movies and music – even pornography. And, if the network's owner had left any files in a Shared Documents folder, we could view, copy and possibly even edit those files.

In truth, the biggest threat most people face is a cheeky neighbour hopping on to your broadband connection to view web pages without

paying for internet access, but it's worth noting that if your connection were to be used to download seriously illegal material, you would be the first port of call for the police.

Wireless hardware, though technically advanced, is easy to install and use and, once it has been configured, you can more or less forget about it – which is where the problem lies.

Router manufacturers, and it is the router that lies at the heart of most home networks, often make setup a bit too easy. That's great for novice users, but means it's up to the user to strengthen the wireless security settings after installing the equipment. All too often this important task is shelved and then forgotten.

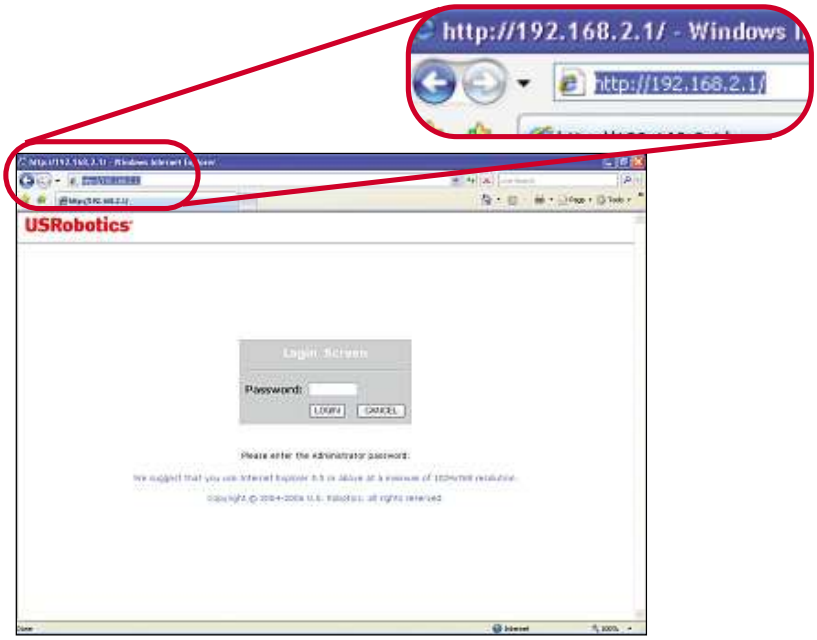
Broadband is delivered to homes either through standard telephone lines or by the same cable that delivers TV and telephone services. Cable subscribers require a **modem**, which is plugged into the incoming cable socket, and a router that is then connected to the modem. Sometimes the modem is built into a TV set-top box. The router does what its name suggests and routes signals between the internet and any computers attached to the router (either by physical cables or wirelessly). It also routes signals and files from computer to computer, so with all communication being handled through the router there is no need for any computer to be directly connected to any other.

A similar system can be used with **ADSL** broadband delivered via phone line, but the majority of users these days opt for a router that has a modem built into it, thus minimising the number of devices, power supplies and cables required. Not all routers have built-in wireless facilities, so it may be necessary to plug a separate box called a wireless access point into the router. Typically a router can handle up to four computers or computing devices connected by cable, and many more connected wirelessly.

In a typical home network, only one computer will be connected to the router by cable, and all the others will use the wireless connection. A network-ready printer can be plugged directly into the router so that any computer can use it, but because many home printers have only **USB** connectors, it's more usual to connect the printer to the PC that is hard-cabled to the router, and let Windows handle any printing requests that come from other computers on the network.

Basic network security

Moving a wireless router as far away from outside walls as possible, and thereby reducing its broadcasting range, is the only physical security measure you can take and isn't worthwhile. All other security measures are implemented by making changes to the router's internal configuration program. This can usually be done through Internet Explorer or any other web **browser** by typing the Internet Protocol (**IP**) address of your router into the address panel at the top of the web browser. The IP address of a router can be found in its printed or online manual. The address typically consists of four numbers separated by dots. For example, to configure the US Robotics modem used in our screenshots, the address is http://192.168.2.1 (most routers' IP addresses begin with 192.168). Although the layout and names of the configuration menus varies from router to router, the facilities offered are more or less common to all.



▲ You can reconfigure the router to make its settings more secure

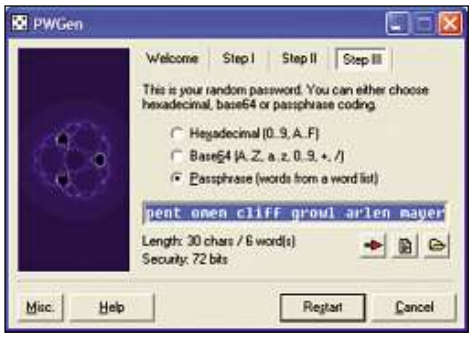
You'll be asked to log in with a username and a password, which you'll find in your router's manual. If no password is supplied, try leaving the password field blank or typing in 'password'. That should give you an idea of why it's so important to set up security. Once you've been granted access to the configuration screens, the first thing to do is change the password. After all, you don't want everybody who uses your network to be able to look up the default password and change the router's security settings.

Once into the configuration program, find where the password settings are and change them to something that's impossible to guess but simple for you to remember, preferably using a mixture of letters and numbers that would not be ▸

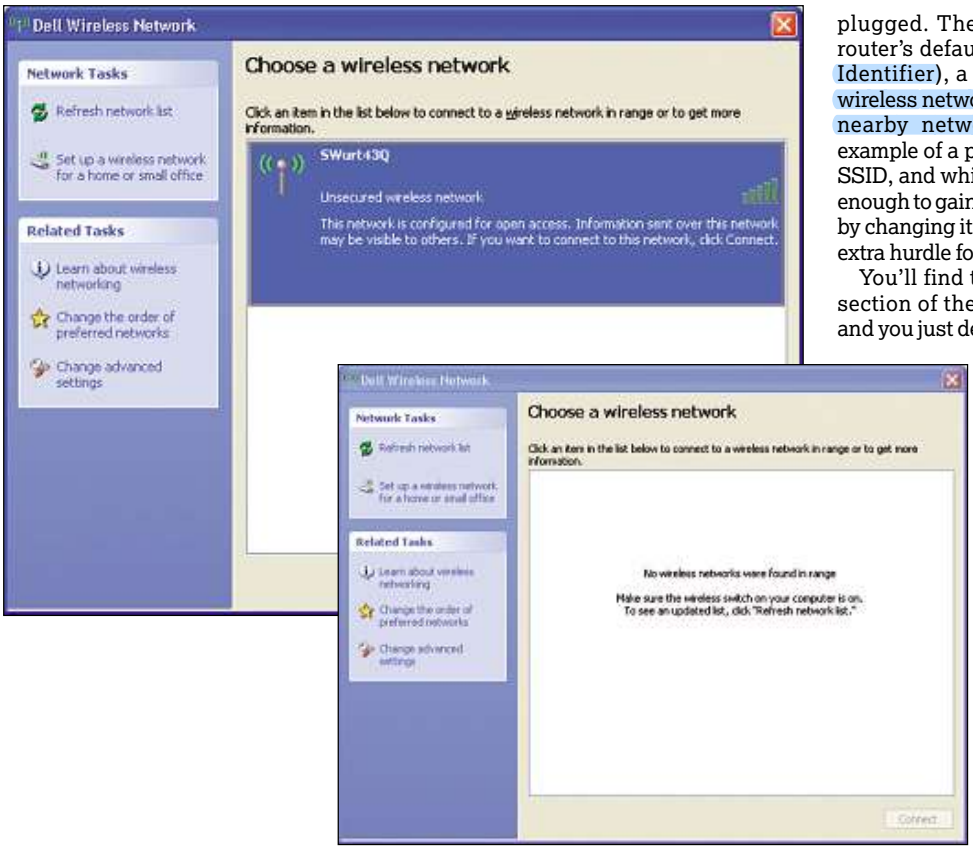
Potent passwords

A short password can typically be cracked in less than a day by software that whizzes through all possible combinations of letters and numbers, or in minutes if it's a word that can be found in a dictionary.

Strong passwords must be randomly selected and should made up of at least 12 characters, numbers and symbols. Unfortunately, strong passwords are hard to remember, but you can get around this by using a phrase made up of five or more randomly generated words. There's an easy-to-use and free program called PWGen, which can generate secure passwords. Download it from **http://tinyurl.com/2dymml**. The file to download is PWGen-2.00-Setup.exe, although the numbers inside the name might be different if a new version has been released since this article went to press. When you run the program, leave the default security level at 72 bits, which is fine for a wireless home network.



▲ PWGen can generate free individual secure passwords



▲ If you disable SSID broadcasting, no one will know there's a Wi-fi network

found in a dictionary.

Most configuration programs require you to explicitly save any changes before moving on, and if you fail to do so the changes will be lost. Do not forget the password to your network – write it down somewhere safe.

In what is likely to be called the System section of the configuration program you may find a remote management option. When this is enabled, the security settings of the router can be changed by a computer elsewhere on the internet and not part of your home network. Always play safe and disable remote management.

Router protection

The advice given so far applies even to cabled networks, but now it's time to look at how weaknesses specific to wireless routers can be plugged. The first thing to do is change the router's default **SSID** (it stands for Service Set Identifier), a name that uniquely identifies a wireless network and distinguishes it from other nearby networks. Manufacturers set every example of a particular router model to the same SSID, and while knowing an SSID is usually not enough to gain unauthorised access to a network, by changing it to something unique you create an extra hurdle for potential hackers to surmount.

You'll find the SSID options in the Wireless section of the router's configuration program, and you just delete the default SSID and type one of your own choosing. Don't use your home address, such as '10 Royal Avenue', as you might as well broadcast a message saying 'valuable PC in this house'. The SSID does not have to be the same as the name you are using for your network in Windows. You should also be able to find an option to disable the broadcasting of the SSID, which makes your network even more secure. By broadcasting an SSID you announce to any wireless device within range that there is a network in operation; and by suppressing it you remove the temptation for anybody stumbling across your network to try to log in.

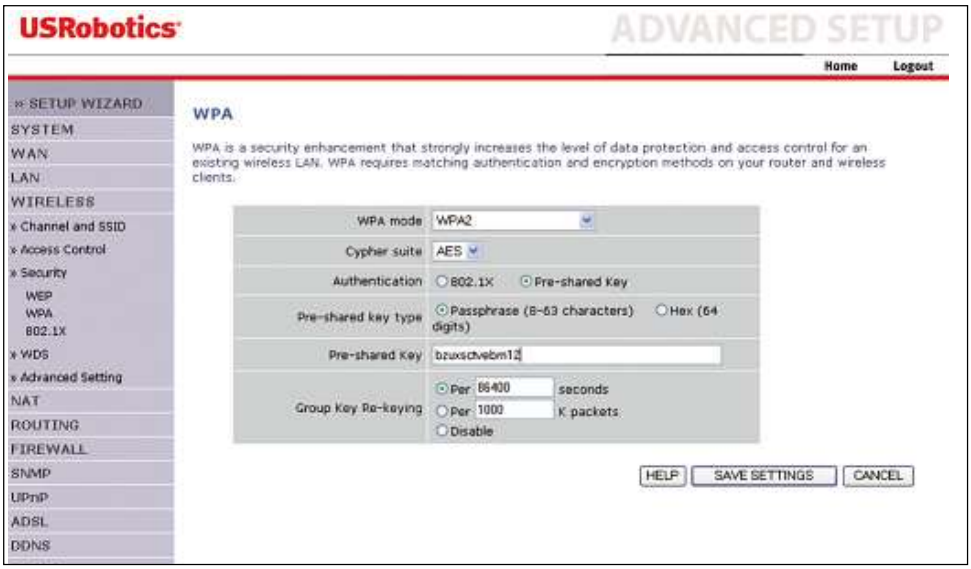
The strongest weapon in a router's security armoury is Wi-fi Protected Access, usually abbreviated to **WPA**. It requires users of a wireless network to identify themselves using a password and scrambles all the data that is sent between them, so even if signals are intercepted by a third party no sense can be made of them. Having to encode every piece of wireless data and then decode it on receipt slows down the speed of a wireless network by a tiny amount, but not enough for users to notice.

Older routers and wireless access points might not be equipped for WPA, using instead the less secure Wired Equivalent Privacy (**WEP**) protection system, but newer routers might offer the ultra-secure upgrade to WPA – WPA2 mode. Any protection is better than nothing, so use WEP if it's all you have, but where the choice exists, always go for WPA and WPA2 if available.

To use WPA2 security, every computer that connects to the network must also be equipped for WPA2, which means having a suitable wireless card and an up-to-date version of Windows XP or Vista installed on each. Even if your computer is running Windows XP and has been updated with Service Pack 2, you may still need to download the WPA2 update, which is available from Microsoft at **http://tinyurl.com/23snrf**.

Set the protection mode by looking in the Wireless section of your router's configuration program, under the heading of Security or a similar word or phrase. Select WPA as the security mode and then set any other options that are related to your choice. Although some of these may look daunting, most of them are mutually exclusive, so you're unlikely to get them wrong. If it's available, select WPA2 rather than

▲ Make sure you change the default user login and password for your router's configuration utility



▲ Encryption is vital for a secure network, and WPA is the best. You can set it up via your router's configuration utility

plain WPA, and for the cipher or encryption type select AES, which stands for Advanced Encryption Standard, a method of encoding data on a network. If WPA2 is not available, use standard WPA in conjunction with the option TKIP as the cipher type, which stands for the Temporal Key Integrity Program, and is the best choice for home networks using WPA.

The remaining settings are the same for WPA and WPA2. You'll need to choose an authentication system, which will be called one of three names: Pre-shared key, PSK or Private. These are just three different terms for the same thing, and selecting any of them simply tells the router that you'd like to use a password for identification purposes. The password is referred to as an 'authentication key'. It can be chosen like any other password by combining letters and numbers typed at the keyboard.

Make a note of the authentication key because every computer that joins the network will need to provide it the first time a connection is made. Thereafter, Windows can be set to automatically use the same key.

Advanced techniques

The steps above will keep a home network safe against anything apart from deliberate attacks by skilled hackers, so unless you have powerful enemies you can sleep easy, but if you do want to beef up network security there are plenty of other tricks. If your router permits it,

▲ Your router can accept connections from a preferred list of MAC addresses to prevent outsiders tapping in

you can reduce the wireless signal strength, keeping it within your own four walls.

You can also set filters within your router configuration program so only designated computers are permitted to join the network. Every wired and wireless network adaptor is identified by a 12-character code called a **MAC** address, so by telling your router that you will only accept connections from a preferred list of MAC addresses, you can prevent outsiders from connecting to your network.

As with all security defences, MAC filtering can be defeated by anybody who knows how to fake a MAC address, but it's still a worthwhile extra line of defence, especially if you're in a suburban street area rather than the IT department of a corporate bank.

To find the MAC address of a network card, click the Windows Start button, then click Run. Type **cmd** in the dialogue box and then press Enter. This opens a command window. Type **ipconfig/all** and then press Enter. Look down the screen to find the name of the wireless adaptor. Note the six pairs of characters designated as the Physical Address. This is the MAC address for the network adaptor in your PC.

Effective checks

While you're tinkering with the configuration options of your router, don't forget to check that its **firewall** is enabled. After taking so much trouble to protect yourself against local interlopers, it would be a shame if you were attacked via the internet instead of your wireless connection. Strictly speaking, if your router has an effective built-in firewall, you don't need a software firewall built into Windows, but it does no harm to have both the router's firewall and the Windows firewall active at the same time.

Controlling access to your private wireless network makes sense. It keeps data on your hard disks secure, stops outsiders from leeching onto your internet connection and prevents the criminally minded from downloading copyrighted material in your name. It will take less than half an hour and give you some insight into how networks are set up, so why not do it today?

Jargon buster

ADSL Transmits digital data at broadband speed on phone lines.

Broadband A fast internet connection, such as ADSL.

Browser A program, such as Internet Explorer, used to view the internet.

Encryption The science of scrambling data so it can only be read by the authorised sender/recipient.

Firewall Software or hardware that prevents unauthorised access to a computer over a network.

Hackers People who break into other people's computers and networks, often in an attempt to steal sensitive information.

IP address An identifying number of a computer attached to a network.

MAC Media Access Control. A type of network address.

Modem A device that enables two computers to communicate with each other over a telephone line.

Router A device used to connect more than one computer together and/or to the internet as an alternative to a modem.

Spyware Software installed surreptitiously to monitor and report back on a computer's use.

SSID A name used to identify a wireless network.

USB Allows quick connection of external peripherals to your PC.

Virus A malicious computer program designed to cause at best annoyance and at worst damage to computer data.

WEP Systems that protect data over wireless networks.

WPA Secure protection for wireless networks.

For more Jargon Buster definitions see page 97 or visit www.computeractive.co.uk