

Wi-Fi and security¹

By Stephen Mason, Barrister

(Advanced copy sent out to Heads of Chambers before publication in the Autumn of 2004)

The author gives you a licence to download and print copies of this article PROVIDED THAT you (a) retain the copyright notice at the end of the article in its entirety, (b) clearly identify this article as being written by the author in electronic and printed versions and (c) only use it for your private use. Commercial use of this article is strictly forbidden without written permission from the author.

~~St Pauls Chambers, St Pauls House, 23 Park Square, LEEDS, LS1 2ND~~

~~www.stpaulschambers.com~~

~~Direct telephone number: 01462 701098~~

~~sewm@stpaulschambers.com~~

~~stephenmason@stephenmason.co.uk~~

¹The author wishes to thank Clive Freedman, 3 Verulam Buildings, Steve Bradley, IT Director Hardwicke Building, Niels J Bjergstrom, editor, Information Security Bulletin and Ian Hughes, a Wireless Security Consultant at BT for offering comments on various drafts of this article. Also Steve Poynter of BT for providing three articles written by members of BT security.

Wi-Fi and security

Any lawyer that has purchased a personal computer, laptop computer, personal digital assistant or other device that holds or is capable of holding client documents, has purchased a device that can be used on a wireless network. Furthermore, in the majority of instances the wireless capability will be automatically switched on. This means your device, when you turn it on, wherever you are located, will send out signals to connect to other devices within range. This article introduced the reader to how a wireless connection takes place, the risks associated with its use and offers some suggestions to reduce the risk of using technology that includes wireless technology.

With wireless networking, your computer can use the services offered by a wireless local area network (often abbreviated to WLAN), such as the Internet, without the need to find a spare telephone line or network connection. This can be a very useful way of obtaining access to essential e-mail and documents when in a court or away from chambers. For instance, BT have recently installed a wireless network in the Royal Courts of Justice, amongst other courts. Wireless networking is also known as Wi-Fi, meaning wireless fidelity (Wi-Fi is a mark used by the Wi-Fi Alliance, formerly known as the Wireless Ethernet Compatibility Alliance, to denote interoperability), and 802.11 networking. The number 802 is the name given to the interoperability standard developed by the Institute of Electrical and Electronic Engineers (IEEE) for Local Area Networks and Metropolitan Area Networks, and Wi-Fi is based on 802.11, which is a sub-set of the 802 standard relating to wireless local area networks. The 802.11 standard was originally developed for ease of use, and was not concerned with security to any great extent. However, you should be aware that wireless networking introduces a number of security issues that must not be ignored.

This article aims to introduce the reader to the basic building blocks of wireless networking, and will discuss

some of the issues that should be considered when using a wireless network. This article does not provide an in-depth analysis of how wireless networking works, and the discussion on security should be considered merely as an introduction that will enable the reader to research and understand the matter more fully in their own time.

How a wireless network works

Wireless technology uses radio waves to transmit and receive, converting binary code used by computers into radio waves, and then re-converting them back into binary code. The IEEE established a standard for this purpose, and named it 802.²

There are several variants of this standard, all of which are available to download in digital format.³ The versions that you are more likely to become aware of are set out in the table below, with the transmission band and speed by which data can be transmitted.

		GHz	Data per second
First version	802.11b	2.4	11 megabits per second (6 to 8 megabits per second is more usual, but some 'lower-end' manufacturers may only achieve 3 to 5 Mbps.)
Improved version of 802.11b	802.11g	2.4	54 megabits per second ("mid to high 20s" Megabits per second is more usual)
Second version	802.11a	5	54 megabits per second ("low to mid 30s" Megabits per second is more usual)

Equipment required

To enable you to use a wireless network, you need a wireless network interface card (NIC), also called a Wi-Fi card. Older computers and laptops may need to have a card inserted to enable you to use wireless technology, although many computers are now sold with a card already built in to the computer.

² The IEEE Committee first met to discuss this topic in February 1980 in the USA, and they used the US date format to denote this – year/month, 80/2 or 802. 802.11 is the 11th task group to be set up under the 802 area.

³ IEEE 802 specifications are made available at no cost six months after they are published, and are available from <http://standards.iee.org/getieee802>. The address of the 802 working group page is <http://group.ieee.org/groups/802/11/>.

How the connection can be made

There are two basic methods by which a wireless connection can be made:

- (1) Through an access point, also called a hotspot. This method connects computers by providing a network infrastructure. It normally provides access to other networks, such as a wired LAN or the Internet. This is formally called a Basic Service Set Network. Several wireless local area networks can be connected together, by means of cables or wireless links between access points, to form Extended Service Set Networks
- (2) Peer-to-peer or ad hoc connection. This method establishes connections between two or more computers without the use of a central access point. This is called an Independent Basic Service Set Network.

A wireless local area network is a collection of computers connected by means of one or more access points. Physically access points are boxes, often interconnected to form large networks and typically connected to the Internet. It is possible for a wireless network to have the capability of connecting many 100s of people using 802.11 network interface cards simultaneously. A wireless local area network can be provided in return for a payment, either by a commercial organization such as BT, or by the owner of a café. In some instances, hotspots of this nature are free to users, provided by the owner of the café as a selling point to encourage people buy their coffee. Alternatively, hotspots can be provided at no cost to the user (without the authority of the network owner), usually because the owner of the wireless network is not aware that the signals they broadcast can carry well beyond the point at which the device is placed. Commercial organizations are prone to discovering their wireless network is broadcasting to a wide area when a hacker discovers their vulnerability and informs the media. Alternatively, some individuals operating a wireless network from home may deliberately or inadvertently broadcast their wireless network and make it available to people outside the home. Finally, a hacker may set up a free hotspot to encourage people to use it with the intention of finding out weaknesses in their computers for various reprehensible purposes.

Activating the network card

Cards already built into new computers may connect to a wireless network automatically, even without your knowledge, permitting you to surf the Internet and send and receive e-mails without doing very much. If you do not have automatic connection, you will probably have to take steps to instruct the computer to make the connection. Depending on the version of your 802.11 card, the card will either actively look for a local wireless network when you instruct it to search, or you may have to obtain the service set identifier of the hotspot yourself (more of these later).

How the network card connects to a hotspot

A wireless network operates in one of three modes: the *ad-hoc*, the *infrastructure* and the *bridge* mode. In the *ad-hoc* mode, a number of people with network cards can connect to each other, making up a cell. This mode of connecting is designed to enable people within range of the radio waves to communicate with each other directly. There is no need for users to communicate with a third party provider – they just communicate directly with each other. If anybody wants to communicate outside the cell, one of the members must operate as a gateway and route the communication outside the cell by means of an alternative connection, wired or wireless, including but not limited to GPRS (GSM (global system for mobile communication) packet radio service) and 3G (third generation mobile telephones).

Where the *infrastructure* mode is in operation, each user connects to a central station, (also know variously as a base station, access point or hotspot). Most users will probably use their wireless connection in this fashion, where the central station acts as the go-between, acting as a bridge between the transmission of the data from the computer to the central station and forwarding the data on to the appropriate network, either to another wireless connection or to the wired network.

The *bridge* mode permits two or more central stations to connect to each other. An example would be to connect two networks between buildings.

All three of these modes can work simultaneously, especially if you use Windows 2000 or XP. For instance, you may think you are only connected to a hotspot in *infrastructure* mode, but your computer may have also connected to devices working in other modes, such as *ad-hoc*, close to the hotspot you are connected to.

Before data can be communicated between the network card and the hotspot, the card and the access point need to establish an association. This process comprises the following steps:

- The hotspot, access point or base station transmits data in the form of frames. The central station constantly sends a beacon management frame out at a fixed interval. To link to a hotspot, the network card can do one of two things. It can listen for the beacon message to identify the access point that is within range. This action can be undertaken automatically or manually, depending on the version of your card and computer, and is called 'passive mode'. Each wireless card has a radio identity, called the service set identifier (SSID) or extended service set identifier. When the base station sends out a beacon frame, it includes the service set identifier. The SSID is not encrypted, but sent out in clear text. The danger with this is discussed below when

dealing with security. When your network card identifies the hotspot, it can determine whether to connect. Alternatively, your network card can send a probe request management frame to find a hotspot that is affiliated to a particular SSID that you may wish to connect to, called 'active mode'.

- When your network card identifies the hotspot, your card and the hotspot undertake a process of mutual authentication by exchanging data in management frames. There are two standard mechanisms that can be used, the *Open System Authentication* and the *Shared Key Authentication*. The 802.11 protocol provides for the open system authentication as the default method of authentication between your card and the access point. Basically, anybody that wants to be authenticated with the base station can be. Even when this information is sent using the wired equivalent privacy protocol (WEP), which is designed to provide for confidentiality when using a wireless network, the authentication management frames are still sent in clear text, thus helping to defeat the use of this particular security protocol. The shared key authentication provides for the standard authentication process, by which the base station and network card exchange a challenge and respond protocol, as follows: your network card sends a request to associate to the base station, the base station responds with what is termed 'challenge text' which your network card then encrypts using your wired equivalent privacy key and returns the encrypted text to the base station. If the text returned to the base station is encrypted correctly, your network card is permitted to communicate with the base station. The authentication process includes the use of a shared secret key as an additional layer of authentication. Unfortunately, shared key authentication has a number of weaknesses, one of which is that the encryption process uses the wired equivalent privacy protocol, which is so weak as to be considered by many in the industry to be worthless. The IEEE has been working on a better protocol (see below for a discussion of this security measure). Further, you may have noted that as the base station and your network card go through the challenge and response protocol, the challenge initiated by the base station is sent in clear text. This means a hacker can listen to this exchange of data. In the process, the hacker can obtain the challenge text, sent in clear text, and the same challenge text after it has been encrypted. With the benefit of obtaining this information, it is merely a matter of solving the shared authentication key, which is a relatively easy matter. The importance of this should not go unnoticed. The same keys that are used to encrypt the shared key authentication protocol with the base station, are also used by your wired equivalent privacy protection. Once the shared key authentication is compromised, your wired equivalent privacy key is

also compromised. This means the hacker can then decipher all the communications between the base station and your computer. This is the reason you need to protect your computer, by ensuring you have appropriate security mechanisms in place, as discussed later in this article.

- Once the hotspot and network card have authenticated each other, the network card sends a request for association, and the hotspot responds with an appropriate association response frame. Upon completion, your computer is associated, or linked, to the wireless network.

For most people that use wireless networking, the process of connecting to a hotspot, base station or wireless network is hidden, and the technical issues remain a confusing mass of jargon that you would be wise take the time to master.

If you use wireless networking on a computer containing confidential information, you should be aware of the security issues associated with the use of wireless networking. It must be emphasised that most commentators that write about Wi-Fi security point out that wireless networking is an inherently insecure medium, and the author has spoken to a number of security managers in large organizations that have implemented Wi-Fi across the organization, not knowing what the security issues are or what questions to ask, but trusting the vendor to provide for the proper security of the network. The security of a WLAN can be compared with that of a computer network connected to the Internet without having a firewall in place. It lends itself to being open to attack by outsiders.

You will have to assess the risks you face and take sufficient precautions that you consider reasonable in the circumstances to protect the information that passes between your computer and the base station when using a wireless network. If you include confidential information on your laptop and use a wireless network, it is suggested you give careful consideration to the management and security of the wireless connection. In particular, establishing and managing a professionally designed security architecture is even more important with a WLAN than with a wired network because of the propagation of radio waves. The apparent low price and ease of use of a WLAN does not include the hidden costs of security.

Some risks

There are a number of risks associated with the use of a wireless network, some of which are discussed below.

Leakage

Not only is your computer vulnerable to attack from those people connected to the same wireless network that you

can see in the vicinity of the network, but you should be aware that the radio signals transmitted by wireless networks often leak beyond the solid walls of a building. The range for a wireless network can be between 300 and 500 feet, although some people that sniff wireless networks have claimed they have picked up e-mails when flying in aeroplanes cruising at altitudes of between 1,500 and 2,500 feet.⁴ Professionally executed attacks using special equipment such as highly directional disk antennas can be carried out from up to 20 miles away. This attribute of wireless networks opens computers up to various types of attack, including sniffing, spoofing and third parties connecting to a network using your computer without authority.

Sniffing

This is the most widely known of the attacks. Hackers drive or walk around a city or particular area with a suitably equipped computer, searching for poorly secured or unprotected wireless networks. This is called *war driving* or *walking*. This involves switching the wireless card receiver on and letting the receiver capture packets moving over the network. Sniffing is a passive activity that cannot be detected. It is wrongly assumed that the 802.11 signals do not travel over long distances. The signals can travel for a greater distance beyond the wireless network than intended, but the further they travel, the weaker they become. As a result, most cards used in laptop computers cannot pick up signals unless they are within a clear range of the wireless network. However, if an external antenna is connected to a laptop, the range can increase significantly. The type of information that a hacker can obtain using this method, depending on the software used, can include the following: the media access control (MAC) address of the access point and any other devices, such as personal computers or personal digital assistants, the network name, the service set identifier (SSID), the name of the manufacturer, which channel that it was heard on (802.11b can operate on 13 channels), whether wired equivalent privacy (WEP) is enabled, the strength of the signal and the signal to noise ratio.⁵ The hacker can see what you are doing, in other words, if you transfer data across the airwaves, the hacker will see this data, and as a result, this data will be copied into their computer. Examples of the data that a hacker can see include all incoming and outgoing e-mails, together with any attachments. Furthermore, if you are connected to a server or a network, a hacker can then use your connection to gain access to the server or network. Some readers may also have heard of the activity called *war chalking*. This activity describes enthusiasts that identify hotspots and indicate the whereabouts of the hotspot by providing relevant information on the ground, written in chalk.⁶

Spoofing

Spoofing is where a hacker sets up their own wireless network, with the aim of getting users to connect to it, thus

enabling the hacker to obtain personal information such as passwords, usernames and credit card details. If you do not have a firewall in place, a hacker may be able to gain access to all of the files on your computer.

Unauthorized connection

Hackers can obtain unauthorized access to laptop computers to obtain information or insert viruses in the same way as they are able with computers connected to the Internet. A particularly dangerous situation can arise if an attacker gains simultaneous access to a computer through a wireless connection and the Internet. If such a connection is effected, the hacker will be able to see data that is both encrypted and in clear text at the same time. This type of scenario can compromise many types of cryptographic keys.

Some security mechanisms⁷

Unless you take appropriate precautions to safeguard your data, a third party may be able to intercept your e-mails, examine your files and records, and use the wireless network and Internet connection to distribute their own messages and communications. If you use Wi-Fi, you should take care to secure your computer from attack, especially if you have a range of confidential documents stored in the computer or utilise wireless networking to send and receive confidential information. Below are some suggestions to improve the security of your wireless network. Some of these suggestions will require technical assistance to implement. It is also important to note that WLAN security is a complex area that needs to be audited when it has been implemented.

Wired equivalent privacy protocol (WEP)

This protocol was designed to ensure the traffic that moves over the wireless network is confidential. Wired equivalent privacy is part of the 802.11 standard, and some network interface cards and vendors of access points support this encryption standard. This protocol is not supported by BT Openzone, the service provider for the wireless hotspots in the Royal Courts of Justice.

If you activate WEP, the network interface card goes through an encryption process using a secret number before transmitting each packet of data. The encrypted data is then sent over the wireless network to the base station. The process of decryption is carried out upon receipt by the base station, using the same secret number. It should be noted that data is only encrypted between 802.11 points, so when it is transferred to a computer connected to telephone lines, the standard no longer applies.

However, it is for the base station to inform you that it can be used, and in addition, WEP is seriously flawed and vulnerable to successful attack within a short space of time. The shared secret key is either 40 or 104 bits, although some

⁴ Bob Brewin, 'War flying: Wireless LAN sniffing goes airborne,' *Computer World*, 30 August 2002, available at <http://www.computerworld.com/printthis/2002/0,4814,73901,00.html>.

⁵ Craig Ellison, 'Exploiting and Protecting 802.11b Wireless Networks', 4 September 2001, available at http://www.extremetech.com/print_article/0,1583,a=13880,00.asp.

⁶ See www.warchalking.org for details.

⁷ A number of selected articles that may be of interest to the reader include: William A. Arbaugh, Narendar Shankar, and Y.C. Justin Wan, 'Your 802.11 Wireless Network has No Clothes' March 30, 2001, available from <http://www.cs.umd.edu/~waa/wireless.pdf>; Scott Fluhrer, Itsik Mantin, and Adi

Shamir, 'Weaknesses in the Key Scheduling Algorithm of RC4' available from http://downloads.securityfocus.com/library/rc4_ksaproc.pdf; Arunesh Mishra and William Arbaugh, 'An Initial Security Analysis of the IEEE 802.11 Security Standard' February 6, 2001, available from <http://www.cs.umd.edu/~waa/1x.pdf>; Jesse R. Walker, 'Unsafe at any key size; an analysis of the WEP encapsulation' IEEE Document 802.11-00/362, October 2000, available from <http://group.ece.icee.org/groups/802/11/Documents/index.html> (It can be found by looking up the year 2000 and identifying its document number, which is 362); Gary Tagg, 'IEEE 802.11 Wireless LAN Security', *Information Security Bulletin*, vol. 8, issue 9 (November 2003).

vendors support stronger keys. No matter what key you have on your computer, the receiving station must use the same key for decryption. The way WEP works means that a hacker can decrypt the files that have been transmitted if they have monitored the network for long enough.

There are a number of problems that render WEP unsafe, the main one of which relates to the encryption process, which is not secure, because it has a technological weakness in its encryption mechanism. The RC4 stream cipher brings together a WEP key with a 24 bit random number known as an Initialization Vector (IV) to encrypt the data. When the data is sent over the wireless network, each packet contains the IV followed by the encrypted data. Clearly a hacker will not know the clear text before it is encrypted, so they cannot immediately break the key (with the caveat mentioned above). One attack a hacker can implement to identify the WEP key that has been used to encrypt the data, is to focus on the numerical limitation associated with the IV. There are only 2^{24} possible values for the IV. On a wireless network that is used heavily, the RC4 mechanism will pick IV numbers repeatedly. In fact the situation is even worse. Several WLAN card manufacturers do not cause the IV to be changed for each packet, and some reset the IV to 0 each time the card is powered up or reset and then simply increments it. As the hacker listens in to the encrypted traffic, IV numbers that are repeated will enable the hacker to infer what the WEP key is.

Some 802.11 network cards will have two WEP keys. Where a network card has two keys, one key is provided to encrypt the data between the base station and your computer. The second key is used to encrypt broadcast transmissions. Where a network card only has one key, this key will be used for both functions. The administrator of the base station sets a specific time that the base station broadcasts a WEP key, encrypting the new key with the old key. The length of time between the broadcast of each new key needs to be set at such a period that a hacker will not have sufficient time to intercept a sufficient number of packets to crack the key. This measure is relatively easy to implement and does not require any additional installation.

Despite its flaws, you should consider enabling WEP where you are able to, especially if operating a home wireless network. You will have a better opportunity of protecting your system with WEP by changing your secret key at reasonable intervals. Whilst it will not keep the determined hacker out, it will stop most people from trying to gain access to your computer.

Another technology worth considering is 802.1X authentication and the Wi-Fi Protected Access (WPA) standard, which provide better security by replacing the weak 802.11 authentication mechanisms. 802.1X needs to

gain access to an authentication server, and can provide authentication for both wired and wireless networks. This standard adds some complexity to the network infrastructure, and will increase the cost of using wireless networks safely. A new layer of authentication is provided. When your wireless card requests access to the base station, the base station requires more credentials from you. You then provide these additional credentials, which the base station forwards to a server that will authenticate your identity. You will need to find a base station that supports this protocol, and you may also need additional software to implement this particular security solution.

Restrict access to the wireless network to “known” devices only

There are two aspects to consider in relation to this matter. First, you should ensure that your network card only connects to a wireless network in the mode you intend it to. In essence, you have two options:

- Leave the default setting on in Windows 2000 and XP (please note, these operating systems are used as examples, and it will be for you to determine how the setting is set if you use any other form of operating system), which means your network card will connect to all three modes: *ad-hoc*, *infrastructure* and *bridge*.
- Alter the default settings to limit the connections your network card can make. For instance, you could set the network card to connect to your home computer, any other trusted hotspot and, in the case of the hotspots in the courts, to BT Openzone.

One method used by vendors to provide a degree of security (usually to a corporate wireless network, but possible to implement in a public hotspot, such as the Royal Courts of Justice), is to restrict access to the base station only to those users that it recognises. Every network card is given a unique identifier known as its media access control (MAC) address. The MAC address, because it is supposed to be unique, is used in the first and last part of the transmission process. The wireless network will only permit devices with a known MAC address to obtain access to the network, and others are filtered out. However, this method is flawed. The media access control address identifies the computer and base station, not the identity of the user. As a result, a hacker with an acquired ‘good’ address can connect to the network and place various eavesdropping programs, spy ware or Trojan horses on to the base station.

Change the default system identity

Each wireless card has a radio identity, called the service set identifier (SSID) or extended service set identifier. The SSID is used as a form of password for your network interface card to join a wireless network. The 802.11 standard requires your network interface card to

have the same SSID as the access point. To add a level of security to wireless networking, some vendors of base stations have begun to switch off the beacon frame that broadcasts the service set identifier, or at least provide the system operator with a configuration option to do so – but the default setting is still typically left to “on”. This is an action you should also consider undertaking on your computer. When you turn the service set identifier off, you will have to type the SSID into your computer, rather than clicking the ‘scan’ button.

By changing this setting, you will retain a degree of anonymity and make it harder for hackers to make an accidental connection to your laptop. If you do not switch it off, all a hacker has to do is wait until a users laptop re-associates with the station when they roam around the network.

Use easy to remember but hard to guess passwords

You should change the administrator’s account name and password. It is good practice to change these passwords for all of your hardware and software. Most passwords provided by manufacturers, such as the default administrator password, tend to be the first line of attack by a hacker because users do not, generally, change them. Each manufacturer has a different default, although this can be related to the manufacturers default SSID, which makes the hacker’s life much easier. Changing the default values for username and password is essential, and you are urged to use a password that is not easily guessed or can be found by password-cracking devices. Passwords should contain a minimum of seven or eight characters in length, and include a mixture of numerals and upper case characters. It is advisable to change passwords regularly. This is also something you can do to reduce your vulnerability when using a wireless network at home.

The Internet protocol address

Before an intruder can obtain access to your computer, they need the SSID and an Internet protocol (IP) address. Many wireless stations use a dynamic host configuration protocol (DHCP) to assign an IP address to a user as they join the network. Where you enable the DHCP, the hacker obtains an IP address in the same way as any other user, and this gives them access to your laptop, which may include files and data, depending on the permissions you have set. Potentially, everything you use in Windows is vulnerable, depending on your settings. For instance, if a hacker has associated to the same wireless address they can see all other users connected to the network. If you have file sharing turned on, the hacker can gain access to your laptop and obtain what documents they feel like, transferring them to their own computer. This is something that you should be aware of, whether using a home or

public wireless network.

Turn off the wireless card when not in use

If you can turn off your wireless card, do so if you are not using it. Many portable personal computers have a small switch on the outside of the case that will allow you to turn off internal cards. This action will also increase your battery life a little.

Security options for the home

Depending on the degree of risk you consider you face, there are a number of additional options you might consider. The following are some suggestions that may be practical and appropriate, depending on your assessment of the risks.

Your base station

Place the access point away from the front of your house to limit the radio spillage into the public road outside. If you are not easily detected you are much less likely to be hacked. Whilst this only offers minimal protection, you should consider it to be the first line of wireless protection. Set up a WEP key for your base station and personal computer, otherwise anybody with a wireless network card can link up with you and surf the Internet at no cost, using your signal. In short, change all the default settings: the SSID, usernames and passwords. Turn on WEP or, in preference, the WPA if this is available.

Virtual private networking

If you are connecting to a Chambers or home network via the Internet from outside, consider using a virtual private network (VPN). This is a method, using third party encryption, by which a secure link is made between two points connected over the Internet.

Protect your computers

Use a personal firewall, and implement security patches for your operating system when they are made available. It might be useful to configure your firewall to only permit incoming or outgoing traffic that you have approved. Do not turn on file or printer sharing on a wireless network. Most computers have the ability to share files between computers, and if you enable this facility and use wireless networking, it is possible for an unsophisticated hacker to obtain access to your files. If you decide to share files in this fashion, it is advisable to do so using a router connected to the computers by means of cables, and ensure that your wireless card is turned off before you do this, and do not turn it back on until the ‘share’ has been removed.

This introductory article illustrates there are similarities between the use of a home wireless network and the use of Wi-Fi in a public place, such as a cafeteria. This article only

seeks to introduce you to the problems, not to provide answers. If you decide to use wireless networking, whether in the Royal Courts of Justice, at home or in a public place, it would be prudent for you to consult an IT network security specialist in order to implement appropriate security safeguards. You should take active steps to protect the confidential information held on your computer.

Check list for your computer

Take the time to understand how wireless networking works

Master the technical jargon – don't let your ignorance increase your exposure to unnecessary risks

Have a personal firewall

Enable the wired equivalent privacy protocol (WEP) where possible

Consider implementing 802.1X authentication

Only connect to a wireless network that will not permit devices with an unknown media access control (MAC) address to obtain access to the network

Turn the service set identifier (SSID) off to retain a degree of anonymity

Change the administrator's username and password for all your hardware and software

Ensure you have no file sharing when using a public hotspot

Download security patches

Install anti-virus software

If you can turn off your wireless card, do so if you are not using it.

Check list for your home wireless network

All the other check list, plus the following:-

Set up and change the default username and password for your base station

If you are connecting to a Chambers or home network via the Internet from outside, consider using a virtual private network (VPN).

If you share files, use a router connected to the computers by means of cables and disable your wireless connection when using file sharing

Place the access point away from the front of your house to limit the radio spillage into the public road outside.