

Chapter 8

Wireless Network Security

Topics in this chapter:

- **The Basics of Wireless Networks**
- **Basic Wireless Network Security Measures**
- **Additional Hotspot Security Measures**

- Summary**
- Additional Resources**

Introduction

I have a wireless network in my home. I am no “Mr. Fix-it” when it comes to home projects, so when I had to figure out how to run network cable from the router in the kitchen to my kids’ rooms, going through walls and floors and around cinder blocks, I sprang for the wireless equipment instead. At first, it was primarily so that I could use my laptop from any room in the house, but as time went by we eventually switched almost every computer in the house to a wireless connection.

Wireless networks provide a great deal of convenience and flexibility, and are relatively easy to set up. Actually, they may be too easy to set up. Some pieces of wireless equipment are almost plug-and-play devices, which might explain why so many people don’t read the manual or do their homework to figure out how to secure the network airwaves.

I took my laptop out with me today to work on this book. I had no particular need for a network connection since I was just using my word processor on my computer, but as I drove through the subdivision I watched as my wireless network adapter detected network after network completely insecure and announcing their presence to the world. Unfortunately, this seems to be the norm rather than the exception.

This chapter will take a look at wireless network security from two perspectives, and the steps you must take to use it securely in both. We will start with a brief overview of the wireless protocols and technology, and then look at what’s required to secure your own home wireless network to keep unauthorized users out of your network. Lastly, we will examine the security precautions you should take to securely use a public wireless network.

The Basics of Wireless Networks

Think about how a wireless network affects the security of your network and your computers. When you have a wired network, you have only one way in more or less. If you put a firewall on the network cable between your computers and the public Internet, your computers are shielded from most unauthorized access. The firewall acts as a traffic cop, limiting and restricting access into your network through that single access point. Now you throw a wireless device on your network. It doesn’t matter if it’s one computer with a wireless network adapter or a wireless router or access point, the results are the same: you are now broadcasting data through the air. Your “access point” is now all around you. Rather than a single point of access that can be easily protected, your access point is now three dimensional, all

around you, at various ranges, from the next room to the house next door to the roadside in front of your home.

Are You Owned?

Wardriving

The practice of cruising around in search of available wireless networks is known as “wardriving.” The term derives from a similar activity to search for available modem connections by “wardialing,” or automatically dialing phone numbers to identify which ones result in a dial-up modem connection.

Armed with a wireless device and antenna, wardrivers patrol city streets and neighborhoods and catalog the wireless networks they discover. Some sophisticated wardrivers also tie their wireless network discovery to a GPS to identify the exact coordinates of each wireless network.

For years, a group dedicated to demonstrating how insecure most wireless networks are and increasing awareness of wireless network security issues has organized something called the WorldWide WarDrive (WWWD). After four years, they have decided that the WWWD has done all it can to raise awareness and have moved on to other projects, but their efforts helped to spotlight the issues with insecure wireless networks.

For more information about wardriving and wireless network security in general, you can check out the book *WarDriving and Wireless Penetration Testing*.

Wireless equipment often boasts of ranges over 1,000 feet. The reality is that unless there are no obstructions, the temperature is above 75 and less than 78, the moon is in retrograde and it's the third Tuesday of the month, the range will be more like 100 feet. But if your wireless data can make it the 75 feet from your wireless router in the basement to where you are checking your e-mail while watching a baseball game as you sit on the couch in your living room, it can also make it the 60 feet over to your neighbor's house or the 45 feet out to the curb in front of your home. Although standard off-the-shelf equipment doesn't generally have tremendous range, the wardrivers, a term used to describe actively scouting areas specifically looking for insecure wireless networks to connect to, have homegrown super antennas made with Pringles cans and common household items from their garage that can help them detect your wireless network from a much greater range.

126 Chapter 8 • Wireless Network Security

It is important that you take the time to understand the security features of your wireless equipment and make sure you take the appropriate steps to secure your network so that unauthorized users can't just jump onto your connection. Not only are your own computers exposed to hacking if an attacker can join your network, but they may initiate attacks or other malicious activity from your Internet connection which might have the local police or the FBI knocking on your door to ask some questions.

A wireless network uses radio or microwave frequencies to transmit data through the air. Without the need for cables, it is very convenient and offers the flexibility for you to put a computer in any room you choose without having to wire network connections. It also offers you the ability to roam through your home freely without losing your network connection.

In order to connect to the Internet, you will still need a standard connection with an ISP. Whether you use dial-up or a broadband connection like DSL or a cable modem, the data has to get to you some way before you can beam it into the air. Typically, you would connect your DSL or cable modem to a wireless router and from there the data is sent out into the airwaves. If you already have a wired router on your network and want to add wireless networking, you can attach a wireless access point to your router. Any computers that you wish to connect to the wireless network will need to have a wireless network adapter that uses a wireless protocol compatible with your router or access point.

A variety of wireless network protocols are currently in use. The most common equipment for home users tends to be either 802.11b or 802.11g with 802.11a equipment coming in a distant third. The most common protocol, particularly for home users, has been 802.11b; however, 802.11g is becoming the default standard because of its increased speed and compatibility with existing 802.11b networks. The following is a brief overview of the different protocols:

802.11b

Wireless network equipment built on the 802.11b protocol was the first to really take off commercially. 802.11b offers transmission speeds up to 11 mbps, which compares favorably with standard Ethernet networks—plus, the equipment is relatively inexpensive. One problem for this protocol is that it uses the unregulated 2.4GHz frequency range, which is also used by many other common household items such as cordless phones and baby monitors. Interference from other home electronics devices may degrade or prevent a wireless connection.

802.11a

The 802.11a protocol uses a regulated 5GHz frequency range, which is one contributing factor for why 802.11a wireless equipment is significantly more expensive than its counterparts. 802.11a offers the advantage of transmission speeds of up to 54 mbps; however, the increased speed comes with a much shorter range and more difficulty traversing obstructions, such as walls, due to the higher frequency range.

802.11g

The 802.11g protocol has emerged as the new standard at this time. It combines the best aspects of both 802.11b and 802.11a. It has the increased transmission speed of 54 mbps like 802.11a, but uses the unregulated 2.4GHz frequency range, which gives it more range and a greater ability to go through walls and floors, and also helps keep the cost of the equipment down. 802.11g is also backwards-compatible with 802.11b, so computers with 802.11b wireless network adapters are still able to connect with 802.11g routers or access points.

Next-Generation Protocols

Wireless networking is relatively new and constantly evolving. A number of new protocols are currently being developed by the wireless industry, such as WiMax, 802.16e, 802.11n, and Ultrawideband. These protocols promise everything from exponentially increasing home wireless network speeds to allowing you to use a wireless connection to your ISP and even maintain a wireless network connection while in a moving vehicle.

Some of these concepts may not appear in the immediate future, but others are already in use in one form or another. Most wireless network equipment vendors have already begun producing Pre-N or Draft-N devices. These devices are based off of the 802.11n protocol, but have been produced before the 802.11n protocol has actually been finalized. They promise speeds 12 times faster than 802.11g, and a range up to four times that of 802.11g.

The major mobile phone carriers, such as Verizon, Cingular, and TMobile, all offer some sort of broadband wireless access which can be used virtually anywhere their cellular phone network can reach. Using a service like this can give you wireless access almost anywhere, any time, without restriction to any specific site.

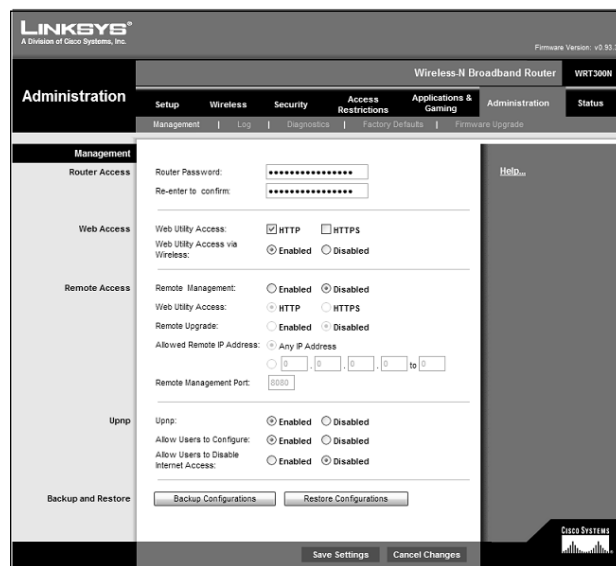
Basic Wireless Network Security Measures

Regardless of what protocol your wireless equipment uses, some basic steps should be taken to make sure other users are not able to connect to your wireless network and access your systems or hijack your Internet connection for their own use.

Secure Your Home Wireless Network

To begin with, change the username and password required to access the administrative and configuration screens for your wireless router. Most home wireless routers come with a Web-based administrative interface. The default IP address the device uses on the internal network is almost always 192.168.0.1. Finding out what the default username and password are for a given manufacturer is not difficult. The equipment usually comes configured with something like “admin” for the username, and “password” for the password. Even without any prior knowledge about the device or the manufacturer defaults, an attacker could just blindly guess the username and password in fewer than ten tries. With a default IP address and default administrative username and password, your wireless router can be hacked into even by novices. Figure 8.1 shows the administration screen from a Linksys wireless router. This screen allows you to change the password for accessing the router management console.

Figure 8.1 The Administration Screen from a Linksys Wireless Router



Make sure you change the username to something that only you would think of. Just like renaming the Administrator account on your computer, you want to choose a username that won't be just as easy to guess as "admin" or whatever the default username was. You also want to choose a strong password that won't be easily guessed or cracked. Lastly, you should change the internal IP subnet if possible. The 192.168.x.x address range is for internal use only. A large percentage of those who use this address range use 192.168.0.x as their subnet, which makes it easy to guess. You can use any number from 0 to 254 for the third octet, so choose something like 192.168.71.x so potential attackers will have to work a little harder. For details on user accounts and administrator privileges, see Chapter 1.

Remember, the goal is to make it difficult for attackers or malware to penetrate your system. Nothing you do will make your network 100-percent impenetrable to a dedicated and knowledgeable attacker. But, by putting various layers of defense in place such as complex passwords, personal firewalls, antivirus software, and other security measures, you can make it sufficiently hard enough that no casual attacker will want to bother.

Change the SSID

Another big step in securing your home wireless network is not to announce that you have one. Public or corporate wireless networks may need to broadcast their existence so that new wireless devices can detect and connect to them. However, for your home, you are trying to prevent rogue wireless devices from detecting and connecting to your network.

The wireless router or access point has a Service Set Identifier (SSID). Basically, the SSID is the name of the wireless network. By default, wireless routers and access points will broadcast a beacon signal about every 1/10 of a second, which contains the SSID among other things. It is this beacon which wireless devices detect and which provides them with the information they need to connect to the network.

Your wireless network will most likely only have a handful of devices. Rather than relying on this beacon signal, you can simply manually enter the SSID and other pertinent information into each client to allow them to connect to your wireless network. Check the product manual that came with your wireless equipment to determine how to disable the broadcasting of the SSID.

Your device will come with a default SSID which is often simply the name of the manufacturer, such as Linksys or Netgear. Even with the SSID broadcasting turned off, it is important that you not use the default SSID. There are only a handful of manufacturers of home wireless equipment, so it wouldn't take long to guess at the possible SSIDs if you leave it set for the default. Therefore, you need to change this, and preferably not to something equally easy to guess, like your last name.

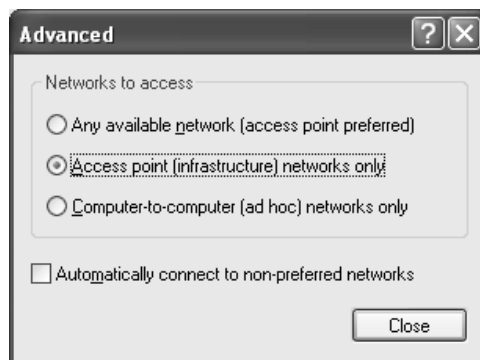
Configure Your Home Wireless Network

Next, you should configure your wireless network and any wireless network devices for infrastructure mode only. Two types of wireless networks are available for set up: infrastructure and ad hoc. In an infrastructure mode network, a router or access point is required, and all of the devices communicate with the network and with each other through that central point.

An ad hoc network, on the other hand, allows each device to connect to each other in an “ad hoc” fashion (hence the name). Since you are going through all of this effort to make your router or access point more secure, you also need to make sure that the wireless devices on your network are not configured for ad hoc mode and might be providing another means for rogue wireless devices to gain unauthorized access to your network.

By accessing the Properties for your wireless connection, you can click the **Advanced** button at the bottom of the Wireless Networks tab to configure whether your wireless adapter will connect to infrastructure, ad hoc, or both wireless network types (see Figure 8.2).

Figure 8.2 Configuring Connections for Your Wireless Adapter



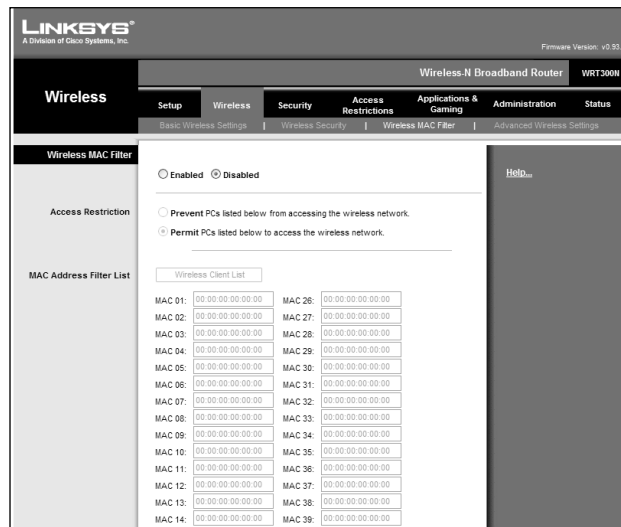
Restrict Access to Your Home Wireless Network

To restrict access to your wireless network even further, you can filter access based on the MAC (Media Access Code) addresses of your wireless devices. Each network adapter has a unique MAC address that identifies it. As stated earlier in this chapter, your network will most likely consist of only a handful of devices, so it wouldn't require too much effort to enter the MAC address of each device into your wireless router or access point and configure it to reject connections from any other MAC addresses.

Even after you do all of these things, you're not completely secure. You're obscure, but not secure. Using tools freely available on the Internet, a war-driver could still intercept your wireless data packets as they fly through the air. They would be doing so blindly because your wireless access point is no longer broadcasting its presence, but it can still be done. Intercepting the traffic in this way can provide an attacker with both the SSID and a valid MAC address from your network so that they could gain access.

By adding the MAC addresses of the devices that you know you want to connect to your wireless network, you can block access by other unknown devices and protect your wireless network (see Figure 8.3).

Figure 8.3 Adding MAC Addresses to Your Wireless Router



Use Encryption in Your Home Wireless Network

To further protect your wireless communications, you should enable some form of encryption. Wireless manufacturers, in their haste to start selling equipment, rushed to create WEP (Wired Equivalent Privacy) encryption to provide some level of security while waiting for the official 802.1x security protocol to be standardized. It was quickly discovered that the underlying technology of WEP has a number of flaws which make it relatively easy to crack.

The wireless industry has since migrated to the newer WPA (Wi-Fi Protected Access) encryption, which offers a number of significant improvements over WEP yet remains backwards-compatible with WEP devices. In order to use WPA though, all devices on the network must be WPA-capable. If one device uses WEP, the network

132 Chapter 8 • Wireless Network Security

will not be able to use some of the improved security features of WPA and your network may still be vulnerable to being exploited by the weaknesses found in WEP.

WPA2 has recently emerged to replace even WPA. Devices that are WPA2-compliant meet stricter security requirements. Windows XP with Service Pack 2 (SP2) fully supports the features and functions of WPA2, allowing a higher level of wireless network security as long as all of your wireless network clients are capable of the same security level.

While a knowledgeable and dedicated attacker with the right tools can still crack the encryption and access your wireless data, this should not discourage you from enabling it. It would be unusual for someone to dedicate that much time and effort to get into your wireless network when they can probably find five more unprotected wireless networks on the next block. It isn't practical to think you will be 100-percent secure, but turning on some form of encryption combined with the other precautions listed previously will deter the casual hacker and curious passerby.

The more complex encryption schemes require more processing power to encode and decode, so you may consider sticking with the 40-bit (64-bit on some devices) WEP encryption rather than the stronger 128-bit, or even the WPA encryption, if you notice any performance issues. It is the difference between locking your house with a normal lock or using a deadbolt. Since an attacker can get past both with about the same effort, you may as well use the one that is easier for you but that still prevents most users from accessing your wireless network.

Review Your Logs

Most wireless routers keep logs of the devices that attach to them. Even if you have taken all of the preceding steps to secure your wireless network, it is a good idea to periodically review the logs from your wireless router and check for any rogue devices that may have gained access.

The other major points to consider regarding a secure home wireless network are the same as they are for a wired network or computer security in general. You should make sure you are using strong passwords that can't be easily guessed or cracked on all of your devices, and protect your computers with personal firewall software.

One final word of advice when it comes to securing your wireless network: a device that is not connected to the Internet can't be attacked or compromised *from* the Internet. You may want to consider turning off your wireless router or access point overnight or when you know that it won't be used for extended periods. If there are too many users trying to access the Internet and use their computers at varying hours, it may be impractical to turn off the wireless router, but you can still

turn off any computers when not in use so that they are not exposed to any threats whatsoever.

Use Public Wireless Networks Safely

Public wireless networks, often referred to as hotspots, are springing up all over. National chains such as Starbucks Coffee, Borders Books, and McDonalds' have started adding wireless network access to their establishments through services provided by companies like TMobile or Boingo. Major hotel chains have gone from no access to dial-up access to broadband access, and now many are offering wireless network access. Many airports and college campuses have wireless networks as well. It seems like every week someplace new pops up where you can surf the Web while you're out and about.

It is perilous enough jumping onto the Internet using your own network in the comfort of your home, but sharing an unknown network and not knowing if the network or the other computers are secure adds some new concerns. Some of the things you must do to use a public wireless network securely are just simple rules of computer security no matter what network you're connecting to, while others are unique to accessing a public wireless network.

Install Up-to-Date Antivirus Software

For starters, you should make sure you have antivirus software installed and that it is up-to-date. You don't know what, if any, protection the network perimeter offers against malware or exploits, or whether or not the other computers on the network with you are trying to propagate some malware. You also need to make sure that your operating system and applications are patched against known vulnerabilities to help protect you from attack. For details on protecting your computer from malware, see Chapter 3.

Install a Personal Firewall

Your computer should have personal firewall software installed. Again, you have no way of knowing offhand if the network you are joining is protected by any sort of firewall or perimeter security at all. Even if it is, you need the personal firewall to protect you not only from external attacks, but also from attacks that may come from the other computers sharing the network with you. For details on personal firewalls, see Chapter 5.

As a standard rule of computer security, you should make sure that your critical, confidential, and sensitive files are password protected. In the event that any attacker or casual hacker happens to infiltrate your computer system, it is even more impor-

134 Chapter 8 • Wireless Network Security

tant that you protect these files when joining a public wireless network. Make sure you restrict access to only the User Accounts that you want to access those files and use a strong password that won't be easily guessed or cracked.

Tools & Traps...**AirSnarf**

AirSnarf, a Linux-based program created to demonstrate inherent weaknesses in public wireless hotspots, can be used to trick users into giving up their usernames and passwords.

The AirSnarf program can interrupt wireless communications, forcing the computer to disconnect from the wireless network. Immediately following the service interruption, AirSnarf will broadcast a replica of the hotspot login page to lure the disconnected user to enter their username and password to reconnect.

The person sitting at the table next to you or sipping an iced latte in the parking lot could be running the program and it would be very difficult for you to realize what was going on. You should monitor your hotspot bill closely for excess usage or charges, and change your password frequently.

More importantly, it is vital that you disable file and folder sharing. This is even more critical if you happen to be using Windows XP Home edition because of the way Windows XP Home manages file and folder sharing and uses the Guest account with a blank password for default access to shared files and folders. Some attackers or malware may still find their way into your system, but that is no reason to leave the door unlocked and a big neon sign welcoming visitors.

Additional Hotspot Security Measures

All of the things I have mentioned so far are basic security measures that apply whether you are at home, at work, or connecting to a public wireless network while browsing books at Borders. Now let's take a look at some extra things you need to do or consider when connecting to a hotspot.

Verify Your Hotspot Connection

To begin with, you need to make sure you *are* connecting to a hotspot and not a malicious rogue access point. When you are connecting to a public wireless network,

it will broadcast the SSID, or network name, along with other information your wireless adapter needs to know in order to connect. It is very easy though for an attacker to set up a rogue access point and use the same or similar SSID as the hotspot. They can then create a replica of the hotspot login Web site to lure users into giving up their usernames and passwords or possibly even get credit card numbers and other such information from users who think they are registering for access on the real site.

You should make sure that the location you are at even has a hotspot to begin with. Don't think that just because you happen to be at a coffee shop and a wireless network is available that it must be a free wireless hotspot.

If you are at a confirmed hotspot location and more than one SSID appears for your wireless adapter to connect to, you need to make sure you connect to the right one. Some attackers will set up rogue access points with similar SSIDs to lure unsuspecting users into connecting and entering their login or credit card information.

Watch Your Back

Once you take care of ensuring that you are connecting with a legitimate wireless network, you need to take stock of who may be sitting around you. Before you start entering your username and password to connect to the wireless network or any other usernames and passwords for things like your e-mail, your online bank account, and so on, you want to make sure that no overly curious neighbors will be able to see what you are typing.

After you have determined that nobody can see over your shoulder to monitor your typing and you have established that you are in fact connecting to a legitimate public wireless network, you can begin to use the Internet and surf the Web. You should always be aware though of the fact that your data can very easily be intercepted. Not only can other computers sharing the network with you use packet sniffer programs such as Ethereal to capture and analyze your data, but because your data is flying through the air in all directions even a computer in a nearby parking lot may be able to catch your data using programs like NetStumbler or Kismet.

Use Encryption and Password Protection

To prevent sensitive data or files from being intercepted, you should encrypt or protect them in some way. Compression programs, such as WinZip, offer the ability to password-protect the compressed file, providing you with at least some level of protection. You could also use a program such as PGP to encrypt files for even more security.

136 Chapter 8 • Wireless Network Security

Password-protecting or encrypting individual files that you may want to send across the network or attach to an e-mail will protect those specific files, but they won't stop someone from using a packet sniffer to read everything else going back and forth on the airwaves from your computer. Even things such as passwords that obviously should be encrypted or protected in some way often are not. Someone who intercepts your data may be able to clearly read your password and other personal or sensitive information.

Don't Linger

One suggestion is to limit your activity while connected to a public wireless network. You should access only Web sites that have digital certificates and establish secure, encrypted connections using SSL (typically evidenced by the locked padlock icon and the URL beginning with "https:").

Use a VPN

For even greater security, you should use a VPN (virtual private network). By establishing a VPN connection with the computer or network on the other end, you create a secure tunnel between the two endpoints. All of the data within the tunnel is encrypted, and only the two ends of the VPN can read the information. If someone intercepts the packets midstream, all they will get is encrypted gibberish.

For SSL-based VPNs, just about any Web browser will do. However, a large percentage of the VPN technology in use relies on IPSec, which requires some form of client software on your computer to establish a connection. It is not important that the VPN software on your computer and that on the other end be the same or even from the same vendor, but it is a requirement that they use the same authentication protocol. Corporations that offer VPN access for their employees typically supply the client software, but you can also get VPN client software from Microsoft or from Boingo.

Use Web-Based E-mail

One final tip for using a public wireless network is to use Web-based e-mail. If you are connecting to a corporate network over an encrypted VPN connection and accessing a corporate mail server like Microsoft Exchange or Lotus Notes, you will be fine. But if you are using a POP3 e-mail account from your ISP or some other e-mail provider, the data is transmitted in clear text for anyone to intercept and read. Web-based e-mail generally uses an encrypted SSL connection to protect your data in transit, and major Web-based mail providers such as Hotmail and Yahoo also scan e-mail file attachments for malware. For details on Web-based e-mail, see Chapter 6.

Summary

Wireless networks represent one of the greatest advances in networking in recent years, particularly for home users who want to share their Internet connection without having to run network cabling through the floors and walls. Unfortunately, if not properly secured, wireless networks also represent one of the biggest security risks in recent years.

In this chapter, you learned about the basic concepts of wireless networking and the key features of the main wireless protocols currently being used. We also covered some fundamental steps you need to do to protect your wireless network, such as changing default passwords and SSIDs, disabling the broadcasting of your SSID, or even filtering access to your wireless network by MAC address.

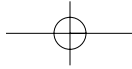
This chapter also discussed the strengths and weaknesses of the wireless encryption schemes such as WEP and WPA, and why you should ensure that your wireless data is encrypted in some way. You also learned that a layered defense, including components such as a personal firewall and updated antivirus software, is a key component of overall security, particularly when using public wireless hotspots.

The chapter ended by discussing some other security concerns that are unique to public wireless hotspots, such as ensuring that the wireless network you are connecting to is a legitimate one and not a rogue hotspot set up to steal your information. In addition, you learned that using a VPN for communications and utilizing Web-based e-mail can help improve your security and protect your information while using public wireless networks.

Additional Resources

The following resources provide more information on wireless network security:

- Bowman, Barb. *How to Secure Your Wireless Home Network with Windows XP*. Microsoft.com
(www.microsoft.com/windowsxp/using/networking/learnmore/bowman_05february10.msp).
- Bradley, Tony, and Becky Waring. *Complete Guide to Wi-Fi Security*. Jiwire.com, September 20, 2005 (www.jiwire.com/wi-fi-security-traveler-hotspot-1.htm).
- Elliott, Christopher. *Wi-Fi Unplugged: A Buyer's Guide for Small Businesses*. Microsoft.com
(www.microsoft.com/smallbusiness/resources/technology/broadband_mobility/wifi_unplugged_a_buyers_guide_for_small_businesses.msp).



138 Chapter 8 • Wireless Network Security

- *PGP Encryption Software* (www.pgp.com/).
- *Wi-Fi Protected Access 2 (WPA2) Overview*. Microsoft TechNet, May 6, 2005 (www.microsoft.com/technet/community/columns/cableguy/cg0505.mspx).
- *WinZip Compression Software* (www.winzip.com/).

