Chapter 1: Wi-Fi Hotspots, Hot Zones, and Cities

In This Chapter

- **Untangling the public Wi-Fi types — Wi-Fi hotspots, hot zones, and muni wireless networks**
- **Equipping yourself to search for public wireless Internet**
- **Connecting to public Wi-Fi networks**
- **Securing your Wi-Fi communications**
- **Getting past the e-mail block on Wi-Fi hotspots**

Your home network is not the only place where you can access the Internet. These days, you have a dazzling array of places to choose from — hundreds of thousands of Wi-Fi hotspots, hot zones, and municipal networks — to connect to the Internet with your laptop and other mobile devices. These Wi-Fi locations throughout the world can serve as an extension of your home network, connecting you to the digital world when you're away from home.

In this chapter, you discover exactly what types of public networks are out there, how to find and connect to them, and how to stay secure.

Understanding Wi-Fi Hotspots and Hot Zones

Wi-Fi hotspots are locations or areas with wireless Internet access that is *intended for public use,* usually within a single building. In a hotspot or hot zone, Internet access may be provided either for free or for a fee. You can find Wi-Fi hotspots at just about any location where you might pop open your laptop or pull out your PDA, VoIP phone, or other mobile device that makes use of the Internet, including:

- Hotels, motels, timeshares, and vacation homes
- Airplanes and cruise ships
- Cafés, coffee shops, and restaurants

- Bookstores and libraries
- Airports and train and bus stations
- Shopping centers and shipping and mailing stores

When wireless Internet access covers larger areas, such as a few city blocks or a collection of buildings, it's referred to as a *Wi-Fi hot zone*. This type of network, such as what you find on a college or company campus, can support access for hundreds or thousands of users.

Even larger Wi-Fi networks exist that offer wireless Internet access to hundreds of thousands of users (or even more than a million). These networks are called municipal (*muni* for short) or Metro-scale networks, and in the past several years, cities and counties (and even some small countries!) have set up wireless networks to support the Internet needs of their residents, businesses, travelers, and government departments.

Though all the public Wi-Fi location types are discussed in this chapter, in many areas you'll see that the text refers only to hotspots, but in many cases this applies to all public network types, Wi-Fi hot zones, and municipal wireless networks as well. The way you go about finding the different types of Wi-Fi locations varies, but the way you connect with, use, and secure each type is pretty much the same across the board.

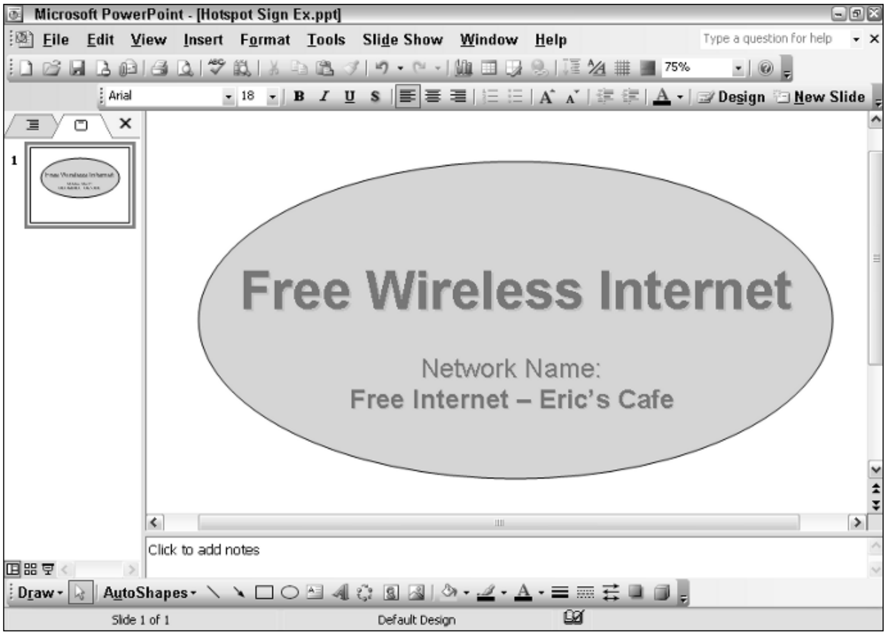
Finding Wi-Fi Hotspots

These days, most major brands or chains of hotels, restaurants, and stores offer some type of wireless Internet access. Even some mom-and-pop stores are getting techy and setting up hotspots. When it comes to figuring out whether a certain place offers wireless Internet or searching for locations, you have many available options and techniques.

Keep your eye out for signs

When you're out and about, the best thing to do when trying to find a Wi-Fi hotspot is just open your eyes. Most places that offer this access let you know with signage. You may find a decal, for example (see Figure 1-1) on the doors or windows of the location.

You may also see signs or tent cards displayed within the establishment. These signs may say something like “Wi-Fi Hotspot,” “Wi-Fi Here,” or “Wireless Internet.”



Free Wireless Internet

Network Name:
Free Internet – Eric's Cafe

Figure 1-1: Example of a "Wi-Fi here" sign.

Check online from your home computer or while on the go

If you need to plan where you can get Internet access before you leave home, or if you can't find a hotspot location on foot, you can always turn to the computer and search the following:

- **Online directories:** When you have access to the Internet, you can check online directories of hotspots on Web sites, such as

  `www.jiwire.com`

  `www.wi-fihotspotlist.com`

  `www.wifinder.com`

  `www.hotspot-locations.com`

- **Downloadable directories:** If you plan on using Wi-Fi hotspots often, you might want to download hotspot directories to your computer. That way, if you get nervous because you can't find a hotspot when you're out in the world, away from your usual Internet access, you can just pop open your laptop to find the nearest hotspot location. Check out the following Web sites (or hotspot directories) that offer downloadable software directories:

`www.jiwire.com`

`www.boingo.com`

`http://hotspot.t-mobile.com`

- **Mapping software and Web sites:** Another way to find Wi-Fi hotspots is through mapping software and Web sites, such as Yahoo Maps (`http://maps.yahoo.com`) and Google Maps (`http://maps.google.com`). Though this type of software shouldn't be your only source, you can usually use the search function of mapping applications (just search using the keyword "hotspot") to find hotspots near the location you're zoomed in on. This is a great (and timesaving) way to take a quick look for hotspots when getting maps or directions.

Check your network list

When trying to locate a hotspot, you can always just turn on your laptop or mobile device and see what nearby wireless networks show up on your list of available networks (which you find by accessing your network icon). Look for unsecured or unencrypted networks. Keep in mind, though, that you might see some private networks left unsecured, which you should leave alone because connecting to them is illegal. Sometimes it's difficult to differentiate these from networks intended as public hotspots; however, here are a few tips that can help you verify them:

- **Look:** Check for signs in the establishment.
- **Ask:** Ask the staff or property owners whether wireless Internet access is available there.
- **Assume:** If neither of the preceding suggestions works out, you're probably safe in assuming that a wireless network named after an establishment or company that is left unsecured is a public hotspot.

Use Wi-Fi finders

If you regularly use Wi-Fi hotspots, a Wi-Fi finder (Figure 1-2 shows an example) might be something you can really use. You can carry the gum-pack–sized device around in your pocket. When you want to check what wireless networks are around, you can pull out the device and see information about nearby networks on the small LCD screen. You see information on each network, such as signal strength, network name, and security status. This is usually enough information to differentiate a hotspot from a public network.

You can even get combination devices, such as USB wireless adapters with built-in Wi-Fi finders. See Book VI, Chapter 3 for more information.

Figure 1-2: Use a Wi-Fi finder to locate nearby wireless networks.

Courtesy of Cisco Systems, Inc.

Sign up for reliable access

If you are a frequent traveler or hotspot user and are willing to pay for access, you should look into signing up with a Wi-Fi hotspot provider. Having this resource gives you better chances of finding reliable hotspots throughout the United States and abroad. As you may have found out already, finding free hotspots isn't always easy and can be frustrating.

Rather than pay per hotspot session or per day, you can get monthly subscriptions for as low as $20 per month that you can use with more than 100,000 locations. Plus, you won't have to search for free hotspots anymore. Before you leave home, you can see exactly where wireless networks exist in the areas you're traveling through and around your destination.

Two popular hotspot providers are Boingo (`www.boingo.com`) and T-Mobile (`http://hotspot.t-mobile.com`).

Finding Municipal Networks

You can use the same searching techniques for municipal Wi-Fi networks as those for traditional Wi-Fi hotspots (discussed in the previous section), plus the techniques described next.

Local media outlets

Check the Web sites of local newspapers and news stations and search the news or IT (Information Technology) section of the city or county Web site.

Online news sites

Browse through online Web sites that cover municipal Wi-Fi topics, such as the following:

- `www.muniwireless.com`: In particular, the list of U.S. cities and counties available in the resources section
- `www.wifinetnews.com`: In particular, the Metro-Scale Networks category

Connecting to Wi-Fi Hotspots

Using Wi-Fi hotspots is similar to using your wireless network at home; however, you should understand a few important differences, discussed throughout this section.

When you find a Wi-Fi hotspot, connecting is similar to what you do with your home network. Here are the basic steps:

1. **Connect to the Network.**

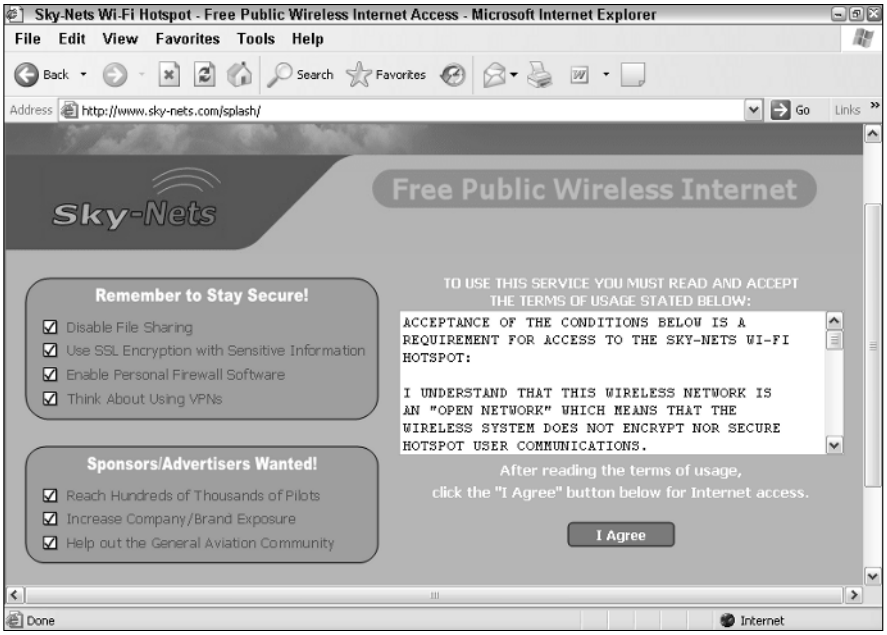
   Choose the network name from your list of available wireless networks and click Connect or OK. For step-by-step directions, refer to Book IV, Chapter 1.

2. **Open your Web browser.**

   If your regular home page shows up, you're probably done and can start using the Internet as you want. However, most hotspots have a splash or portal page, which automatically comes up instead of your home page; this feature is called *captive portal.* Figure 1-3 shows an example.

3. **Accept terms, make payment, or both.**

   If a splash screen does appear, it usually displays the terms of service or rules of using the hotspot, or maybe shows just a portal page with advertisements. After reviewing the page, you should know whether you can access the Internet for free or have to pay for it first. Follow the directions given and, if necessary, accept the terms and make payment to proceed.


Sky-Nets Wi-Fi Hotspot - Free Public Wireless Internet Access - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.sky-nets.com/splash/
Go
Links
Sky-Nets
Free Public Wireless Internet
I Agree
Done
Internet

Remember to Stay Secure!

- ☑ Disable File Sharing
- ☑ Use SSL Encryption with Sensitive Information
- ☑ Enable Personal Firewall Software
- ☑ Think About Using VPNs

Sponsors/Advertisers Wanted!

- ☑ Reach Hundreds of Thousands of Pilots
- ☑ Increase Company/Brand Exposure
- ☑ Help out the General Aviation Community

TO USE THIS SERVICE YOU MUST READ AND ACCEPT THE TERMS OF USAGE STATED BELOW:

ACCEPTANCE OF THE CONDITIONS BELOW IS A REQUIREMENT FOR ACCESS TO THE SKY-NETS WI-FI HOTSPOT:

I UNDERSTAND THAT THIS WIRELESS NETWORK IS AN "OPEN NETWORK" WHICH MEANS THAT THE WIRELESS SYSTEM DOES NOT ENCRYPT NOR SECURE HOTSPOT USER COMMUNICATIONS.

After reading the terms of usage, click the "I Agree" button below for Internet access.

Figure 1-3: A hotspot splash page opens instead of your home page.

Securing Your Hotspot Connections

Using a Wi-Fi hotspot poses risks similar to using your wireless home network without encryption, as discussed in Book III, Chapter 2. Wi-Fi eavesdroppers can capture the Web sites you visit and the login information you use for unsecured (non-SSL) Web sites and services (including POP3 e-mail accounts). Furthermore, any files or folders you have shared may be accessible to the other hotspot users.

What's an "SSL" Web site, you're wondering? SSL stands for *Secure Socket Layer* (also sometimes seen as *Secure Sockets Layer*), which is an encryption standard for securing Web pages.

Securing your real-time traffic

Real-time traffic consists of the Web sites you visit, login information, and any other content or data transferred to and from your computer and the public network. To secure your real-time traffic, you should follow a few safety measures:

Use a virtual private network (VPN) connection

A virtual private network, or VPN, is a technique to securely connect remote computers. A VPN network can consist of computers around the world, connected via the Internet, with all the traffic being encrypted and extremely secure from one computer to another. VPNs traditionally are used within businesses to allow employees to access their work files when away from the office.

You can also use VPN technology to secure your hotspot traffic. This method can provide even better encryption and security than what you get on your wireless home network using WPA or WEP. Here are a few ways to use VPNs to make your hotspot connections secure:

Use a company-provided VPN

If your work involves regular computer usage, you should inquire with your boss or the company IT or tech team about any available VPN access and the procedures and rules related to its use. Even though you may not always want to access your work files, you can connect to and use the VPN connection to secure your real-time traffic from people at the hotspot locations.

Use hosted hotspot access or software

You may want to consider using hosted hotspot security solutions that make use of VPN or SSL technology, such as the following:

- **AnchorFree Hotspot Shield (**`www.anchorfree.com/hotspot-shield/`**):** Free
- **JiWire Hotspot Helper (**`www.jiwire.com/hotspot-helper.htm`**):** Free trial, then around $25 per year
- **WiTopia's personalVPN (**`www.witopia.net`**):** Around $40 per year

What to do if you don't use a VPN connection

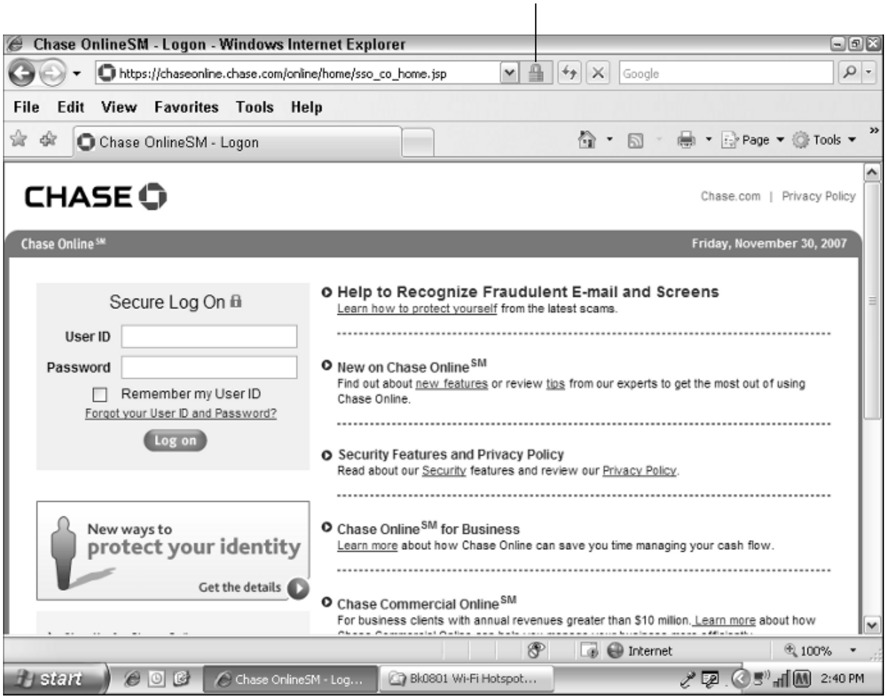
If you don't use a VPN (or SSL) connection to encrypt all your real-time traffic while you're on a hotspot, you should at least follow a few minimal security measures, as follows:

- **Secure any services used:** Make sure any Internet services you use, such as POP3 e-mail and FTP for file transfers, are secured. Some e-mail hosts provide SSL encryption for e-mail accounts, which you have to set up in your e-mail client. If not, most e-mail providers do offer secure access to accounts through a Web site.

- **Use SSL (or HTTPS) Web sites:** Don’t log in to accounts or services that require you to use a username and password, unless they’re secured with SSL (see earlier in this section for an explanation of SSL) and use an HTTPS address (note the *S* at the end of *HTTP*) — for example, `https://www.website.com`. Most Web browsers also display a padlock icon when a Web site is using SSL. Figure 1-4 shows an example of the padlock in Internet Explorer 7. Previous versions of Internet Explorer and other Web browsers, however, display their padlocks in the lower-right corner of the browser window.

  This technology encrypts the communications between your computer and the particular Web site. You can still visit unsecured (or non-SSL) Web sites; however, when you do so, all the Web page’s contents can be captured and viewed by others. This should be fine when you’re visiting nonsensitive Web sites.

Padlock icon



Chase OnlineSM - Logon - Windows Internet Explorer

https://chaseonline.chase.com/online/home/sso_co_home.jsp

Secure Log On

User ID □

Password □

□ Remember my User ID

Forgot your User ID and Password?

Help to Recognize Fraudulent E-mail and Screens
Learn how to protect yourself from the latest scams.

New on Chase Online^{SM}
Find out about new features or review tips from our experts to get the most out of using Chase Online.

Security Features and Privacy Policy
Read about our Security features and review our Privacy Policy.

Chase Online^{SM} for Business
Learn more about how Chase Online can save you time managing your cash flow.

Chase Commercial Online^{SM}
For business clients with annual revenues greater than $10 million. Learn more about how

Figure 1-4: SSL padlock indicator in Internet Explorer 7.

Protecting your computer

Depending upon the equipment used at particular hotspot locations, connecting to a hotspot can open your computer to being accessible to other hotspot users. For example, if you have set up folders to be shared, some hotspot solutions out there may not block user-to-user communication, making your shared files accessible to other hotspot users, just as they are for your home network. Regardless of the hotspot solution you use, you can safeguard your computer and personal documents in the following ways:

- **Disable sharing:** Before connecting to a Wi-Fi hotspot, you should disable the sharing of any files, folders, and services that you may not want others to view, use, or edit. Refer to Book IV, Chapter 3 for step-by-step directions on checking for and disabling shared resources. Turning off sharing while you're away from home and then reactivating it for your home network is easy, after you get the hang of it, so I urge you to get in the habit of doing it. It's an important aspect of safeguarding your computer.
- **Use personal firewall software:** When connecting to hotspots — and even your home network — you should use personal firewall software. This software helps protect you from Internet intruders and hackers. Windows XP and Vista have built-in firewall utilities, accessible via the Control Panel. Or, if you prefer, you can use a third-party firewall application, such as ZoneAlarm (`www.zonealarm.com`) or whatever is included with your antivirus software. (You *do* keep a regularly updated antivirus application running, right?)
- **Keep your OS up-to-date:** Make sure that your operating system (Windows, Mac, or any other) is up-to-date at all times so that you're receiving patches for security holes and fixes for known issues. See Book II, Chapter 5 for information on how to update your operating system.

Watching out for fake hotspots

A technique used by some techy criminals is to set up a fake hotspot — sometimes referred to as an "evil-twin hotspot" — copying the look and feel of a real hotspot, and maybe even a specific hotspot provider's brand. The intention is for people to connect to the hotspot and make a payment so that the criminals can capture the users' credit card and personal information. This is known as a "man-in-the-middle" attack.

You may find spotting these fakes difficult, but you do have several ways to check the legitimacy of a hotspot, as follows:

- **Make sure that payment pages are secure:** If the hotspot requires payment, the pages where you make payment and log in should be protected with SSL encryption; otherwise, you may be on a fake hotspot. A properly secured Web page should use an HTTPS address (the *S* at the end signifies that it's a secure site), and a padlock icon should be displayed in your Web browser. For examples, see Figure 1-4, shown previously.
- **Check the SSL certificate:** If the hotspot does require payment and its payment and login pages are secured with SSL, look at the SSL certificate details. You may find some clues as to the legitimacy of the hotspot. If the certificate contains any errors or problems, you shouldn't use the hotspot. In Internet Explorer, you can check the SSL certificate details by double-clicking the padlock icon that appears on the right of the Address bar or in the lower-right corner of the browser.
- **Check for signage:** If you are suspicious of a hotspot, you can check for signs or with the staff at the location to see whether the establishment even has a hotspot.

Sending E-Mail on Hotspots

If you use POP3 e-mail accounts, you may find that some Wi-Fi hotspots — and even some ISPs, such as your home Internet connection — block the outgoing port(s) so that you can't send any e-mail through your POP3 e-mail server. This is a security measure put in place by the hotspot owner so that the owner's Internet connections aren't used to send spam messages. You have a few ways to get around this security feature:

- **Use Web-based e-mail:** Use a different account that's Web-based, or find out whether your POP3 account provider offers Web-based access (that's secured by SSL, of course).
- **Use a redirector:** You can use an SMTP port relay or redirector, such as the one offered by the JiWire Hotspot Helper (`www.jiwire.com/hotspot-helper.htm`).
- **Try another port:** You may have success with other outgoing e-mail ports, such as 2525 or 587, in place of the usual port 25. For help on making these changes, you can refer to the documentation and Help files of your e-mail client application or your POP3 account provider.