7 tips for working securely from wireless hotspots

Wireless hotspots are changing the way people work. These wireless local area networks (LANs) provide high speed Internet access in public locations—as well as at home—and require nothing more than a notebook PC with a wireless card. From coffeeshops to restaurants, airports to hotel lobbies, hotspots are ubiquitous. They are the de facto connection method for travelers and remote workers to access the Internet, their e-mail, and even their corporate networks.

Hotspots range from paid services, such as T-Mobile or Boingo, to free connections at your local coffee shop or library. But they all have one thing in common: These are all open networks that are vulnerable to security breaches. And that means it's up to you to protect the data on your PC. Here are a few tips to make working in public locations more secure.

1. **Try to choose more secure connections.** It's not always possible to choose your connection type—but when you can, opt for wireless networks that require a network security key or have some other form of security, such as a certificate. The information sent over these networks is encrypted, which can help protect your computer from unauthorized access. The security features of different networks appear along with the network name as your PC discovers them.

2. **Make sure your firewall is activated.** A firewall helps protect your mobile PC by preventing unauthorized users from gaining access to your computer through the Internet or a network. It acts as a barrier that checks all incoming information, and then either blocks the information or allows it to come through. All Microsoft Windows operating systems come with a firewall, and you can make sure it's turned on.

    1. Click **Start**, and then click **Control Panel**.
    2. In **Control Panel**, double-click **Network Connections**.
    3. In the **Network Connections** window, under **Network Tasks**, click **Change Windows Firewall Settings**.
    4. In the **Windows Firewall** dialog box, on the **General** tab, ensure that **On** is selected.

    To activate the Windows Vista Firewall

    1. Click **Start** and then click **Control Panel**.
    2. In **Control Panel**, select **Network and Internet**.
    3. Under **Windows Firewall**, click **Turn Windows Firewall on or off**.
    4. Ensure that **On** is selected.

3. **Monitor your access points.** Chances are, there are multiple wireless networks anywhere you're trying to connect. These connections are all access points, because they link into the wired system that gives you Internet access. So how do you make sure you're connecting to the right one? Simple—by configuring your PC to let you approve access points before you connect.

Configure Windows XP Access Points

1. Click **Start**, and then click **Control Panel**.
2. In **Control Panel**, double-click **Network Connections**.
3. In the **Network Connections** window, right-click **Wireless Network Connection**, and then click **Properties**.
4. In the **Wireless Network Connection Properties** dialog box, on the **Wireless Networks** tab, make sure that the **Use Windows to configure my wireless network settings** check box is selected.
5. Under **Preferred networks**, make sure that the name of the network that you want to connect to is highlighted, and then click **Advanced**.
6. In the **Advanced** dialog box, click **Access point (infrastructure) network only**, and then click **Close**.
7. Click **OK**.

Configure Windows Vista Access Points

Windows Vista takes the guesswork out of connecting to hotspots because you are automatically prompted to approve new connections. In addition, after you approve a connection, you assign it a profile for future use.

4. **Disable file and printer sharing**: File and printer sharing is a feature that enables other computers on a network to access resources on your computer. When using your mobile PC in a hotspot, it's best to disable file and printer sharing because when enabled, it leaves your computer vulnerable to hackers. Remember, though, to turn this feature back on when you return to the office.

Disable file and printer sharing in Windows XP

1. Click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **Security Center**.
3. In the **Security Center** window, click **Windows Firewall**.
4. In the **Windows Firewall** dialog box, click the **Exceptions** tab.

5. On the **Exceptions** tab, under **Programs and Services**, clear the **File and Printer Sharing** check box and then click **OK**.

Disable file and printer sharing in Windows Vista

1. Click **Start** and then click **Control Panel**.
2. In **Control Panel**, select **Network and Sharing Center**.
3. Under **Sharing and Discovery**, turn **File Sharing** and **Printer Sharing** to off.

5. **Make your folders private**. When the folders on your mobile PC are private, it's more difficult for hackers to access your files.

To make a folder private in Windows XP:

1. Click **Start**, and then click **My Computer**.
2. In the **My Computer** window, double click the drive where Windows is installed, and then double click **Documents and Settings**.
3. Double click your user folder, right-click the folder that you want to make private, and then click **Properties**.
4. In the **Properties** dialog box, on the **Sharing** tab, click **Do no share this folder**, and then click **OK**. Repeat the steps above for each folder that you want to make private.

To make a folder private in Windows Vista

Windows Vista not only makes folders private by default, but it also requires passwords for shared folders. As a result, you're already covered! But if you want to double check, simply right click on the folder in question, and select **Properties**. On the **Security** tab, you can review the set permissions.

6. **Encrypt your files**. You can protect your files further by encrypting them, which requires a password to open or modify them. Because you must perform this procedure on one file at a time, consider password-protecting only the files that you plan to use while working in a public place.

- Encrypt files using Windows XP.
- Encrypt files using Windows Vista.

7. **Consider completely removing sensitive data from your notebook PC.** If you're working with extremely sensitive data, it might be worth taking it off your notebook PC altogether. Instead, keep it behind the corporate firewall and use your company's VPN to access it when necessary. This way, you have multiple safeguards in place.

A few simple precautions can help make working in public places more secure. And by selecting the best connections and adjusting settings, you can enjoy productive and safe work sessions no matter where you are.