WHITE PAPER

A Manager’s Guide To Wireless Hotspots — How To Take Advantage Of Them While Protecting The Security Of Your Corporate Network

This paper discusses the security risks inherent in public Wi-Fi Internet access and the best ways to mitigate these risks. It also discusses the benefits of hosting a corporate hotspot of your own.

Introduction

In urban environments, wireless Internet access is an easy find for anyone with a notebook or handheld computer that supports the wireless LAN protocol known as Wi-Fi. The term "hotspot" has become a part of the public lexicon, referring to a place where a user can connect to a public Wi-Fi network. There are more than 150,000 Wi-Fi hotspots worldwide today. Some of these, namely municipal hotspots, span entire cities.

In coffee shops, hotels, airport terminals and libraries, public Wi-Fi hotspots are increasingly becoming commonplace. Hotspots are convenient, but there are safety risks that come with using them. Some are safer than others, and they should be used cautiously.

Know the risks:

There are a few obvious security risks for the Wi-Fi public hotspot user:

1. **Lack of encryption:** While not officially in an attempt to be both public and easy to use, many hotspots forgo data encryption protocols such as WEP (wired equivalent privacy), 802.11i, or WPA (Wi-Fi Protected Access.) This makes it especially easy for others to eavesdrop on a session, and so it's up to the user to employ smart security practices. (See basic rules, below.)

2. **The evil twin:** There are a variety of tools that can be used to eavesdrop on an unsecured network session. One of the most nefarious of these has a name to match: the evil twin. An evil twin is a wireless network signal that masquerades as a legitimate hotspot for the purpose of stealing information from the user, such as a network password or a credit card number. With a little software and some ingenuity, a thief can make a device with a wireless signal look just like an access point to the unsuspecting computer.

3. **Malware:** On the road, a computer can be subject to viruses, worms, and spyware.

Basic rules for business travelers who want to use hotspots:

The majority of corporate enterprises use Microsoft Windows®, so this paper assumes a Windows environment. Windows 2000 and XP are set up by default to encourage information sharing, and sharing information is the last thing you want to do at a public hotspot.

To that end, you'll want to change the default settings to secure your employees' computers. "IT needs to enforce and assure compliance with appropriate policies," says Craig Mathias, principal analyst at the Farpoint Group, a wireless industry consultancy in Massachusetts.

That said, it's a good idea to teach the following rules to roving employees, so they understand how to help keep their computers from becoming attack magnets at hotspots.

1. **Turn off ad-hoc networking features.** Default settings in Microsoft Windows allow a notebook computer running Windows to look for any available wireless networks – including peer-to-peer networks. It takes several steps to undo this, and employees probably won't bother to do so. Because you'll want to prevent the sharing of corporate information with strangers in a coffee shop, you should insist that your employees disable the ad-hoc networking feature in Windows before they use a public hotspot.

   Here's how to do it: In the **Network Connections** menu, click the "Wireless Network Connection" icon. Click the icon that says "change the settings of this connection." When the Windows Network Connection Properties window opens, click the tab that says "Wireless Networks." In that tab, click "Advanced." In the "Advanced" window, click "Access point (infrastructure) networks only." Voila.

2. **Turn off file sharing, too.** Again, Microsoft Windows is a friendly program. It's set by default to enable its users to share files with strangers. You'll want employees to turn that feature off before they hit the road. On the **Start** menu, select **Settings** and then **Network Connections**. Find the Internet connection and right-click to select **Properties**. Under the **General** tab, you'll likely see a check mark next to **File and Printer Sharing for Microsoft Networks**. Uncheck it!

3. **Encrypt any folder that contains sensitive data.** Securing that data that resides on a device is a safety issue any time that device leaves the office — hotspot or not. Employees may be lax about encrypting the contents of their computers, but they need to know that sensitive data means more than financial information and social security numbers. Explain that "sensitive data" includes that folder in which they store all their network passwords, in giant font on a Microsoft Word document, for all the world to see. (Odds are good that they have created such a thing.)

   Although labeled as an "advanced" function in Windows, encrypting a folder is pretty easy. Right-click on that folder to select **Properties**. Under the **General** tab, click **Advanced**, and then click **Encrypt contents to secure data**.

   Employees should also make sure nobody's looking over their shoulders at hotspots. Thieves can steal passwords just by watching someone type those passwords.

4. **Use a VPN!** A virtual private network creates a tunnel between the employee's computer and the corporate network. Your corporation probably has a policy requiring the use of VPN software for remote access to the corporate server. If such a policy doesn't exist, it should. A VPN virtually guarantees that nobody can intercept sensitive information on your company's server. Most commercial hotspot providers support VPNs. Public libraries often do not. (Make sure employees have VPN clients installed on their notebooks before they hit the road. Nothing garners an angry phone call to the IT department like a VPN client that doesn't work!)

5. **Run a firewall.** With a wireless hotspot, a group of strangers are sharing the same IP subnet Odds are that most of these strangers have no ill intentions, but they might unknowingly have malware or viruses on their computers. Thus, they might unknowingly infect the computers of those around them. Installing (and running) firewall software will help to prevent successful attacks from both on and off the subnet. A firewall should block attacks and send an alert when it detects any unwanted attempts to connect to your employee's computer. Microsoft Windows XP comes with a firewall, but it's up to the user to turn it on.

6. **Run antivirus software.** Should a virus get through, antivirus software will detect and thwart it - provided the software recognizes the virus. New viruses are created daily. For that reason, most antivirus software companies provide frequent updates to their software. It's up to the user to go to the vendor's Web site to obtain the updates. This should be done at least once a week.

7. **Keep the computer up to date with the latest operating system patches.** Microsoft regularly sends out patches to fix problems — including security problems — in the Windows operating system. The system alerts users to new patches with a little explanation point in the right-hand corner of the screen. Installing these patches is generally a matter of just clicking on that exclamation point.

8. **Make sure the device is connecting to the correct network.** Employees using a hotspot should make sure that their notebooks or handheld computers actually are actually connecting to the hotspot — and not to some other Wi-Fi network. In urban areas, chances are good that there are several wireless networks within range. Some of these may be from nearby apartment buildings — residential networks that their owners didn't bother to secure. And some of them may be malicious rogues that are set up to steal private data. Tell your employees to be careful to choose the correct SSID from the list of available net works when signing on to a public hotspot. "Fluffykitty123" most likely isn't the commercial hotspot provider. A network

named for a hardware manufacturer is probably indicative of someone who was too lazy not only to secure the network, but too lazy to name it; but it also could be a trick. It's a good idea to ask an official employee for the right SSID. Hotels always should have this information on hand, and the barista in the coffee shop is probably more tech-savvy than he looks. Piggybacking on an unsecured residential network for free is easier than signing up for an official hotspot, but it's not worth the risks.

Once connected, most commercial hotspots will take you to a dedicated Web page for authentication and/or billing. Tell your employees to watch for "https…" in the Web address or a logo that looks like a gold lock in the right-hand corner of the page. This means the browser is using SSL for server-side authentication, which is a good thing. If the connection doesn't include a log-in page, it's likely that the computer is connected to the wrong network. If you're at a hotspot that charges a usage fee, you probably want to avoid entering your credit card information into a site that does not employ SSL.

In fact, if your employees are conducting any sensitive business transactions via the Web, they should try to use only Web sites that employ SSL.

There's always the chance, however, that there is an "evil twin" lurking about, masquerading as the official hotspot network. Adhering to rules 1-4 should help lessen this chance.

9. **Turn off the radio when you don't need it.** Disabling ad-hoc networking should prevent a computer from connecting to wireless networks indiscriminately. But disabling the radio will guarantee it. In Windows, you can do this simply by right-clicking on the wireless network icon in the right-hand corner of your screen. Click disable.

Basic rules for business travelers who want to use hotspots:

Nobody wants to think of employees as intruders, but they can be an unintentional threat to the network. Alas, there's always the chance that your employees have left their wireless radios on when they return to the office and plug back into the corporate network. If devices start finding Wi-Fi networks that reside outside the office walls, they could threaten the corporate network, forming a bridge between the outside wireless network and the corporate wired network. This can be a problem even if the corporation adheres to wireless LAN security protocols such as 802.11i, which addresses wireless authentication. "802.11i only secures a tiny portion of the value chain," says Farpoint's Mathias.

Furthermore, even if the employee's device's radio is turned off, there's a chance that the device was infected with spyware. If devices have been infected with malware on the road, there's a chance they can infect the corporate network when they return. This is a serious problem that can cause major headaches for network administrators. In short, it means that viruses can be spread from the trusted side of the corporate firewall.

Separately, there's a possible threat from the onslaught of municipal Wi-Fi networks, which are, essentially, city-wide hotspots. If your corporation sits in a city with its own Wi-Fi network, then that network is in your air space.

One way to mitigate such threats is simply to keep track of them with an intrusion protection system. Motorola's **Wireless Intrusion Protection System** (Wireless IPS) is a server software sentry that alerts the IT manager to myriad wireless network menaces, including those caused by imprudent hotspot users.

Wireless IPS monitors the network for network intruders, including rogue access points, client devices, and ad hoc networks that may have made an automatic connection to an employee's computer. The software also detects wrong configurations and weak or missing encryption implementations. And it provides real-time detection of all rogue access points, unauthorized client devices, and ad-hoc networks. The software immediately alerts the IT managers of any problems, allowing them to terminate rogue device or ad-hoc network connections.

Setting up a hotspot in your own office. It makes sense!

Again, wireless hotspots are becoming prevalent enough that business travelers expect access to a wireless network, wherever they go. They expect it in airport terminals, they expect it in their hotels, they expect it while they're getting coffee, and they expect it when they visit your office. Wi-Fi is mature and prevalent enough that some of your clients may consider it practically a birthright. For both security and business reasons, it makes good sense to set up a wireless hotspot in your office lobby.

Setting up a guest hotspot for your visitors does a couple of things. One, it helps you to be a hospitable host. Two, it protects you. You may not know these guests very well, and you may not know whether they are network spies. If your guests have their own wireless network, or at least a separate SSID, then they won't insist on using your corporate network, and you can worry less about whether they pose security risks.

Most enterprise-level wireless LAN infrastructures include the ability to support multiple SSIDs from a single wireless LAN switch, meaning you can set aside one for guest access. Some include the ability to support VLANs (virtual, logically-independent networks), which means you can support guests without compromising the corporate network. Guest users can be provisioned on a separate VLAN keeping them completely isolated.

Motorola's RFS7000, WS5100 and WS2000 wireless switch and the AP-5131 Access Point support multiple SSIDs and multiple VLANs.

Motorola provides the ability to make a guest network look and feel like a commercial hotspot. It makes a guest network easier to manage, too.

The latest version of the WS5100 switch includes a feature that will redirect a guest user to an official log-in page immediately after the user opens a Web browser — much like a commercial hotspot, except you will probably not charge your guests for access. The IT administrator has the ability to customize the log-in page. Your front desk administrator then easily can provision guest users on the wireless network and even set time limits for network access. The switch also includes integrated authentication features designed for guest access.

The WS5100 switch can be set up to receive all the guest user information automatically, keeping track of log-in times and any odd usage behavior.

In Summary

With some 150,000 hotspots blanketing airspace all over the world, your employees have the luxury of easy access to the corporate network, wherever they may roam. But it's important to make sure they do so without compromising the personal data or the corporate network.

For more information about Motorola's RFS7000, WS5100 and WS2000 Wireless Switches, AP-5131 Access Point, or Wireless Intrusion Protection System visit www.motorola.com/enterprisewlan.

MOTOROLA

motorola.com