Working Wirelessly

First and foremost, what is WiFi? WiFi stands for Wireless, or WiFi, technology is another way of connecting your computer to the network using radio frequency and no network cables.

Wireless works similarly to cordless phones; they transmit data from one point to another through radio signals. But wireless technology also requires that you be within the wireless network range area to be able to connect your computer. There are three different types of wireless networks:

- **Wireless Local Area Network (WLAN)**: WLAN are wireless networks that use radio waves. The backbone network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network. The range of a WLAN can be anywhere from a single room to an entire campus
- **Wireless Personal Area Network (WPAN)**: WPANs are short-range networks that use Bluetooth technology. They are commonly used to interconnect compatible devices near a central location, such as a desk. A WPAN has a typical range of about 30 feet.
- **Wireless Wide Area Networks (WWAN)**: WWANs are created through the use of mobile phone signals typically provided and maintained by specific mobile phone (cellular) service providers. WWANs can provide a way to stay connected even when away from other forms of network access. Also, be aware that additional charges are often associated with the usage of WWANs in some locations.

Working wirelessly can offer you the following benefits.

- **Flexibility:** The lack of cables that comes with wireless networking enables you to roam with your mobile PC. You can roam from your office to a nearby conference room for a meeting, or from the couch in the living room to a kitchen for a snack. For example, if you're working wirelessly in a meeting you can printout a report for a co-worker without having to leave the meeting.
- **Time-saving:** If you're waiting for an important response you can use your mobile PC to monitor your e-mail even when you're in meetings or at lunch. As soon as you get the data needed, you can promptly forward it to your customer rather than wondering whether the information has come in while you were away and having to run back to your office between meetings and other commitments.
- **Increased productivity:** Working wirelessly enables you to turn down times between meetings or while in transit into productive time. For example, you may be attending a conference and just found out that one of the sessions you were planning on attending has been cancelled. Rather than waste the next hour, you can check e-mail, start compiling your trip report, or order your son's birthday present.
- **Easier collaboration:** Using wireless mobile PCs, you can easily share files and information with others. For example, you can collaborate on a presentation with

colleagues during a flight delay in an airport lounge, or you can share the syllabus of a course while attendees so that they can take more digitally during the class.

What Should I Worry about when Working Wirelessly?

When working wirelessly from hotspots and public places, you are responsible for ensuring the security of your files and your mobile PC.

To make network access easier for their users, public hotspots typically leave all security turned off. This means that any information you send from a hotspot is most likely unencrypted, and anyone within range of the wireless LAN—whether at a next table or in the parking lot—can access and use your Internet connection, and look at your unprotected information.

WiFi gives you the freedom to go anywhere and still be connected to your office, your family, and other important aspects of your life. Your virtual office can now be an ice cream parlor in a seaside resort. Embrace and enjoy the flexibility that WiFi affords you.

Stay Secure When Using Your Mobile PC in Public Hotspots

Hotspots in public places usually don't provide any type of security. It's your responsibility to take the necessary precautions to ensure a safe connection to your corporate network or to the Internet. Here are some steps you can take.

- **Install a firewall**. 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 any information coming from the Internet or a network, and then either blocks the information or allows it to pass through to your computer. Microsoft Windows XP includes a firewall that you simply need to turn on. If you're running Microsoft Windows XP Service Pack 2, Windows Firewall is turned on by default for all network and Internet connections. To turn on Windows Firewall, visit http://support.microsoft.com/?kbid=283673.
- **Password-protect your files**. You can protect your files further by requiring 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.
- **Turn off wireless when you are not using it**. When you're using your mobile PC in a public place but you are not connected to a wireless network, you should turn off your wireless device. You can either remove your Wi-Fi card or press the manual hardware button on your computer if you're using a Centrino-based mobile PC. In addition to protecting your computer from hackers, turning off wireless when you don't need it helps save battery power.

By selecting the best connection method for your needs and by being aware of security pitfalls when working in public places, you can enjoy productive and safe work sessions remotely.

For additional tips for working at home visit Lisa Shea at http://www.lisashea.com/workfromhome/