

**INFORMATION TECHNOLOGY MANAGEMENT COMMITTEE  
LIVINGSTON, NJ  
WWW.LIVINGSTONNJ.ORG**

**ITMC TECH TIP  
ROB COONCE, MARCH 2008**

**What is wireless technology?**

In our world today, this may mean sitting down at a coffee shop, an airport, or a hotel and connecting your laptop to a wireless Internet Hotspot. Maybe you use a wireless keyboard or mouse in your office...or maybe you use a wireless headset with your cell phone. It could also be as simple as using a portable phone or TV remote control. Wireless technology, simply defined, enables communication between one or more devices without a physical connection or a cable.

The benefits of wireless communications include portability, flexibility, scalability and rapid installation, (installation time can be reduced because wires are no longer needed).

Disadvantage of connecting to a wireless network include the possibility of slower transmission of data and additional security risks associated with the transmission.

**Frequently Asked Questions about Wireless Technology**

**How does the information pass from point A to point B without a wire?**

Through an airwave or a radio wave.

**What is a WLAN ?**

A **WLAN** is a **Wireless Local Area Network**. This is a group of computers and associated devices that communicate with each other wirelessly.

**What are the risks associated with conducting business with wireless technology?**

Some of the risks associated with the use of **WLANs** are similar to those of wired communications, however the greatest difference is that wireless technology passes information over the communications medium of an airwave, which is open to intruders. Since a physical connection to the network is not needed -- intruders only need to be within range of the wireless transmissions.

For example, in an Internet café or airport, this intruder could be a person sitting next to you or they may be out of your sight but not outside of the access point. Wireless networks in public places do not offer control over infrastructure safeguards – it is up to the mobile user to protect his or her data when accessing these public domains.

For our organization this risk could result in unauthorized users gaining access to our systems and information, which could lead to corruption of our data, consumption of valuable bandwidth, or degraded network performance. Intruders could even use our systems to launch attacks against other networks.

For personal use this risk could also result in the same unauthorized user gaining access to our personal computer systems and all of the information that is stored or used on them.

### **What is a wireless hot spot?**

A **WLAN (Wireless Local Area Network)** that provides an Internet connection from a location.

### **How can I use a wireless hotspot securely for personal use?**

- **Disable File Sharing.** Use the Windows Help function to guide you through this process.
- **Install a Personal Firewall.** Make sure that personal firewall software is installed and kept updated.
- **Disable Wireless Network connections** when not in use.
- **Use wireless hotspot providers that provide secure encrypted connections.**
- **Avoid sending sensitive information**

**For more information on WIFI hotspot security ->**

<http://spotlight.getnetwise.org/wireless/wifitips/>

**Would you take the risk of passing your personal information over an open airwave for anyone interested to see it?**

In this advisory we have highlighted the basic idea of wireless technology and some of risks associated with using this technology in the world that we live in.

Effective - 3/14/2008

## [Wireless Advisory – Setting up a Wireless Network for Personal Use](#)

### **How can I set up and use a WLAN securely for personal use?**

Below are important points you need to consider when using and setting up non-Company wireless network. This information is being provided by FS/ISAC – Financial Services Information Sharing and Analysis Center.

### **Is a Wireless Network Secure?**

Wireless networks are not as secure as the traditional "wired" networks, but you can minimize the risk on your wireless network (at home or at work) by following the tips below.

### **How Does it Work?**

The standard set up for a wireless network requires two components: a Wireless Access Point (WAP) and a computer with a wireless network adaptor. Properly configuring a wireless device can be challenging and the steps will vary depending on the manufacturer. If you do not feel comfortable doing it yourself, be sure that whomever is configuring the wireless network follows these best practices.

### **Wireless Access Point (WAP)**

The WAP connects to your high-speed Internet connection or your internal network. This is the foundation for building a wireless network. It provides the ability to use a computer without being constrained by the distance of a wire. Keep in mind that metal filing cabinets as well as certain building materials, such as bricks and blocks, can interfere or limit the range - the distance between your wireless computer and the wireless access point. Generally, the indoor range for a WAP is approximately 125 feet.

### **Wireless Network Adaptor**

A wireless network adaptor, used for transmitting and receiving information, is required for each computer you intend to connect to a WAP. When purchasing wireless networking hardware from separate vendors, be sure to obtain guarantees that the hardware will conform to defined standards and interoperate properly. The wireless network adaptor is usually built into laptop computers while it is an add-on component inserted into a USB port on desktop computers.

### **Enable Encryption**

Every wireless network should enable encryption. Encryption scrambles the data in a way that if your signal is intercepted there is reduced risk of someone being able to eavesdrop or monitor your communications. There are several standards of encryption common to most WAPs. **Wired Equivalency Privacy (WEP) is the older standard. WEP has a number of known security flaws and should only be used if no other method of encryption is available.** If you use this standard, be sure to set the WEP authentication method to "shared key" instead of "open system." Under "open system" the initial sign-on is encrypted but the data is not. **The Newer wireless access points include Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is the stronger and the preferred method of encryption.**

## **Change the Default Password**

Change the default password that comes with your WAP. The default passwords used by manufacturers are well known to the hacking community. Be sure to use a strong password, at least eight characters including numbers and special characters.

## **Change SSID Name**

The Service Set Identifier (SSID) is the name of your wireless network. Default SSIDs are well known, often the name of the manufacturer and easy to guess. Change the SSID name to something unique and be careful not to use a name that freely discloses information. For example, avoid using your family name. Avoid descriptive or functional names as well, such as "Payroll" or "Accounting" since this would advertise an attractive target for an attacker.

## **Turn Off SSID Broadcasting**

By turning off SSID Broadcasting, your wireless access point does not advertise its presence. It is similar to having an unlisted telephone number. This is a way to reduce the visibility of your network to others in your neighborhood. The only way to connect to a WAP with SSID Broadcasting turned off is to know the SSID name and password.

## **Use MAC Filtering on Your WAP**

The MAC (Media Access Control) address is the unique ID assigned to your computer's network interface card. It is referred to as the computer's "physical address." Enabling MAC filtering on your WAP allows you to designate and restrict which computers can connect to your WAP. If the computer's address is not listed, a wireless connection cannot be made to the WAP. To look up a MAC address on a Windows computer, go to "Start" then "Run" and type "cmd". A new window will open and you will need to type ipconfig /all and press the enter key. A number of attributes will be displayed. The MAC address is identified as the "Physical Address."

## **RF Interference**

Assuming your WAP point functions in the 2.4 GHz range, you may experience Radio Frequency (RF) interference from other 2.4 GHz devices, such as cordless phones, microwaves and baby monitoring devices. These devices can limit wireless performance. To manage the problem, limit sources of RF interference in proximity to the WAP.

### **Additional resources for wireless networks can be found at:**

Wireless Network Tutorial including manufacturer step-by-step procedures.

<http://spotlight.getnetwise.org/wireless/wifitips/>

(<http://spotlight.getnetwise.org/wireless/wifitips/>)

Microsoft: [www.microsoft.com/technet/network/wifi/wifisoho.mspx](http://www.microsoft.com/technet/network/wifi/wifisoho.mspx)

(<http://www.microsoft.com/technet/network/wifi/wifisoho.mspx>)

For more monthly tips go to: [www.msisac.org/awareness/news/](http://www.msisac.org/awareness/news/)

(<http://www.msisac.org/awareness/news/>)

### **Additional Notes:**

- The range of the AP (access point) should not exceed the boundaries of the Physical boundaries of the buildings walls. Exceeding the boundaries means that anyone sitting outside of the building may be able to eavesdrop on then network
- Remember your secure password rules when creating passwords; passwords should contain at least 8 characters with a mix of letters, numbers and symbols. Do not use any information that can be easily obtained about you or any words from and English or Foreign dictionary.
- Install a personal firewall on your workstation/laptop. A personal firewall is a necessity for any PC that is connected to "always on" broadband facilities such as cable modems, DSL phone lines, or wireless "hot spots".
- Ensure that your operating system is up-to-date from a patch perspective.
- Follow secure file-sharing practices. Share only what you need to share (think Folders, not entire hard drives). Seriously consider password protecting **anything** that is shared with a **strong password** (passwords that are a minimum length of 8 characters containing both alpha/numeric characters).
- If possible, use a hardwired PC to administer your wireless access point or router. Disable wireless administration; if that's not possible, then use a complex password for the device.

## **Glossary**

### **802.11b**

The original baseline IEEE (Institute of Electrical and Electronics Engineers) wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

### **802.11g**

This is five times faster than the original 802.11b, which it is displacing in the marketplace. Users should note that devices from both of these standards will communicate between each other, although at a lesser maximum speed overall.

### **802.11a**

A faster standard than 802.11b, but it is on a different radio frequency and is NOT compatible with either 802.11b or 802.11g.

### **Access Point**

Device that allows wireless-equipped computers and other devices to communicate with a wired network. It can also be used to expand the range of a wireless network.

### **DHCP (Dynamic Host Configuration Protocol)**

A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

### **MAC (Media Access Control) Address**

The unique address that a manufacturer assigns to each networking device, such as a LAN card.

### **SOHO**

An acronym for Small Office/at-Home Office environments.

### **SSID (Service Set Identifier)**

Your wireless network's name.

**TCP/IP (Transmission Control Protocol/Internet Protocol)**

A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

**VPN (Virtual Private Network)**

An extension of an organization's private network across a public network (usually the Internet). 'Tunneling', that is, encryption is used to retain privacy from one point in the private network, across the Internet to another point

**WEP (Wired Equivalent Privacy)**

A method of encrypting data transmitted on a wireless network for greater security. Now considered flawed and by itself an inadequate security control.

**WLAN (Wireless Local Area Network)**

A group of computers and associated devices that communicate with each other wirelessly.

**WPA (Wi-Fi Protected Access)**

Is the newest and best available option in Wi-Fi security. **WPA2 is the stronger and the preferred method of encryption.**