



NYS Office of Cyber Security

Monthly Security Tips NEWSLETTER

September 2012

Securing Your Wireless Network

From the Desk of Thomas D. Smith, Director

Wireless networks are not as secure as the traditional “wired” networks, but you can minimize the security risks (at home or at work) by following the tips below.

How Does it Work?

A wireless network requires two components: a Wireless Access Point (WAP) and a computer with a wireless network adapter. Properly configuring a wireless device can be challenging and the steps will vary depending on the manufacturer.

The WAP connects to your high-speed Internet connection and/or your internal network. It provides the ability to use a computing device (laptop, copier, printer, etc.) without being constrained by a wire. A wireless network adapter, used for transmitting and receiving information, is required for each device you intend to connect wirelessly to a WAP. The wireless network adapter is usually built into laptop computers, while it is an add-on component for other devices.

Tips for Securing Your Wireless Network

Enable Encryption

It is critical that every wireless network has encryption enabled. Encryption scrambles the data to reduce the risk of someone being able to eavesdrop or monitor your communications if they are intercepted. There are several standards of encryption common to most wireless components. Newer wireless components include Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) encryption. WPA2 is stronger and the preferred method of encryption. If WPA2 is not available, it is recommended that you use WPA. If your network only allows for WEP (Wired Equivalency Privacy), an older standard of encryption, it is recommended that you replace your wireless components with ones that support WPA2 or WPA.

Change the Default Password

Change the default password that comes with your WAP. The default passwords used by manufacturers are well known. Be sure to use a strong password that is at least eight characters in length and includes a mix of upper and lower case letters, as well as 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—or 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 WAP 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 within range of your WAP. 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 wireless adapter. 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, select "Start" then "Run" and type "cmd"; then a new window will open; type "ipconfig /all" and press the enter key. A number of attributes will be displayed. The MAC address is identified as the "Physical Address."
- For a Mac Operating System, click on "System Preferences"; select "Network"; select "WiFi"; click on "Advanced"; in the tool bar that appears, click on "Hardware." The MAC address will be displayed on the first line.

Update the Software/Firmware in Your Wireless Components

Contact the manufacturer for directions and guidelines on how to update the software and firmware in your wireless components. If the option is available, enable the auto-update feature.

For More Information:

- **OCS Newsletter Tips**
<http://www.dhSES.ny.gov/ocs/awareness-training-events/news/>
- **PC World: How to Use Your Wireless Network**
http://www.pcworld.com/article/130330/how_to_secure_your_wireless_network.html
- **OnGuard Online: Securing Your Wireless Network**
<http://onguardonline.gov/articles/0013-securing-your-wireless-network>

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:



MULTI-STATE
Information Sharing
& Analysis Center™

A DIVISION OF  CENTER FOR
INTERNET SECURITY