



## Secure Your Wireless Network

Although its importance can't be stressed enough, many people tend to take for granted the importance of securing their wireless routers when they implement wireless systems in their business. It is actually the first thing that people should do as soon as they have installed a wireless system in the workplace.

[Securing your business' wireless network](#) is of the utmost importance. Why? An unsecured wireless access point could leave your company's network and data wide open. Anyone with access to your network can view sensitive information from your servers and other networked computers. Add to the fact that since your network is open, other people can use your network, which can use up your network bandwidth and affect your company's operations.

So be sure to have your network safely secured from outside threats. To secure your company's wireless router or access point, here are the basic steps that you need to do:

- First, know how your wireless network works. Today's wireless technology uses radio signals when transmitting data and these could be transmitted over great distances. People with greater technological capabilities could sniff out data transmitted from your wireless systems and take them away.
- Most wireless routers come with a default username and password. Change it right away! This can never be overemphasized. Make sure that you choose a complex combination of characters for your username that only you can remember, but don't lose it. Ideally, passwords should be at least eight



## All Covered®

characters long. However, be sure to choose a strong password with a combination of alphanumeric characters. Stay away from passwords that are associated with birthdays, anniversaries, etc.

- If your wireless router supports WPA2, use it. It is by far the strongest encryption technology to date. If you haven't purchased a router yet, stay away from routers that only support WIFI Protected Access or WPA and Wired Equivalency Privacy or WEP. Only choose routers that support WPA2. Why? WPA and WEP can be easily cracked, and many of these tools are available online.
- Immediately change the default SSID of your wireless router and disable broadcasting. Your router's SSID is nothing more than your network's identity. Routers use generic manufacturer SSID upon purchase by default such as Linksys, default, etc. Change it to something that is not common or can be remembered easily. When choosing a strong network identity or name, the best practice is to stay away from anything that are associated to your business' name, birthdays, anniversaries, spouse's name, etc. A poorly configured SSID is very prone to attacks that could lead to devastating results. It is also very important to do is turning off broadcasting. By doing so, you keep your routers out of sight from prying cyber criminals.
- Enable Media Access Control or MAC address restriction. A MAC address is a 12-character ID that is attached to network devices. Enabling MAC address restriction will allow only specific devices to access your wireless router. This can add more security to your system.



Another important thing that you should do to keep your wireless network secure is to keep yourself abreast with the latest in wireless technology. Doing so will keep you informed of the latest trends in network security, as well as potential vulnerabilities that can affect your company's IT infrastructure.

To learn more about how you can safely secure your company's wireless network, visit [All Covered](#) or call 866-446-1133.

Contact All Covered Toll-Free Nationwide at (866) 446-1133 or at [www.allcovered.com](http://www.allcovered.com)

©2009 All Covered, Inc. All rights reserved. All Covered is a registered trademark of All Covered, Inc.