

Forum:[Hack Forums](#)

Thread: [How To Secure WiFi Zone \(Full Tutorial\)](#)

¢?I? T????? - December 9, 2010, 11:26 am

[img]http://www4.picturepush.com/photo/a/4661462/img/4661462.jpg[/img]

It's very important to secure your WiFi connection to prevent unauthorized access to your computer files and online activity.

Wireless networks are extremely convenient, allowing access to the Internet without being connected to a cord. But networks can extend more than 400 feet from the router, allowing anyone in the vicinity to access your home network.

This is dangerous for many reasons.

1. Anyone connected to your network can gain access to your hard drive and online activity, capturing private information like passwords and account numbers.
 2. Computers connected to your network can spread viruses or other dangerous software.
 3. If someone using your network commits a crime, the activity will be traced back to your router.
- With identity theft being so prevalent, it's important to take precautions when setting up a wireless network in your home and using one when you're away from home.

Step 1: Change default login

Once your router is connected, you will be able to access your router settings through a web-based set up page.

1. The manufacturer will provide a URL with a login and password to access the router configurations.
2. Once you access this page for your router and log in with the default password, find the "administration" or "settings" section where you can change your password.
3. Select a difficult to guess password, with a mix of numbers, symbols and letters, and don't use personal information or common words.

Leaving the login information as the default allows hackers to easily gain access to your router settings by going through all default logins.

Step 2: Use Encryption

There are two main types of wireless encryption

1. WEP (Wired Equivalent Privacy) is an older form and less secure, but if it's the only available option on your machine, it's better than not having any encryption. 128-bit WEP is better than 64-bit WEP.
2. WPA (WiFi Protected Access) is more secure and newer than WEP, and is available on more current machines. WPA2 is the newest type, and provides the highest level of protection.

Step 3: Change SSID

The SSID (Service Set Identifier) is the name of your network. The manufacture sets a default

identifier like the default administrative login for the router settings.

1. While in your router's web-based set up page, find your wireless settings.
2. Find the field labeled SSID.
3. Change it to a unique name.
4. Do not use your address, company name, or other identifying names like "Parker Residence" or "Finance Department of ABC Company."

Like the default logins/passwords, hackers know the default names of different manufacturer's SSIDs and will be one step closer in getting onto your network.

Step 4: Disable broadcasting

Wireless networks will "broadcast" its SSID so any computer within range can see the available networks in the area. In order to access a wireless network, the SSID name and password needs to be entered. By broadcasting your SSID, you're providing important access information to your network. Disable the broadcast option so someone needs to know both your SSID and password in order to get onto your network.

1. You should be able to disable the SSID Broadcast on the same page you configure your SSID name.
2. Select the option to disable or turn it off.

Step 5: Enable Mac filtering

Every computer has a MAC (Media Access Control) address. Limit access to your network by only allowing specific computers to connect to it.

1. While in your router's web-based set up page, find the Wireless section.
2. Look for MAC filter.
3. Enter the MAC addresses of the computers allowed on the network and make sure to enable, confirm, or turn it on.

Step 6: Reduce your WLAN transmitter power

You won't find this feature on all wireless routers and access points, but some allow you lower the power of your WLAN transmitter and thus reduce the range of the signal. Although it's usually impossible to fine-tune a signal so precisely that it won't leak outside your home or business, with some trial-and-error you can often limit how far outside your premises the signal reaches, minimizing the opportunity for outsiders to access your WLAN.

Step 7: Disable remote administration

Most WLAN routers have the ability to be remotely administered via the Internet. Ideally, you should use this feature only if it lets you define a specific IP address or limited range of addresses that will be able to access the router. Otherwise, almost anyone anywhere could potentially find and access your router. As a rule, unless you absolutely need this capability, it's best to keep remote administration turned off. (It's usually turned off by default, but it's always a good idea to check.)

Most hackers will target easy to crack and unsecured public networks. By taking these precautions, you can prevent the most common online security intrusions.

[img]<http://www4.picturepush.com/photo/a/4661462/img/4661462.jpg>[img]

N.B: Please post your feedback here.

