



## **Internet Wireless Access Points and What You Should Know**

Consider this scenario – It is 6:00 AM and you hear loud knocking at your front door followed by the words, “Police – Search Warrant!” You answer the door and several police officers come into your house, read you a search warrant and seize your computers. The search warrant refers to child pornography possession and you have no idea why the police are at your door for this. After a few hours of your entire house being searched, the police give you a receipt for the items they seized and leave your home.

This scenario is very real, it has happen before in our county and the cause was an unsecure, open Internet wireless access point (AP) or router at the persons home or office that has been accessed by a criminal who looked at child pornography. Within the past few months the Southern Oregon High-Tech Crimes Task Force has investigated several cases where an Internet Protocol (IP) address was captured during some illegal activity. Upon further investigation we determined the suspect actually used a neighbor’s unsecure wireless router to conduct the illegal activity.

When someone uses your wireless connection to access the Internet, all of their activity will come back to your IP address. If a neighbor of yours is sitting on their couch, downloading child pornography or pirated music, to the investigators it will look like it’s all coming from your home address. A law enforcement agency could easily obtain a search warrant for your home to seize any evidence relating to the illegal Internet activity.

By now, if you have an unsecure wireless router I’m sure I have your attention. What can you do to fix this problem? I will give you some general suggestions and provide you with an Internet link to find more detailed instructions on how to make your wireless router or AP more secure.

By default when you take a DLink, Linksys, Netgear, or most other brand wireless AP’s or routers out of the box it is configured to be completely open and unsecure. Once you connect the wireless access point to your Internet connection, you should also connect a computer to the router using an Ethernet cable. This will allow you to log directly into the wireless router and change the configuration settings. Each wireless router has an IP address (discussed in the owner’s manual) that you can type directly into the address bar of your preferred Internet browser to login.

Here is a very brief overview of the steps you should follow to make your router or AP safer. If you would like to view a more in-depth set of instructions please visit <http://onguardonline.gov/wireless.html>. Once you login to your device I recommend the following:

#1 – Disable the SSID (Service Set Identifier) broadcast. This will make most computers searching for a wireless connection not even see that you have a wireless router. While this is a good first step, it does nothing to secure your device

#2 – Enable MAC (Media Access Control) address filtering. You will need the MAC addresses from each of your Internet devices you wish to connect to the router.

#3 – Enable WAP (WiFi Protected Access) encryption. If you have devices that won't accept WAP, at least use WEP (Wired Equivalent Privacy) encryption.

#4 – Change the default administrator password to access your router or AP.

By taking these steps you will make it much more difficult (not impossible) for someone to gain access to your wireless router or AP. Most criminals choose the path of least resistance, if you take these steps they most likely will pass your home or office to look for a much easier target that is open and unsecure.

Sergeant Josh Moulin – CFCE, CEECS  
Southern Oregon High-Tech Crimes Task Force Commander  
Central Point Police Department