

LAW and ORDER

Wi-Fi Concerns

by Kevin Gordon

A useful guide is available on the use of wireless networks. This was produced by the Global Security Working Group. Global works with information technology and interoperability issues. The guide, titled "So You Want to Set Up Wi-Fi..." is an excellent document that provides eight quick tips, in order of importance, that you should take if you are setting up a Wi-Fi network.

Tip #1: Change Passwords

Default administrator login and passwords are set at the factory. The recommendation is even before plugging the wireless access point (WAP) into your network, plug a computer into the WAP and change the password for the administrator. It is also recommended to change the administrator passwords every one to three months. While this is obviously important for security concerns, many of us are guilty of violating this simple security method. If you are in an administrative position, how recently have you changed the administrator password hardware system? Most of us would never install a new electronic garage door opener without changing the default code but often we overlook the same basic security at work. After all, the average police agency in the United States is fewer than 10 officers, and in such agencies, rarely is an officer assigned to department security issues, be those electronic or the physical plant itself.

Tip #2: Turn on Encryption

We all realize that Wi-Fi security issues are a concern to the common business as well as government agencies, and just about everyone in the business can give their favorite horror story of failed security. Many levels of security exist, but criminal justice agencies are held to an even higher standard. Those requirements can be found in the Criminal Justice Information Services (CJIS) Security Policy. Quite simply, the encryption used must be better than the norm, and it has to be used. I'm betting you haven't investigated too many burglaries of residences that had good security dead bolt locks except those who chose not to use the locks. How many stolen car reports have you taken where the victim left the car unlocked, key in the ignition and maybe even running? Get professional advice on encryption, and then use it.

Tip #3: Configure the Firewall

Many administrators know what a firewall is and why it is used but may not really understand firewalls. Most likely, you have an effective firewall installed in your agency network. Remember that the firewall between your network and the Internet has no effect whatsoever on the wireless access point. It is comparable to having a high security steel door to protect your assets but you leave the windows wide open.

Tip #4: Change the Network Name

Wireless access point manufacturers ship their products with a default network name as with the already mentioned administrator login and password. The fact that a hacker knows your network name doesn't make it any easier for him/her to break in, but it is an indicator of a possible easy mark. After all, if you left this default in place, maybe you left others in place, and the hacker's path may be easier. The name you change the default network name to should not be something that easily identifies your agency.

Tip #5: Enable MAC Address Filtering

A user device connected to your wireless access point has a Media Access Control (MAC) address. This

address determines who is allowed to access the media. This is called a unique address, but that isn't an accurate descriptor because it is often possible to change the MAC address on a unit. Not all WAPs permit the administrator to list the addresses of those devices permitted to connect, but it is an additional option to consider.

Tip #6: Disable the Name Broadcast

Do you realize that a wireless network, by default, broadcasts a signal that provides needed information including the service set identifier (SSID) or name? The network name broadcast tells the world "here we are; come talk to us." If they can't find the item, they can't steal it. If you don't want folks to break in, why tell them you are open for business. The broadcast can be disabled, which, in essence, hides the fact you are there.

Tip #7: Static IP Addresses

The Internet Protocol (IP) address is a unique number for each item connected to a network. A dynamic IP address is usually used by Wi-Fi systems as it allows the user to automatically connect without the need to know the address details of each network. A static IP address is used for devices with a constant IP address such as your internal server and the units within your agency. The dynamic IP address is more convenient, hence the use on Wi-Fi, but it is also less secure. Assigning static addresses makes it harder to hack.

Tip #8: Access Point Safely

The last tip is to position the access point safely. That includes several areas including permitting only the administrator to actually have physical access to the WAP so no settings can be changed intentionally or by accident. It also means that you should know the actual range of your network. This not only tells you where you can be to access the network, but also how far away a potential hacker can be.

Kevin Gordon spent 25 years in law enforcement and retired as a chief of police. He is a national and regional officer of the International Police Association. He can be reached at Kevin@KGordon.com.

This article was printed in Law and Order Magazine, October 2006.