Unless you take some kind of action to find it, a rogue access point can operate undetected on your network for months or even years. You may not discover it until you report to work one day and find that your network has been trashed by an intruder who found his way into your network via an unprotected wireless access point that you didn't even know existed.

Here are some steps you can take to reduce the risk of rogue access points appearing on your system:

- **Establish a policy prohibiting users from installing wireless access points on their own.** Then make sure that you inform all network users of the policy, and let them know why installing an access point on their own can be such a major problem.
- **If possible, establish a program that quickly and inexpensively grants wireless access to users who want it.** Rogue access points show up in the first place because users who want access can't get it. If you make it easier for users to get legitimate wireless access, you're less likely to find wireless access points hidden behind file cabinets or in flower pots.
- **Once in a while, take a walk through the premises, looking for rogue access points.** Take a look at every network outlet in the building and see what's connected to it.
- **Turn off all your wireless access points and then walk around the premises with a wireless-equipped mobile device such as a smartphone and look for wireless networks that pop up.** Just because you detect a wireless network, of course, doesn't mean you've found a rogue access point — you may have stumbled onto a wireless network in a nearby office or home. But knowing what wireless networks are available from within your office will help you determine whether any rogue access points exist.

Hopefully I've convinced you that wireless networks do, indeed, pose many security risks. Here are some steps you can take to help secure your wireless network:

- **Create a secure wireless password.** The first thing you should do when you set up a wireless network is change the default password required to access the network. Most manufacturers of wireless routers secure the SSID with a standard password that is well known. Make sure you change it to something that only you know, and then only share that password with those you want to grant access to.
- **Change the administrative password.** Most access points have a web-based setup page that you can access from any web browser to configure the access