How to lock your Wi-Fi and protect your home

Tech Talk

Kim Komando

Take steps to secure your Wi-Fi before moochers and criminals slow down your connection. GETTY IMAGES

People love to mooch Wi-Fi. They find an unprotected signal and sign on. Why not? It's free. Your neighbor won't mind if you steal a little broadband to watch Netflix, right?

Criminals also love unsecured Wi-Fi, and they do mean harm. They use your network to attack your gadgets and steal your personal information. They download illegal files through your router, making you vulnerable to a police investigation.

Moochers slow down your connection, causing buffering, and make it harder for you to finish online tasks or a movie. But moochers aren't the only cause for a pokey connection.

If your router is more than a few years old, it's time to get a new one. I like picking the router based on the size of a home.

Here are a few tips for securing your Wi-Fi router against unauthorized hitchhikers:

1. Get a list of everything using your network

Time to look at your network. First, you'll want to log into your router's administration console. You will log into your router, the same way you'd log into any computer. Every router has a different way of doing this, so check your manual for specific instructions.

(If you don't have your manual anymore, check the manufacturer's site.)

Ensure your device is connected to your router; it doesn't matter whether this is through a wireless connection or by cable. Open a browser and type in the router's IP address. The IP address is a set of numbers, and the default depends on your router's manufacturer. The common ones are 192.168.1.1, 192.168.0.1, or 192.168.2.1.

Check the DHCP Client List or Attached Devices section that shows what gadgets are connected to your router. Typically, they are listed by IP address, MAC address and/or Name. Once you've surveyed this list of connected gadgets, figure out which ones belong to you. You should recognize your main computer's name, and your tablet or smartphone should have the name of the manufacturer or model.

If you can't make sense of the list or identify certain devices, turn off each gadget one by one. You can also disable each gadget's Wi-Fi. For tracking purposes, jot these network details down or take a quick pic using your smartphone so you can reference them later. If you've switched everything off and still see unknown gadgets, you know you have a culprit.

Now, there's a much simpler way: You can use the aptly named Wireless Network Watcher. This free program gives you a list of gadgets connected to your Wi-Fi network. You can quickly fire it up whenever you want to check or leave it open for real-time monitoring. Easy.

2. Lockout unauthorized users

You may find intruders, or you may not. Either way, you can protect your Wi-Fi connection (and your data) by encrypting your connection.

Every router on the market offers several encryption options. One type to avoid is "WEP," which is outdated and easy to circumvent. Instead, look for any encryption that starts with "WPA2," the most recent being "WPA2-PSK AES." The WPA2 family of encryption should protect your router from any run-of-the-mill hacker.

Your network may already be encrypted, yet outsiders are still accessing your Wi-Fi. If so, change your password immediately. You can also reset your router to factory settings (consult your manual) and set up your Wi-Fi signal from scratch.

This step means changing the default password, enabling encryption, picking a new SSID and turning off any remote management features. Just remember, if you change your encryption password, you'll have to update the password on all your devices as well.

3. Clever idea to set up another network

Friends and family always want to use your Wi-Fi. They ask politely, phone in hand, because they hate to burn up their data plans when they can use your connection. Instead of handing them your real password, use your router's "Guest Network."

This feature lets you share your internet connection with your guests while keeping them off your main network, preventing them from seeing your shared files and services. To avoid confusion with your main network, set up your guest network with a different network name (SSID) and password.

Although the guest network is available to guests, maintain the same level of security as your primary network. This means developing a strong password and restricting access to your shared files and devices. Make sure that "local access" is set to "off," which will prevent guests from tampering with your system.

4. Turn off the ability for others to access your router

"Remote administration" is a feature that allows you to log into your router over the internet and manage it. If you've ever called tech support, you may have experienced something similar: A faraway technician speaks with you on the phone and then operates your computer as if he's sitting right next to you.

Remote administration is a handy tool, especially when you need to fix a problem, but it leaves your computer vulnerable to hackers. Unless you need it, turn this feature off. You can find this under your router settings, usually under the "Remote Administration" heading.

You can always switch it on again if the need arises. The last thing you need is to invite strangers to your home network.

Learn about all the latest technology on the Kim Komando Show, the nation's largest weekend radio talk show. Kim takes calls and dispenses advice on today's digital lifestyle, from smartphones and tablets to online privacy and data hacks. For her daily tips, free newsletters and more, visit her website at Komando.com.