6 Steps: Keep Unauthorized Devices Off Your Wireless Network

How many devices are connected to your home's wireless network? As time passes and you add new gadgets, it's easy to lose track.

And that's a problem; hackers may have accessed your network, gaining access to your logins and personal data. These tips from the pros show you how to check and eliminate devices if necessary:

1. **Make note of your router's unique Internet Protocol address.** Ideally, you captured this info when you purchased and installed the router. But if you didn't, note the manufacturer and model number. From there, a quick Google search will show you how to discover the IP address.

2. **Type the IP address** into your browser's address bar. This will open your router menu.

3. **Log in.** When your router was installed, you should have created a unique username and password for login purposes. If you didn't—that is, if you committed the security sin of sticking with the defaults—now's the time to do another search, learn the router's factory default username and password, and change them. All the usual password advice applies, of course: Create a password of at least eight characters, and be sure to use upper- and lowercase letters, a numeral, and a special character.

4. **Check for a list** that says DHCP Client or Connected Devices. This is where you'll see a list of devices currently using your network.

5. **Delete** any devices you do not recognize.

6. **Change your wifi password** and reconnect only the devices you trust.

Being more aware of who's using your network is an important step forward for your internet speed and privacy, and we could all be a lot more vigilant about that.

5 Things to Never Search for on Google

SEI New ways. New answers.®

Experts say there are some seemingly innocent search terms that could expose you to malicious actors. No matter how innocent your intentions, these Googles may lead to trouble:

1. **Customer service toll-free numbers.** Even the top-ranked results can lead you to fake phone numbers at which scammers will request personal information, including credit card numbers. You may also come across a malicious link that will infect your computer with malware. To contact a company, go to its official page for info.

2. **Tech support.** Scammers "spoof" websites that look like the real thing. You'll be faced with a bogus phone number where they try to get payment out of you. They aren't fixing anything, just ripping you off. Always find tech support links and phone numbers through official websites.

3. **Financial services and apps.** Payment apps like Venmo, Zelle, and PayPal make it easy to send money to a business or friend—but be careful when using them. Use these services' official websites, or the app itself, to get any contact information you need. And take the same precautions with your banking activity.

4. **Government programs.** The pandemic has been rough on everyone, and you may be anxious to find out when you will be receiving some help. Unsurprisingly, criminals are just waiting for you to search for something like "Where is my stimulus check?" Such a search may direct you to a site that requests payment or installs malware on your devices.

5. **Tradespeople.** A result at the top of a search doesn't automatically mean a plumber, contractor, or electrician is reputable. Before you give away any information or pick up the phone, check a review site such as Angie's List or Yelp.