THREE SECURITY-BOOSTING STEPS TO PERFORM ON YOUR ROUTER

BEGINNERS KAFFEE KLATCH
PRESENTED BY BILL WILKINSON

The computer industry has worked hard to make sure that a lot of the gadgets we use are mostly plug-and-play. In other words, you just fire up the device, login and you're ready to go—no configuration necessary. One device you should never consider "plug-and-play," however, is your home's network and wireless router.

After the technician leaves your house there are a few important things everyone should do.

Log in to your router and change the admin details

The first thing you should always do when you have a new router is log into its control panel. You want to do this so you understand where to change the Wi-Fi access password, change the type of security protocol your router is using, change the router name, et cetera. Most importantly, however, you need to login to your router so you can change the admin name and password.

Alas, some routers won't let you change the admin user name, but changing the admin password is the crucial part. If you *don't* do this and a bad actor is able to get onto your home network, they can easily log in to your control panel and own your router using the device's default settings.

If you don't know how to login to your router check the manual that came with it, ask your Internet service provider, or try to find a user manual for your model online.

Use WPA2

Now that you've logged in to your router, it's time to make sure you are using WPA2 (Wi-Fi Protected Access II) as the encryption standard for connecting to your router.

Right now, WPA2 is considered the best way to secure your router connection. This standard works by encrypting all traffic between devices and the router, making it much harder for anyone to nab your data as it travels through the air.

One thing you'll also want to do is make sure that Wi-Fi Protected Access (WPA) is disabled. This feature allows a weakness in your router that could be exploited by a determined attacker.

Your router's encryption protocol settings are often found under the Security heading or something similar.

Use an uncomfortably long password

Now don't go too nuts with this one. Don’t use a 100-character password or something like that, but a 20-30 character password with randomly generated letters, numbers, and special symbols (if allowed) is a pretty solid idea. The point is to make it as hard as possible for an attacker to figure out your password. One easy way to do that is to make this password a little longer than most passwords you use online.

It *does* mean you should probably use a password manager to remember it, and the occasional need to log new devices onto the network can be a pain. But the extra effort pays off with a more secure password that keeps the bad guys off your network.

Those are just three basic things, but once you're inside your router there's all kinds of other settings you could tweak such as changing the Wi-Fi broadcast channel, change the channel width, adjust your NAT settings, and configure port forwarding.