NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

Secure Your Home Router

Most home routers ship with default settings that are easy for an attacker to find. This guide covers the handful of changes that close the biggest holes: default logins, Wi-Fi passwords, encryption, updates, and a separate guest network.

Why this matters

A few minutes of setup closes the biggest holes.

It's the gatekeeper
Every device in your home connects through it, including your smart home gear.

Defaults are public
The default login and settings for most routers are easy to look up online.

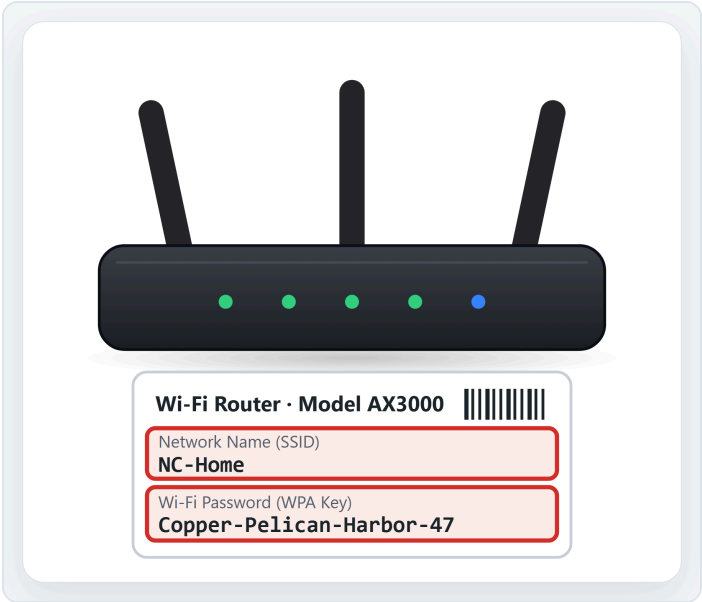
A quick fix
Changing a handful of settings closes the biggest, easiest holes.

The router settings that actually matter for security

1 Change the defaults

That sticker has your router's login, network name, and Wi-Fi password, all set at the factory.

WHAT TO DO
Change the router login, the network name, and the Wi-Fi password. Use a long, random passphrase for each.



2 Set up a guest network

A separate network, with its own password, for visitors and smart-home or IoT devices.

WHAT TO DO

Guest devices stay off your main network, so a vulnerable smart plug can't see your computer.



NAPLES COMPUTERS

★ Not sure what your router can do?

We'll check your settings, lock it down, and set up a guest network, or recommend a new one if it's time.

WHAT TO DO

Call 239-513-1960. We work with TP-Link Deco, EnGenius, and Ubiquiti.



Encryption and updates

- [ ] WPA3, or WPA2 with AES
  Those are the only two encryption types considered safe today
- [ ] Keep the firmware current
  Turn on automatic updates if your router offers it
- [ ] Skip personal info in the network name
  A name like “The Smiths” tells a stranger who lives there

Lock down a few features

- [ ] Disable remote management
  It lets someone change your router's settings from outside your home
- [ ] Disable WPS
  The “push to connect” button is an easy way in for an attacker nearby
- [ ] Disable UPnP once devices are set up
  Useful for adding a smart device, risky to leave on afterward

Recap: secure your home router

- [ ] Change the default login, network name, and Wi-Fi password
- [ ] Use WPA3 or WPA2 with AES, and keep the firmware updated
- [ ] Disable remote management, WPS, and UPnP
- [ ] Set up a separate guest network for visitors and smart devices
- [ ] Not sure what your router can do? Call Naples Computers

The Wi-Fi password printed on your router's sticker is a good start, but also change the router's own login (the one that controls its settings), which is often the same generic default across every unit of that model.



Not sure what your router can do? We'll check it and lock it down.

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**