

5 Things Exposing Your Wi-Fi Right Now

A fast, no-fluff list of the most common Wi-Fi vulnerabilities. Check every one in ten minutes.

From the TechODash Home & SOHO Network Security series. Each item below takes two minutes or less to check.

CHECK THESE FIVE THINGS

- **The router's default admin password**
If you've never changed it, it's likely still the manufacturer's default — attackers keep searchable databases of these by brand and model.
- **An outdated Wi-Fi encryption standard**
Check your Wi-Fi security setting. If it says WEP, WPA, or WPA2 and your router supports WPA3, switch to it now.
- **An SSID that names your router's make and model**
A network name like "NETGEAR54" hands an attacker a head start on which known vulnerabilities to try first.
- **No guest network separating visitors and smart devices**
Every guest or IoT device sharing your main network can potentially reach every other device on it.
- **Firmware that hasn't been updated in months**
Firmware updates patch real security holes, not just add features, and most routers won't apply them automatically.

WANT TO GO DEEPER?

The SOHO 2026 Guide covers the full picture: network architecture, device segmentation, remote work security, and AI scam defense — with checklists and templates for home offices and small businesses.

soho2026.gumroad.com//soho-2026