

Guest Wi-Fi should never touch your business network. Work down the list, then prove it with the test in section 2.

1. THE SETUP

- ☐ Create a separate guest network name (SSID), named professionally: YourBusiness-Guest.
- ☐ Put guests on their own segment. On most current home and prosumer routers, the built-in "guest network" toggle does this, but check for a setting like "allow guests to access my local network" and make sure it is off. On access points or mesh units in bridge mode, a guest SSID often separates nothing, which is why section 2 is not optional. On business gear, this means a separate VLAN with a firewall rule between it and your main network.
- ☐ Turn on client isolation (some routers call it AP isolation) so guest devices cannot see each other. Guest network only: on some routers this is a global wireless setting, and enabling it everywhere stops staff devices from printing or casting.
- ☐ Protect it with WPA2 or WPA3 and a simple passphrase, using the WPA2/WPA3 mixed option if available so older phones can still connect. A fully open network invites neighbors and parking-lot traffic.
- ☐ If your router offers it, cap the guest network share of your internet connection so one video streamer cannot eat the whole circuit.

2. PROVE THE SEPARATION

- ☐ Confirm the one rule that matters: the guest network cannot reach your main network. On business gear, look for an explicit guest to LAN deny rule.
- ☐ Prove it with a phone. First, while on your main network, get the printer or camera IP address from its own screen or settings. Then join the guest Wi-Fi, turn cellular data off, and type that IP into a browser. It should time out or refuse to connect, not load a page. Try your router admin IP too. If either loads, your separation is not real.
- ☐ Audit what is on the guest network today. No printers, no cameras, no card readers or point of sale, no back-office laptops. Ever.

3. KEEP IT THAT WAY

- ☐ Rotate the guest password on a schedule. Quarterly works for most businesses, and always after staff turnover.
- ☐ Disable WPS (the pairing shortcut with the router button and an 8-digit PIN). The PIN half can be brute forced, so turn the whole feature off.
- ☐ Keep router and access point firmware updated, after hours, since updates reboot the gear. Put a recurring reminder on the calendar.
- ☐ Label the equipment in the closet: which box is the modem, the router, the firewall, the switch.
- ☐ Write down where the configuration lives and who to call when something breaks.

RED FLAGS

- ⚠ Card readers or point of sale on the same network as guests. That can put your PCI compliance at risk.
- ⚠ Security cameras reachable from the guest network. That is a privacy problem waiting for a headline.
- ⚠ One flat network for everything with the password on a sticky note. That is all of the above at once.