

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to turn on WPA3 or the strongest Wi-Fi encryption you have

<https://cyberguardlab.com/blog/wifi-wpa3-strongest-encryption>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

CYBERGUARDLAB · GUIDE

How to turn on WPA3 or the strongest Wi-Fi encryption you have

WI-FI SECURITY

WPA3-Personal

Prefer WPA3 or WPA2/WPA3 transitional.

Avoid open / WEP / WPA

Router Wi-Fi settings

Strongest mode available

Rejoin devices after

Turn on WPA3-Personal (or WPA2/WPA3 transitional if older devices need it) in your router's Wi-Fi security settings so new connections use the strongest handshake your hardware supports. Avoid open, WEP, and WPA-only modes. This how-to is wireless encryption-not changing the router admin password, not Android Private DNS, and not VLAN design for cameras.

1. Before you change Wi-Fi security

- * Update router firmware from the vendor's official channel.
- * Inventory old gadgets that may not speak WPA3 (some IoT sticks, printers, older phones).
- * Have the admin login ready (change it if still default-see admin guide).
- * Plan a short outage: devices will reconnect with the new settings.

Third-party firmware from unknown downloads can brick hardware or add backdoors. Prefer vendor-signed updates when you only need WPA3 toggles.

Paid link

Norton 360 | See the Norton first-year offer



Norton 360

From \$39.99

first year - 30-day refund

See the offer

[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton>

2. Encryption choices compared

Encryption choices compared

Mode | Use when | Avoid when

WPA3-Personal | Clients are modern | Legacy IoT cannot connect and you need that device online

WPA2/WPA3 mixed | Household transition period | You can fully retire WPA2-only gear

WPA2-only | Hardware cannot do WPA3 | WPA3 is available and all clients work

WEP / Open | Never for home data | Always for primary SSIDs

WPA3 vs router admin password

WPA3 protects traffic between devices and the access point. The admin password protects who can rewrite those Wi-Fi settings. Do both.

3. Steps: enable WPA3 or strongest available

- * Connect to the router admin UI on LAN (typed IP or official app).
- * Open Wireless / Wi-Fi settings for the band you use (2.4 GHz and 5/6 GHz may be separate).
- * Find Security mode / Authentication.
- * Select WPA3-Personal if all important clients support it.
- * If something critical fails to join, use WPA2/WPA3-Personal mixed (transitional) rather than dropping to WPA/WEP.
- * Set a long, unique Wi-Fi passphrase (different from the admin password). Save/Apply.
- * Reboot the router if prompted. Rejoin devices; forget old SSIDs on stubborn clients.
- * Disable WPS push-button if your threat model includes nearby tampering and your household can live without it.
- * Optional: separate guest SSID with its own passphrase for visitors.

4. After you apply settings

- * Confirm phones show WPA3 or the expected security in Wi-Fi details when the OS exposes it.
- * Segment risky IoT later with a VLAN or guest network.
- * Keep endpoint security on PCs with Norton or Bitdefender (TotalAV, McAfee, Avast on-site)-Wi-Fi encryption is not antivirus.

FAQ

My smart bulb will not connect after WPA3-only. What now?

Use mixed WPA2/WPA3 or move fragile IoT to a dedicated SSID/VLAN still using WPA2 while phones stay on WPA3.

Is WPA3 the same as a VPN?

No. WPA3 is local wireless security. VPN protects paths beyond your LAN.

Does changing Wi-Fi encryption change the admin password?

No. Set admin credentials separately.

Mesh satellite will not adopt-help?

Adopt nodes while on Ethernet if the vendor recommends it; ensure all nodes support the same security mode.

If you still want a paid suite

Avoiding how to turn on WPA3 or the strongest Wi-Fi encryption you have does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV ([paid link](#)), Norton ([paid link](#)), Bitdefender ([paid link](#)), McAfee ([paid link](#)), Avast ([paid link](#)).

Sources

- * FTC: Secure your home Wi-Fi
- * CISA: Secure your home network
- * Wi-Fi Alliance: WPA3 overview
- * Example vendor (Asus WPA3)

Also read

- * How to change your router admin password safely
- * How to set up a guest Wi-Fi network at home
- * How to update home router firmware
- * How to segment smart TVs and cameras on a separate VLAN
- * How to check if your home Wi-Fi is safe