WEP vs WPA - what they are, why WEP is unsafe, and the settings to use

Gridinsoft Help Center

What it is

WEP and WPA are Wi-Fi security standards. WEP is the early, weak option that is easy to break. WPA and newer WPA2/WPA3 use stronger encryption to protect your Wi-Fi so others can’t read your traffic or hop on your network. More: https://gridinsoft.com/wep-wpa

Why it matters

If your router uses WEP or "Open" Wi-Fi, nearby attackers can crack it in minutes, spy on browsing, or use your internet. Using WPA2 or WPA3 keeps your connection private and much harder to hijack.

How it works

- WEP: old method with flaws. Static keys and weak design make it easy to crack.
- WPA/WPA2: stronger encryption. WPA2 with AES is the long-time standard for home networks.
- WPA3: newest option. Better protection against password guessing and safer on public Wi-Fi.
- Passwords matter: even strong standards fail with short or reused passphrases.

Red flags

- Your network shows WEP or Open in Wi-Fi details.
- Router set to WPA/WPA2 (TKIP) instead of WPA2-PSK (AES) or WPA3-Personal.
- Short Wi-Fi password or the default from the sticker never changed.
- Very old router with no firmware updates available.

Do it right

- Use WPA3-Personal if supported. If not, choose WPA2-PSK (AES). Avoid WEP and TKIP.
- Set a long passphrase: at least 14-16 characters, mix words and numbers.
- Change the router’s admin password and update firmware.
- Turn off WPS push-button/pin. Create a guest network for visitors and smart devices.
- Replace aging routers that can’t do WPA2-AES or WPA3.