

Co je WPA2

Poslední aktualizace 2 března, 2026

WPA2 (*Wi-Fi Protected Access 2*) je bezpečnostní standard pro bezdrátové sítě Wi-Fi, který byl uveden v roce 2004 jako nástupce původního WPA. Více než deset let byl nejrozšířenějším způsobem zabezpečení Wi-Fi sítí a stále ho používá mnoho domácích i firemních routerů.

WPA2 chrání bezdrátovou komunikaci mezi routerem a zařízeními pomocí šifrování. Pokud máte Wi-Fi síť s heslem a váš router je nastavený na WPA2, data putující přes síť jsou chráněná proti odposlouchávání.

Jak WPA2 funguje

WPA2 využívá šifrovací protokol **AES (Advanced Encryption Standard)**, který byl v době svého zavedení považován za velmi bezpečný. Na rozdíl od původního WPA tak poskytuje výrazně silnější ochranu dat.

Existují dvě varianty WPA2:

- **WPA2-Personal (PSK)** – určeno pro domácnosti a menší firmy, zabezpečení pomocí sdíleného hesla.
- **WPA2-Enterprise** – určeno pro větší organizace, využívá ověřování přes [server](#) (RADIUS) a poskytuje vyšší úroveň zabezpečení.

Slabiny WPA2

I když je WPA2 mnohem bezpečnější než původní WPA, časem se ukázalo, že má své slabiny. Nejznámější je tzv. **útok KRACK (Key Reinstallation Attack)** z roku 2017, který umožnil útočnickům prolomit šifrování a získat přístup k síťové komunikaci.

Pro běžného uživatele to znamená, že WPA2 sice stále poskytuje solidní ochranu, ale již není tak spolehlivé jako modernější [WPA3](#).

WPA2 vs. WPA3

Rozdíl mezi WPA2 a WPA3 je podobný jako rozdíl mezi starým a novým bezpečnostním

zámkem. WPA2 stále funguje a chrání, ale WPA3 má silnější „mechanismus“, který je odolnější proti novým typům útoků.

WPA2	WPA3
Starší standard, rozšířený od roku 2004	Nejnovější standard z roku 2018
Šifrování AES (128 bitů)	Silnější šifrování AES (256 bitů) a protokol SAE
Zranitelný vůči některým útokům (např. KRACK)	Odolnější proti hádání hesel a slovníkovým útokům
Stále široce podporovaný i na starších zařízeních	Postupně se stává novým doporučeným standardem

Co to znamená pro běžného uživatele

Pokud váš router podporuje jen WPA2, síť je stále relativně dobře chráněná – zejména pokud používáte **silné heslo**. Přesto byste měli myslet na to, že WPA2 je zastaralé a časem přestane být doporučované.

- Pokud to zařízení umožňuje, přepněte zabezpečení na WPA3.
- V případě, že máte pouze WPA2, nastavte **dlouhé a složité heslo**, aby bylo těžší na prolomení.
- Pravidelně aktualizujte firmware routeru – výrobci často opravují známé slabiny.
- Využívejte také další bezpečnostní prvky, např. vestavěný [firewall](#), který chrání síť před nevyžádaným provozem zvenčí.