

WHAT A VPN ACTUALLY DOES. AND WHAT IT DOESN'T.

THE CLAIM: "A VPN makes you completely anonymous online."

THE REALITY: FALSE. A VPN hides your IP and encrypts your traffic, but your browser fingerprint, login cookies, and account activity still identify you. True anonymity takes far more than a VPN subscription.

THE CLAIM: "Free VPNs are just as good as paid ones."

THE REALITY: FALSE. Most free VPNs log and sell your browsing data to advertising networks. You're not the customer, you're the product. Stick to audited paid providers.

THE CLAIM: "A VPN protects you from malware and viruses."

THE REALITY: FALSE. A VPN only encrypts your network traffic. It does nothing against malware you download or click. You still need updated software and antivirus.

THE CLAIM: "A VPN protects you on public wifi."

THE REALITY: TRUE. On open networks, others nearby can intercept unencrypted traffic. A VPN prevents this by tunneling your data through an encrypted connection first.

THE CLAIM: "A VPN hides your activity from your ISP."

THE REALITY: TRUE. Your ISP sees a connection to a VPN server, not your actual browsing. Useful in places with ISP-level surveillance or data retention laws.

THE CLAIM: "A VPN protects your passwords."

THE REALITY: FALSE. A VPN protects data in transit, not passwords at rest or ones you type into a phishing site. Use a password manager for that job.

Audited VPNs worth considering: Mullvad (no-logs, accepts cash), ProtonVPN (open-source, Swiss law), ExpressVPN (independently audited).

→ rexcalloway.com/free-tools

Educational content only. Not financial, legal, tax, or professional cybersecurity advice. No professional-client relationship is created. Consult a qualified professional for your specific situation. Full disclaimer at rexcalloway.com/disclaimer.