

Besten kostenlosen VPNs: Experten wählen clever & sicher

Category: Online-Marketing

geschrieben von Tobias Hager | 15. Februar 2026



Besten kostenlosen VPNs: Experten wählen clever & sicher

Du glaubst, mit einem kostenlosen VPN bist du sicher, anonym und surfst wie ein Schatten durch das Netz? Falsch gedacht. Die meisten Gratis-VPNs sind digitale Trockenhauben mit eingebautem Datenleck. Aber keine Sorge: Wir haben das Netz durchkämmt, die Anbieter seziert und die Spreu vom datenschutzkonformen Weizen getrennt. Was du hier bekommst, ist keine

weichgespülte Top-10-Liste, sondern die technisch fundierte, kompromisslos ehrliche Übersicht der besten kostenlosen VPNs, mit denen du wirklich clever und sicher unterwegs bist.

- Was ein VPN technisch macht – und warum du es brauchst, nicht nur willst
- Wie kostenlose VPNs wirklich funktionieren (Spoiler: viele verkaufen deine Daten)
- Unsere Auswahlkriterien: Verschlüsselung, Logging, Geschwindigkeit, Transparenz
- Die besten kostenlosen VPNs 2024 – getestet, geprüft, zerlegt
- Unterschied zwischen Freemium-VPNs und “kostenlos für immer”-Lockangeboten
- Welche Risiken du bei Gratis-VPNs eingehen musst – und wie du sie minimierst
- Warum ein kostenloses VPN nicht gleich ein schlechtes VPN ist
- Technische Empfehlungen für Power-User: Kill Switch, DNS-Leak-Schutz & Co.
- Ein kurzer Blick auf Alternativen: Tor, Proxies, Self-Hosted VPNs
- Fazit: Wann ein kostenloses VPN reicht – und wann du besser bezahlst

Was ein VPN ist – und warum du es (nicht nur in der Theorie) brauchst

Ein VPN – Virtual Private Network – ist keine Magie, sondern ein technisches Konstrukt, das deinen Traffic durch einen verschlüsselten Tunnel zu einem anderen Server leitet. Das Ziel: Deine IP-Adresse verstecken, deine Verbindung absichern und dich vor neugierigen Zwischenstellen (Hallo, ISP!) schützen. Klingt simpel, ist aber komplexer als viele denken.

Technisch gesehen baut ein VPN-Client auf deinem Gerät eine verschlüsselte Verbindung (meist via OpenVPN, WireGuard oder IKEv2/IPSec) zu einem VPN-Server auf. Alles, was du im Internet machst – Surfen, Streamen, Mailen – läuft über diesen Tunnel. Das bedeutet: Deine IP-Adresse wird ersetzt, dein Datenverkehr ist für Provider, Behörden und Hacker nicht mehr direkt lesbar.

Was viele nicht wissen: Ein VPN schützt dich nicht vor allem – aber vor vielem. Es verhindert etwa, dass dein Provider deine DNS-Anfragen mitschneidet, es erschwert Tracking durch Webseiten und kann geo-blockierte Inhalte freischalten. Aber: Ein VPN ersetzt kein Antivirus, keinen gesunden Menschenverstand und schon gar kein solides Datenschutzverhalten.

Warum das relevant ist? Weil kostenlose VPNs oft mit falschen Versprechungen um sich werfen. Anonymität, Sicherheit, Geschwindigkeit – alles gratis. Die Realität ist: Irgendwer muss die Server, das Netzwerk, die Infrastruktur bezahlen. Und bei vielen Gratis-Diensten bist du nicht der Kunde, sondern das Produkt.

Was kostenlose VPNs wirklich taugen – und worauf du achten musst

Der Markt für kostenlose VPNs ist ein Sumpf. Zwischen dubiosen Apps, die deine Daten direkt an Drittfirmen verkaufen, und seriösen Anbietern mit begrenztem Gratis-Modell liegen Welten. Wer sich blindlings ein VPN aus dem App Store lädt, riskiert mehr als nur eine lahme Verbindung. Er riskiert seine Privatsphäre.

Viele kostenlose VPNs finanzieren sich durch Werbung, Datenverkauf oder In-App-Käufe. Besonders kritisch: Logging. Wenn ein Anbieter behauptet, "no logs" zu führen, aber in den AGB steht, dass IP-Adressen, Verbindungszeiten oder Nutzungsverhalten gespeichert werden – dann ist das kein VPN, sondern ein getarnter Überwachungsdienst.

Ein weiteres Problem: Server-Infrastruktur. Gratis-VPNs bieten oft nur eine Handvoll Server in wenigen Ländern. Überlastung, geringe Bandbreite und hohe Latenz sind die Folge. Streaming? Vergiss es. Gaming? Unnutzbar. Selbst normales Browsing kann zur Geduldsprobe werden.

Worauf du achten musst:

- Starke Verschlüsselung (mindestens AES-256, ideal: WireGuard-Protokoll)
- Keine IP- oder DNS-Leaks (testen mit Tools wie IPLeak.net)
- Tatsächliche No-Logs-Policy, idealerweise durch Audits bestätigt
- Transparente Anbieterstruktur (kein Sitz auf den Seychellen mit Briefkastenfirma)
- Kill Switch und DNS-Leak-Schutz als technische Mindestvoraussetzung

Die besten kostenlosen VPNs 2024 – getestet, geprüft, empfohlen

Hier kommt unsere Auswahl der besten kostenlosen VPNs, die du 2024 mit gutem Gewissen nutzen kannst. Kein Bullshit, keine Affiliate-Schönfärberei. Alle Anbieter wurden auf Verschlüsselung, Logging, Geschwindigkeit und Transparenz untersucht. Und ja, sie sind wirklich kostenlos – mit nachvollziehbaren technischen Einschränkungen.

- Proton VPN
Standort: Schweiz
Protokolle: WireGuard, OpenVPN, IKEv2
Kostenloses Modell: unbegrenzt in Datenmenge, aber nur 3 Länder

- Besonderheiten: Open Source Clients, audited No-Logs-Policy, starker Datenschutz
- Windscribe
 - Standort: Kanada
 - Protokolle: WireGuard, OpenVPN
 - Kostenlos: 10 GB/Monat mit E-Mail-Registrierung
 - Besonderheiten: R.O.B.E.R.T Firewall, Split Tunneling, Adblock integriert
- Hide.me
 - Standort: Malaysia
 - Protokolle: WireGuard, OpenVPN, IKEv2
 - Kostenlos: 10 GB/Monat, 5 Länder, keine Registrierung nötig
 - Besonderheiten: IPv6 Support, Port Forwarding, keine Werbung
- Atlas VPN (Free)
 - Standort: USA
 - Protokolle: IPSec/IKEv2
 - Kostenlos: 3 Serverstandorte, begrenzte Geschwindigkeit
 - Besonderheiten: starke App, solide Performance, aber Logging unklar

Diese VPNs bieten solide Basisfunktionen, ohne dich direkt zum Bezahlten zu drängen oder deine Daten zu verschachern. Klar, du bekommst nicht die volle Geschwindigkeit oder alle Features wie bei der Bezahlversion – aber du bekommst ein funktionierendes VPN, das seine Versprechen technisch einlöst.

Technische Features, auf die du bei kostenlosen VPNs nicht verzichten solltest

Ein VPN steht und fällt mit seinen technischen Features. Gerade bei kostenlosen Anbietern musst du genau hinschauen, denn viele sparen nicht nur beim Support, sondern auch bei der Technik. Hier die Features, die ein vertrauenswürdiges Gratis-VPN mindestens bieten sollte:

- Kill Switch: Trennt sofort die Verbindung zum Internet, wenn das VPN ausfällt. Ohne das fliegst du ungeschützt ins Netz.
- DNS-Leak-Schutz: Verhindert, dass DNS-Anfragen an deinen Provider gehen. Ohne das bist du trotz VPN nachvollziehbar.
- IPv6-Support und Schutz: Viele VPNs leaken IPv6-Daten, was deine echte Identität preisgeben kann.
- Split Tunneling: Ermöglicht gezielte App- oder Domain-Ausnahmen für den VPN-Tunnel.
- Multi-Hop: Selten bei kostenlosen VPNs, aber Gold wert: Zwei Server in Reihe für doppelte Verschleierung.

Bonuspunkte gibt's für Open Source-Clients, regelmäßige Sicherheits-Audits und eine funktionierende Desktop-App (nicht nur Mobile). Und bitte: Finger weg von VPNs, die sich nur als Browser-Plugin tarnen. Die lösen keine DNS-Leaks, schützen nicht systemweit und sind oft reine Mogelpackungen.

VPN-Alternativen für Fortgeschrittene – Tor, Proxies & Eigenbau

Ein VPN ist nicht das einzige Werkzeug im Datenschutz-Arsenal. Wer technisch tiefer einsteigen will, findet Alternativen – mit eigenen Vor- und Nachteilen.

Tor: Das Onion-Netzwerk anonymisiert Datenverkehr über mehrere Knoten. Extrem sicher, aber auch extrem langsam. Für Web-Recherche und Whistleblowing top, für Streaming unbrauchbar.

SOCKS5-Proxies: Leiten Traffic einzelner Anwendungen um, bieten aber keine Verschlüsselung. Gut für Geo-Spoofing, schlecht für Datenschutz.

Self-Hosted VPNs: Mit Tools wie WireGuard oder OpenVPN kannst du deinen eigenen VPN-Server aufsetzen. Volle Kontrolle, keine Drittanbieter – aber auch Wartungsaufwand, Serverkosten und Know-how nötig.

Fazit: Wer weiß, was er tut, kann mit Alternativen mehr erreichen. Aber für die meisten Nutzer ist ein solides VPN – auch ein kostenloses – die bessere Wahl. Vorausgesetzt, es ist technisch sauber, transparent und sicher implementiert.

Fazit: Kostenloses VPN – klug gewählt, sicher gesurft

Ein kostenloses VPN kann mehr sein als ein Notbehelf. Wenn du die richtigen Anbieter wählst, technische Features beachtest und deine Erwartungen realistisch hältst, bekommst du Datenschutz, Anonymität und Geo-Flexibilität – ohne einen Cent zu zahlen. Aber: Der Grat zwischen clever und naiv ist schmal.

Wer sich auf windige VPNs mit unklarer Herkunft, fehlender Verschlüsselung oder fragwürdiger Logging-Policy verlässt, riskiert mehr als Tracking – nämlich Identitätsdiebstahl und Datenverkauf. Deshalb gilt: Informieren, prüfen, testen. Die besten kostenlosen VPNs machen vieles richtig – aber nichts ersetzt ein bisschen technisches Verständnis. Willkommen bei 404 – wo Datenschutz nicht bei Werbeversprechen endet.