



Anzeige

VPN unter Android manuell einrichten und empfehlenswerte Apps



Erfahren Sie, wie Sie eine VPN-Verbindung manuell unter Android einrichten und welche Apps sich als Alternative eignen.

Wenn Sie beim Surfen mit Ihrem Handy öfters in fremden WLAN-Netzen unterwegs sind, sollten Sie besondere Vorsicht walten lassen. **Ohne entsprechende Sicherheitsvorkehrungen können unbefugte Dritte dort nämlich ganz leicht Ihre Onlinekommunikation, Browser-Aktivitäten oder Passwörter mitlesen. Damit das nicht passiert, sollten Sie für den Austausch von sensiblen Daten immer ein VPN („Virtual Private Network“) nutzen.** In diesem Beitrag zeigen wir Ihnen, wie Sie mit Hilfe von Bordmitteln VPN auf Ihrem [Android-Smartphone](#) einrichten können. Außerdem stellen wir Ihnen die besten mobilen VPN-Apps im Überblick vor.

- ✓ Ein VPN ist ein in sich geschlossenes Netzwerk, mit dessen Hilfe Daten anonym und verschlüsselt über das Internet versendet werden können.
- ✓ In unsicheren öffentlichen WLANs sollten Sie grundsätzlich immer über eine VPN-Verbindung surfen, damit Hacker Ihren Datenverkehr nicht mitlesen oder manipulieren können.
- ✓ Mit VPN können Sie Geoblocking umgehen, und so auch im Ausland auf Inhalte zugreifen, die mit einer länderspezifischen Sperre versehen sind.

Inhalt [\[Ausblenden\]](#)

1. [So richten Sie manuell eine VPN-Verbindung unter Android ein](#)
 2. [Die besten VPN-Apps für Anroid-Smartphones im Überblick](#)
 - 2.1. [VyprVPN - Verschlüsselungstechnik aus der Schweiz](#)
 - 2.2. [TunnelBear VPN - Bärenstarke Sicherheit trifft auf Komfort](#)
 - 2.3. [CyberGhost - Android VPN für Streaming-Fans](#)
- [Ähnliche Artikel:](#)

1. So richten Sie manuell eine VPN-Verbindung unter Android ein

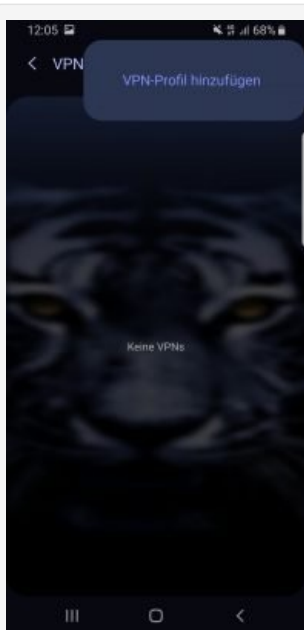
Eine VPN-Verbindung können Sie unter Android auch mit Bordmitteln einrichten. Rufen Sie dazu die Einstellungen Ihres Handys auf und gehen Sie anschließend auf „**Verbindungen**“.

Wählen Sie „**Weitere Verbindungseinstellungen**“ aus und tippen Sie dort auf den Unterpunkt „**VPN**“.



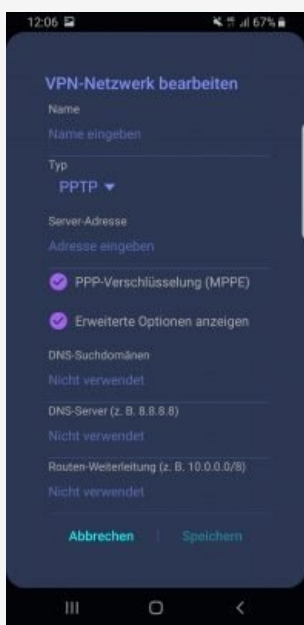
Wählen Sie in den weiteren Verbindungseinstellungen Ihres Smartphones den Unterpunkt VPN aus.

Wenn Sie noch keine VPN-Verbindungen angelegt haben, ist das nächste Fenster leer. Gehen Sie auf das Menü rechts oben und wählen Sie „**VPN-Profil hinzufügen**“ aus.



Fügen Sie über das Menü ein neues VPN-Profil hinzu.

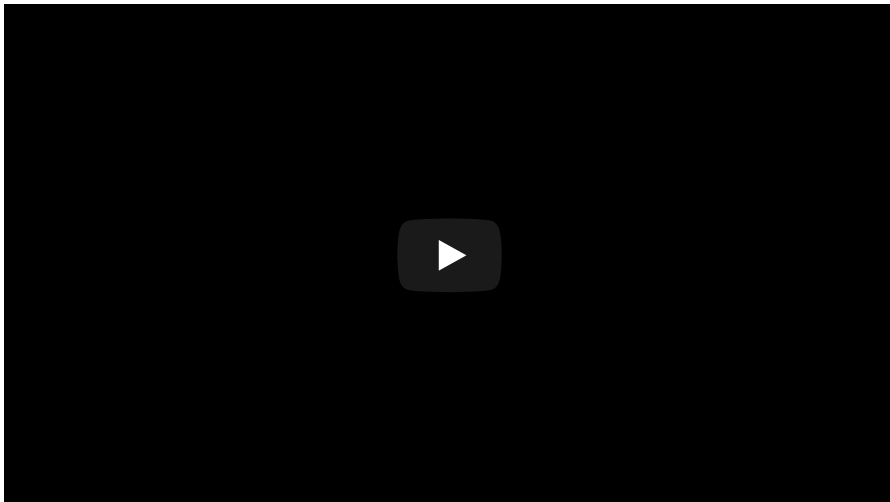
Legen Sie nun einen Namen für Ihre VPN-Verbindung fest und geben Sie die Parameter wie Typ, Serveradresse, IPSec-ID oder den vorinstallierten Schlüssel ein. Diese sind immer vom VPN-Server abhängig. Unter „Erweiterte Optionen“ haben Sie zudem die Möglichkeit, eine DNS-Suchdomäne, einen DNS-Server sowie eine Routen-Weiterleitung zu definieren.



VPN unter Android: Legen Sie die Parameter für Ihre neue Verbindung fest.

1. Geben Sie Ihren Benutzernamen und das Passwort für den VPN-Server ein und klicken Sie auf „**Speichern**“. Wählen Sie „**Kontoinformationen speichern**“ aus, wenn Sie sich nicht bei jedem Login erneut anmelden möchten.
2. Tippen Sie auf „**Verbinden**“ um eine VPN-Verbindung herzustellen. Eine erfolgreiche Einwahl wird über **ein Schlüsselsymbol in der Statusleiste (rechts oben) angezeigt**.
3. Ihr **Datenverkehr ist nun verschlüsselt** und wird über den VPN-Server auf die Webseite oder den jeweiligen Dienst weitergeleitet.

Gut zu wissen: Für die Einrichtung eines neuen VPN-Profiles ist ein sicherer Sperrbildschirm erforderlich. Sollte Sie diesen bisher noch nicht eingerichtet haben, ändern Sie den Typ in „**Muster**“, „**Passwort**“, „**Bioemtrie**“ oder „**PIN**“ und starten Sie den Vorgang erneut.



2. Die besten VPN-Apps für Anroid-Smartphones im Überblick

2.1. VyprVPN - Verschlüsselungstechnik aus der Schweiz



Server in 64 Staaten, ein einzigartiges Verschlüsselungsprotokoll und Sicherheitsstandards nach den strengen Datenschutzgesetzen der Schweiz: **Die technischen Daten von VyprVPN klingen auf den ersten Blick sehr vielversprechend. Besitzer der gesamten Infrastruktur ist das US-Unternehmen Golden Frog GmbH**, das in der Schweiz registriert ist, und durch die dort geltenden Richtlinien einen hundertprozentigen Schutz vor Weiterverwendung oder -verkauf der Nutzerdaten verspricht.

Der VyprVPN Client ist mit Windows, macOS und Linux kompatibel und kann in der mobilen Version auf Android und iOS genutzt werden. Er unterstützt **OpenVPN** und **L2TP** (jeweils unter Verwendung einer 256-Bit-**Verschlüsselung**). Daneben steht mit dem speziell von Golden Frog entwickelten „**Chameleon**“-Protokoll eine weitere Alternative zu Verfügung, mit Hilfe derer Geoblocking (z.B. in

Ländern mit staatlicher Zensur) umgangen werden kann.

2.1.1. Schneller Reagieren durch den integrierten Kill-Switch



Der Kill-Switch stellt sicher, dass Sie auch bei Ausfall der VPN anonym bleiben.

Die Anwendung verfügt außerdem über einen Kill-Switch, der im Falle eines VPN-Ausfalles sofort den gesamten Internetverkehr des Gerätes beendet. Zudem bietet VyprVPN die Möglichkeit, die **VPN-Verbindung automatisch herzustellen**, sobald Sie sich mit einem ungeschützten (öffentlichen) Netzwerk verbinden.

Auch sehr praktisch: Über die [VyprVPN Cloud](#) können Sie bequem sichere Verbindungen zu Cloud-Plattformen wie Amazon Web Services, Virtual Box oder Digital Ocean herstellen.

Für die Nutzung von VyprVPN **benötigen Sie grundsätzlich ein Abo (Es gibt nur eine 3-tägige Testversion)**. Dafür können Sie aus zwei verschiedenen Varianten auswählen:

- Mit dem **Standard-Abo** können Sie die Software auf drei Geräten gleichzeitig betreiben. Dafür werden monatlich 7,95 Euro fällig. Das Jahresabo fällt mit 47,50 Euro (3,95 Euro pro Monat) allerdings deutlich günstiger aus.
- Das **Premium-Abo** erlaubt die parallel Nutzung auf bis zu 5 Endgeräten und beinhaltet darüber hinaus das bereits erwähnte „Chameleon“-Protokoll. Es schlägt mit 10,50 Euro im Monat oder jährlich 65 Euro zu Buche.

Gut zu wissen: Seit Ende 2018 kann VyprVPN noch einen zusätzlichen Pluspunkt in Form eines Sicherheits-Audits durch die Leviathan Security Group vorweisen, das in seinem Abschlussbericht bescheinigt, dass das Nutzerverhalten zu keinem Zeitpunkt aufgezeichnet wird.

Hier finden Sie noch einmal die Vor- und Nachteile im Überblick:

Vorteile

- ✓ Sehr guter Support
- ✓ Server in vielen unterschiedlichen Staaten
- ✓ Eigene Infrastruktur

Nachteile

- ✗ In einigen Staaten nur wenige Server verfügbar
- ✗ Geschwindigkeit teilweise zu gering
- ✗ mittelmäßiges Interface

2.2. TunnelBear VPN - Bärenstarke Sicherheit trifft auf Komfort



Der kanadische Dienst [TunnelBear VPN](#) (gehört seit 2008 zu [McAfee](#)) präsentiert sich **als kompakter Dienst mit plattformübergreifender Kompatibilität und besonders einfachem Handling**. Das Unternehmen hält in 21 Ländern VPN-Server bereit, mit Hilfe derer Sie **anonym Surfen** und **länderspezifische Restriktionen umgehen** können.

Für die Übertragung werden die Daten per 256 Bit-Standard (AES) verschlüsselt und mittels [SSL-Handshake](#) der Zugriff durch

unautorisierte Dritte verhindert. Durch den Firmensitz in Toronto unterliegt TunnelBear der kanadischen Gesetzgebung, wodurch ein gewissenhafter Umgang mit sensiblen Kundendaten garantiert wird.

Das Setup des TunnelBear VPN Client ist dabei denkbar einfach: Mit wenigen Mausklicks werden automatisch alle notwendigen Konfigurationen vorgenommen und gleichzeitig ein Button in der Menüleiste platziert, mit dem sich **schnell und einfach eine Verbindung zu den verfügbaren Servern aufbauen** lässt.

Smartphone- oder **Tablet-**Nutzer profitieren von der **praktischen Weltkarte, auf der sie per Fingertipp den entsprechenden Server für die jeweilige Lokation auswählen können**. Einzelne Server innerhalb eines Ziellandes können leider nicht ausgewählt werden. Auch die grafische Oberfläche von TunnelBear VPN ist äußerst intuitiv gestaltet, daher erfordert die Nutzung keine speziellen IT-Kenntnisse.



Pro Monat stehen Ihnen bei TunnelBear VPN 500 MB Datenvolumen kostenlos zur Verfügung, ein unbegrenztes Volumen gibt es hingegen nur in Form eines monatlichen oder jährlichen Abos. Für 9,99 USD monatlich können Sie Anwendung auf fünf Endgeräten gleichzeitig nutzen, mit rund 60 USD (umgerechnet 4,99 USD im Monat) fahren Sie mit einem Jahresabo aber deutlich günstiger.

Vorteile

- ✓ einfache, intuitive Bedienung
- ✓ AES 256-Bit Verschlüsselung
- ✓ ordentliche Geschwindigkeiten
- ✓ 500 MB Datenvolumen kostenlos

Nachteile

- ✗ In einigen Staaten nur wenige Server verfügbar
- ✗ Keine manuelle Serverauswahl möglich

2.3. CyberGhost - Android VPN für Streaming-Fans



Mit 1200 Servern in über 50 Staaten wartet **CyberGhost VPN** mit einer der umfangreichsten Infrastrukturen auf. **Das Unternehmen mit Standort Bukarest verfolgt eine strikte „No-Logs“-Mentalität und unterliegt zudem den strengen Datenschutzrichtlinien der EU.**

Für die Verbindung mit dem VPN-Knoten werden die Protokolle OpenVPN, L2TP und [IKEv2](#) unterstützt, unter OpenVPN besteht zudem noch die Möglichkeit, manuell von UDP auf TCP zu wechseln. Die Konfiguration kann dabei entweder innerhalb der Software oder direkt im [Router](#) oder in einem alternativen VPN-Programm erfolgen.

CyberGhost VPN nutzt ausschließlich eigene DNS-Server, wodurch DNS-Leaks während der Verbindung unterbunden werden. Als einer der wenigen Dienste bietet es außerdem Funktionen für **ein automatisches Umgehen von Länderrestriktionen** an. Besonders Streaming-Freunde dürften an der großen Serveranzahl von CyberGhost VPN ihre Helle Freude haben. Unterstützt werden Amazon Video, Pandora und Hulu, Netflix hingegen bleibt leider außen vor.

Gut zu wissen: Je mehr Server ein Dienst anbietet, desto geringer ist die Wahrscheinlichkeit, dass diese anhand doppelter [IP-Adressen](#) von den Streaming-Anbietern identifiziert und gesperrt werden können.

Aktuell kostet CyberGhost VPN 11,99 Euro monatlich, wie bei den meisten bezahlpflichtigen Anwendungen können Sie aber auch hier mit einem längerfristigen Abo eine Menge Geld sparen. **Das Jahresabo kostet knapp 64 Euro (5,29 Euro pro Monat), wer sich gleich für 3 Jahre bindet zahlt für den gesamten Zeitraum nur noch 88 Euro (2,45 Euro pro Monat).** Sollten Sie aus irgendeinem Grund nicht zufrieden sein, gewährt das Unternehmen Ihnen gratis eine 45-tägige Geld-zurück-Garantie.

Vorteile

- ✓ große Serveranzahl
- ✓ Anlegen von Nutzerprofilen für verschiedene Anwendungsbereiche möglich
- ✓ No-Log-Mentalität
- ✓ 24/7 Support
- ✓ kann auf sieben Endgeräten gleichzeitig genutzt werden
- ✓ manuelle Serverauswahl- und konfiguration möglich

Nachteile

- ✗ Download-Geschwindigkeit nur mittelmäßig



50 Bewertungen

★★★★☆ Ø 4,10

Ähnliche Artikel:

- [Inkognito surfen - Wie anonym sind Sie tatsächlich?](#)
- [NordVPN Test: So schneidet der Marktführer im Praxistest ab](#)
- [Avast Test 2019: Wie schlägt sich die Internet...](#)
- [Dashlane-Test: Wie gut ist der Passwort-Manager?](#)
- [Kindersicherung im Internet: So bewahren Eltern ihre...](#)
- [Fritzbox unter Windows nutzen - Deutschlands...](#)

Weitere Rubriken: [Android](#),
[Mobil](#)

Plattformen: [Android](#)

Eingetragen am: 02.05.2019

Aktionen: [Aktionen](#) ▼

Please upgrade to a [supported browser](#) to get a reCAPTCHA challenge.

[Why is this happening to me?](#)