**वीपीएन क्या है और यह कैसे काम करता है?**

मूल बातें

एक वीपीएन (वर्चुअल प्राइवेट नेटवर्क) आपके डिवाइस और इंटरनेट के बीच एक सुरक्षित, एन्क्रिप्टेड कनेक्शन बनाता है, जो आपके आईपी एड्रेस को छिपाने के लिए ट्रैफ़िक को एक रिमोट सर्वर से रूट करता है। यह आपके डेटा को हैकर्स, आईएसपी और ट्रैकर्स से बचाता है और गोपनीयता सुनिश्चित करता है। 2025 में, बढ़ते साइबर खतरों, व्यापक डेटा ट्रैकिंग और बढ़ती सामग्री प्रतिबंधों के कारण वीपीएन बेहद महत्वपूर्ण हो गए हैं। ये सार्वजनिक वाई-फ़ाई पर सुरक्षित ब्राउज़िंग, नेटफ्लिक्स लाइब्रेरी जैसी भू-अवरुद्ध सामग्री तक पहुँचने और प्रतिबंधित क्षेत्रों में सेंसरशिप को दरकिनार करने के लिए एकदम सही हैं।

**हमारी सिफारिश: एक्सप्रेसवीपीएन**

4.9/5

94+ देशों में सैन्य-ग्रेड एन्क्रिप्शन और बिजली की गति के साथ उद्योग-अग्रणी वीपीएन।

30-दिन की गारंटी24/7 सहायतानो-लॉग्स नीति5 डिवाइस

🎉 49% की बचत करें + 3 महीने मुफ़्त

ExpressVPN को जोखिम-मुक्त आज़माएं

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**क्या VPN का उपयोग करना कानूनी है?**

कानूनी

संयुक्त राज्य अमेरिका, कनाडा, ब्रिटेन और अधिकांश यूरोपीय देशों सहित दुनिया भर के अधिकांश देशों में वीपीएन कानूनी हैं। हालाँकि, चीन, रूस और ईरान जैसे कुछ देशों में वीपीएन के उपयोग पर प्रतिबंध या प्रतिबन्ध हैं। वीपीएन का उपयोग करने से पहले हमेशा स्थानीय कानूनों की जाँच करें।

संबंधित मार्गदर्शिकाएँ:

[देश के अनुसार VPN कानून गाइड](https://bestvpn.digital/guides/vpn-laws-by-country)

[विभिन्न देशों और क्षेत्रों में VPN की वैधता के लिए संपूर्ण मार्गदर्शिका](https://bestvpn.digital/guides/vpn-laws-by-country)

[कानूनी वीपीएन उपयोग युक्तियाँ](https://bestvpn.digital/guides/legal-vpn-usage)

[VPN का कानूनी और ज़िम्मेदारी से उपयोग करने के सर्वोत्तम तरीके](https://bestvpn.digital/guides/legal-vpn-usage)

**हमारी सिफारिश: नॉर्डवीपीएन**

4.8/5

उन्नत सुरक्षा सुविधाओं और वैश्विक सर्वर नेटवर्क के साथ ऑडिटेड नो-लॉग्स वीपीएन।

डबल VPNCyberSecKill स्विच6 डिवाइस

🎉 68% की बचत करें + 3 महीने मुफ़्त

अभी NordVPN प्राप्त करें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**क्या VPN इंटरनेट की गति को धीमा कर देते हैं?**

प्रदर्शन

एन्क्रिप्शन ओवरहेड और वीपीएन सर्वरों के माध्यम से डेटा की अतिरिक्त दूरी के कारण वीपीएन इंटरनेट की गति को कम कर सकते हैं। हालाँकि, प्रीमियम वीपीएन आमतौर पर न्यूनतम गति हानि (5-15%) का कारण बनते हैं, और कुछ आईएसपी थ्रॉटलिंग को बायपास करके गति में सुधार भी कर सकते हैं।

संबंधित मार्गदर्शिकाएँ:

[वीपीएन स्पीड टेस्ट के परिणाम](https://bestvpn.digital/guides/vpn-speed-tests)

[शीर्ष VPN प्रदाताओं की तुलना में वास्तविक गति परीक्षण](https://bestvpn.digital/guides/vpn-speed-tests)

[वीपीएन स्पीड को कैसे अनुकूलित करें](https://bestvpn.digital/guides/optimize-vpn-speed)

[अपने VPN कनेक्शन की गति को अधिकतम करने के लिए सुझाव और तरकीबें](https://bestvpn.digital/guides/optimize-vpn-speed)

**हमारी सिफारिश: सर्फशार्क**

4.7/5

अधिकतम गति और सुरक्षा के लिए वायरगार्ड प्रोटोकॉल के साथ असीमित डिवाइस।

असीमित डिवाइसवायरगार्डक्लीनवेबमल्टीहॉप

🎉 82% की बचत करें + 2 महीने मुफ़्त

सर्फशार्क से शुरुआत करें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**क्या मैं नेटफ्लिक्स, हुलु और अन्य सेवाओं की स्ट्रीमिंग के लिए वीपीएन का उपयोग कर सकता हूं?**

स्ट्रीमिंग

कई वीपीएन स्ट्रीमिंग प्लेटफ़ॉर्म पर भू-प्रतिबंधित सामग्री तक पहुँच प्रदान करते हैं, लेकिन सभी वीपीएन हर स्ट्रीमिंग सेवा के साथ विश्वसनीय रूप से काम नहीं करते। ऐसे वीपीएन की तलाश करें जो विशेष रूप से स्ट्रीमिंग क्षमताओं का विज्ञापन करते हों और जिनके सर्वर लोकप्रिय प्लेटफ़ॉर्म के लिए अनुकूलित हों।

संबंधित मार्गदर्शिकाएँ:

[नेटफ्लिक्स के लिए सर्वश्रेष्ठ वीपीएन](https://bestvpn.digital/guides/best-vpns-for-netflix)

[शीर्ष VPN सेवाएँ जो Netflix सामग्री को विश्वसनीय रूप से अनब्लॉक करती हैं](https://bestvpn.digital/guides/best-vpns-for-netflix)

[नेटफ्लिक्स वीपीएन सेटअप गाइड](https://bestvpn.digital/guides/netflix-vpn-setup)

[VPN के साथ Netflix स्ट्रीमिंग के लिए चरण-दर-चरण मार्गदर्शिका](https://bestvpn.digital/guides/netflix-vpn-setup)

**हमारी सिफारिश: एक्सप्रेसवीपीएन**

4.9/5

अनुकूलित स्ट्रीमिंग सर्वर और 4K समर्थन के साथ नेटफ्लिक्स के लिए सर्वश्रेष्ठ वीपीएन।

नेटफ्लिक्स अनब्लॉकिंग4K स्ट्रीमिंगस्मार्ट DNSराउटर सपोर्ट

🎉 49% की बचत करें + 3 महीने मुफ़्त

ExpressVPN के साथ Netflix स्ट्रीम करें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**निःशुल्क और सशुल्क VPN में क्या अंतर है?**

मूल्य निर्धारण

मुफ़्त वीपीएन में आमतौर पर सीमित सर्वर, धीमी गति, डेटा सीमा और कम सुरक्षा सुविधाएँ होती हैं। वे उपयोगकर्ता डेटा लॉग भी कर सकते हैं या विज्ञापन दिखा सकते हैं। सशुल्क वीपीएन बेहतर सुरक्षा, तेज़ गति, ज़्यादा सर्वर और नो-लॉग गारंटी के साथ मज़बूत गोपनीयता नीतियाँ प्रदान करते हैं।

संबंधित मार्गदर्शिकाएँ:

[वायरगार्ड बनाम ओपनवीपीएन तुलना](https://bestvpn.digital/guides/wireguard-vs-openvpn)

[दो सबसे लोकप्रिय VPN प्रोटोकॉल की विस्तृत तुलना](https://bestvpn.digital/guides/wireguard-vs-openvpn)

[वीपीएन प्रोटोकॉल सुरक्षा गाइड](https://bestvpn.digital/guides/vpn-protocol-security)

[विभिन्न VPN प्रोटोकॉल और उनकी सुरक्षा विशेषताओं को समझना](https://bestvpn.digital/guides/vpn-protocol-security)

**हमारी सिफारिश: नॉर्डवीपीएन**

4.8/5

इष्टतम प्रदर्शन के लिए नॉर्डलिंक्स (वायरगार्ड) सहित उन्नत प्रोटोकॉल चयन।

नॉर्डलिंक्स प्रोटोकॉलओपनवीपीएनआईकेईवी2कस्टम प्रोटोकॉल

🎉 68% की बचत करें + 3 महीने मुफ़्त

नॉर्डवीपीएन प्रोटोकॉल चुनें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**मैं कितने डिवाइस को VPN से कनेक्ट कर सकता हूँ?**

उपकरण

यह प्रदाता के अनुसार अलग-अलग होता है। कुछ वीपीएन 5-10 एक साथ कनेक्शन की अनुमति देते हैं, जबकि सर्फशार्क और आईपीवीनिश जैसे अन्य असीमित कनेक्शन प्रदान करते हैं। अगर आपके पास कई डिवाइस हैं, तो वीपीएन चुनने से पहले डिवाइस की सीमा की जाँच कर लें।

**हमारी सिफारिश: साइबरघोस्ट**

4.6/5

एक-क्लिक कनेक्शन और अनुकूलित सर्वर के साथ उपयोगकर्ता-अनुकूल मोबाइल ऐप।

आसान मोबाइल ऐप्सऑटो-कनेक्ट7 डिवाइस45-दिन की गारंटी

🎉 84% की बचत करें + 4 महीने मुफ़्त

साइबरघोस्ट मोबाइल प्राप्त करें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**नो-लॉग्स वीपीएन नीति क्या है?**

गोपनीयता

नो-लॉग्स नीति का अर्थ है कि वीपीएन प्रदाता आपकी ऑनलाइन गतिविधियों, कनेक्शन समय, आईपी पते या ब्राउज़िंग इतिहास के बारे में कोई भी जानकारी रिकॉर्ड या संग्रहीत नहीं करता है। यह आपकी गोपनीयता सुनिश्चित करता है, भले ही वीपीएन कंपनी के साथ कोई समझौता हो या उसे कानूनी रूप से डेटा साझा करने के लिए बाध्य किया गया हो।

**हमारी सिफारिश: सर्फशार्क**

4.7/5

असीमित डिवाइस और सभी सुविधाओं के साथ सबसे सस्ती प्रीमियम वीपीएन।

असीमित डिवाइससभी सुविधाएँ30-दिन की गारंटी24/7 सहायता

🎉 82% की बचत करें + 2 महीने मुफ़्त

सर्वश्रेष्ठ VPN डील प्राप्त करें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**मुझे कौन सा VPN प्रोटोकॉल उपयोग करना चाहिए?**

तकनीकी

सबसे अच्छे प्रोटोकॉल वायरगार्ड (सबसे तेज़ और सबसे आधुनिक), ओपनवीपीएन (सबसे सुरक्षित और व्यापक रूप से समर्थित), और आईकेईवी2 (मोबाइल के लिए बेहतरीन) हैं। पीपीटीपी से बचें क्योंकि यह पुराना और असुरक्षित है। ज़्यादातर उपयोगकर्ताओं को उपलब्ध होने पर वायरगार्ड चुनना चाहिए।

संबंधित मार्गदर्शिकाएँ:

[टोरेंटिंग के लिए सर्वश्रेष्ठ वीपीएन](https://bestvpn.digital/guides/best-vpns-for-torrenting)

[पोर्ट फ़ॉरवर्डिंग समर्थन वाली शीर्ष P2P-अनुकूल VPN सेवाएँ](https://bestvpn.digital/guides/best-vpns-for-torrenting)

[सुरक्षित टोरेंटिंग गाइड](https://bestvpn.digital/guides/safe-torrenting-guide)

[VPN के साथ सुरक्षित और गुमनाम तरीके से टोरेंट कैसे करें](https://bestvpn.digital/guides/safe-torrenting-guide)

**हमारी सिफारिश: एक्सप्रेसवीपीएन**

4.9/5

सुरक्षित टोरेंटिंग के लिए पोर्ट फॉरवर्डिंग और सख्त नो-लॉग्स नीति के साथ पी2पी-अनुकूलित सर्वर।

P2P सर्वरपोर्ट फ़ॉरवर्डिंगकिल स्विचकोई लॉग ऑडिट नहीं किया गया

🎉 49% की बचत करें + 3 महीने मुफ़्त

ExpressVPN के साथ सुरक्षित रूप से टोरेंट करें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**क्या मैं अपने राउटर पर VPN का उपयोग कर सकता हूँ?**

तकनीकी

हाँ, कई VPN प्रदाता राउटर इंस्टॉलेशन का समर्थन करते हैं, जो आपके नेटवर्क पर सभी डिवाइस की सुरक्षा करता है। आपको एक संगत राउटर की आवश्यकता होगी जो VPN क्लाइंट का समर्थन करता हो, या आप एक पूर्व-कॉन्फ़िगर किया हुआ VPN राउटर खरीद सकते हैं। यह डिवाइस सीमाओं के लिए एक कनेक्शन के रूप में गिना जाता है।

संबंधित मार्गदर्शिकाएँ:

[वीपीएन किल स्विच की व्याख्या](https://bestvpn.digital/guides/vpn-kill-switch-guide)

[VPN किल स्विच और वे आपकी सुरक्षा कैसे करते हैं, इसकी पूरी गाइड](https://bestvpn.digital/guides/vpn-kill-switch-guide)

[वीपीएन सुरक्षा सुविधाएँ](https://bestvpn.digital/guides/vpn-security-features)

[VPN सेवा में देखने योग्य आवश्यक सुरक्षा सुविधाएँ](https://bestvpn.digital/guides/vpn-security-features)

**हमारी सिफारिश: नॉर्डवीपीएन**

4.8/5

उन्नत किल स्विच तकनीक जो VPN के डिस्कनेक्ट होने पर तुरन्त इंटरनेट ब्लॉक कर देती है।

ऐप किल स्विचसिस्टम किल स्विचऑटो-रीकनेक्टDNS लीक सुरक्षा

🎉 68% की बचत करें + 3 महीने मुफ़्त

नॉर्डवीपीएन किल स्विच के साथ सुरक्षित रहें

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**क्या मुझे मोबाइल डिवाइस के लिए VPN की आवश्यकता है?**

गतिमान

हाँ, मोबाइल वीपीएन सार्वजनिक वाई-फ़ाई पर आपके डेटा की सुरक्षा, मोबाइल ट्रैकिंग को रोकने और भू-प्रतिबंधित सामग्री तक पहुँच के लिए महत्वपूर्ण हैं। अधिकांश वीपीएन प्रदाता आईओएस और एंड्रॉइड के लिए डेस्कटॉप संस्करणों के समान सुरक्षा सुविधाओं वाले समर्पित मोबाइल ऐप प्रदान करते हैं।

संबंधित मार्गदर्शिकाएँ:

[मुफ़्त बनाम सशुल्क वीपीएन तुलना](https://bestvpn.digital/guides/free-vs-paid-vpn)

[मुफ़्त विकल्पों की तुलना में सशुल्क VPN निवेश के लायक क्यों हैं?](https://bestvpn.digital/guides/free-vs-paid-vpn)

[वीपीएन परीक्षण और धन-वापसी गारंटी](https://bestvpn.digital/guides/vpn-trials-guarantees)

[परीक्षण अवधि के साथ प्रीमियम वीपीएन को जोखिम-मुक्त कैसे आज़माएँ](https://bestvpn.digital/guides/vpn-trials-guarantees)

**हमारी सिफारिश: साइबरघोस्ट**

4.6/5

45 दिन की मनी-बैक गारंटी के साथ प्रीमियम वीपीएन - किसी भी निःशुल्क परीक्षण से अधिक।

45-दिन की गारंटी, कोई डेटा सीमा नहीं, सभी सुविधाएँ, 7 डिवाइस

🎉 84% की बचत करें + 4 महीने मुफ़्त

साइबरघोस्ट को जोखिम-मुक्त आज़माएं

30-दिन की मनी-बैक गारंटी • नो-लॉग्स नीति • 24/7 सहायता

**स्प्लिट टनलिंग क्या है?**

विशेषताएँ

स्प्लिट टनलिंग आपको अपने कुछ इंटरनेट ट्रैफ़िक को VPN के ज़रिए रूट करने की सुविधा देती है, जबकि बाकी ट्रैफ़िक को सीधे इंटरनेट एक्सेस करने की सुविधा देती है। यह संवेदनशील गतिविधियों के लिए VPN सुरक्षा बनाए रखते हुए स्थानीय सेवाओं तक पहुँचने के लिए उपयोगी है।

**मैं सर्वोत्तम VPN सर्वर स्थान का चयन कैसे करूं?**

प्रयोग

**किल स्विच क्या है और मुझे इसकी आवश्यकता क्यों है?**

सुरक्षा

अगर वीपीएन कनेक्शन अचानक टूट जाता है, तो किल स्विच आपके इंटरनेट कनेक्शन को अपने आप काट देता है। यह आपके असली आईपी एड्रेस और अनएन्क्रिप्टेड डेटा को सार्वजनिक होने से रोकता है। यह गोपनीयता और सुरक्षा बनाए रखने के लिए ज़रूरी है।

**क्या VPN का पता लगाया जा सकता है?**

गोपनीयता

हाँ, कभी-कभी वीपीएन का पता आईपी ब्लैकलिस्ट, डीप पैकेट इंस्पेक्शन और व्यवहार विश्लेषण सहित विभिन्न तरीकों से लगाया जा सकता है। कुछ वीपीएन वीपीएन उपयोग को छिपाने के लिए अस्पष्टीकरण सुविधाएँ प्रदान करते हैं, जिससे पता लगाना बहुत मुश्किल हो जाता है।

**क्या VPN का उपयोग करने में कोई जोखिम है?**

सुरक्षा

जोखिमों में डेटा लॉग करने वाले अविश्वसनीय प्रदाता को चुनना, नकली वीपीएन ऐप्स में मैलवेयर, धीमी इंटरनेट स्पीड और कुछ सेवाओं के साथ संभावित असंगति शामिल हैं। हमेशा विश्वसनीय, ऑडिट किए गए वीपीएन प्रदाताओं को चुनें जिनकी गोपनीयता नीतियाँ मज़बूत हों।

**मुझे VPN के लिए कितना भुगतान करना चाहिए?**

मूल्य निर्धारण

उच्च-गुणवत्ता वाले वीपीएन की कीमत आमतौर पर $2-12 प्रति माह होती है, जबकि लंबी अवधि के सब्सक्रिप्शन बेहतर मूल्य प्रदान करते हैं। $2 प्रति माह से कम कीमत सुरक्षा या सुविधाओं में समझौता का संकेत हो सकती है। बचत के लिए वार्षिक प्लान पर विचार करें, लेकिन सेवा का परीक्षण करने के लिए छोटी अवधि से शुरुआत करें।

**क्या मैं टोरेंटिंग के लिए VPN का उपयोग कर सकता हूँ?**

पी2पी

कई VPN, P2P ट्रैफ़िक और टोरेंटिंग का समर्थन करते हैं, लेकिन सभी नहीं। समर्पित P2P सर्वर, मज़बूत एन्क्रिप्शन, नो-लॉग पॉलिसी और किल स्विच वाले VPN देखें। कुछ प्रदाता विशेष रूप से टोरेंटिंग की अनुमति देते हैं जबकि अन्य इसे प्रतिबंधित करते हैं।

**वीपीएन और प्रॉक्सी में क्या अंतर है?**

तुलना

वीपीएन आपके सभी इंटरनेट ट्रैफ़िक को एन्क्रिप्ट करते हैं और पूरे सिस्टम में काम करते हैं, जबकि प्रॉक्सी केवल विशिष्ट एप्लिकेशन से आने वाले ट्रैफ़िक को बिना एन्क्रिप्शन के रीडायरेक्ट करते हैं। वीपीएन, प्रॉक्सी की तुलना में कहीं बेहतर सुरक्षा और गोपनीयता प्रदान करते हैं।

**क्या चीन में VPN काम करते हैं?**

सेंसरशिप

चीन में VPN का इस्तेमाल प्रतिबंधित है, और ग्रेट फ़ायरवॉल कई VPN सेवाओं को ब्लॉक कर देता है। कुछ VPN अभी भी विशेष ऑबफस्केशन तकनीक के साथ काम करते हैं, लेकिन उनकी विश्वसनीयता अनिश्चित हो सकती है। वर्तमान रिपोर्ट देखें और सिद्ध चीन बाईपास क्षमताओं वाले VPN चुनें।

**क्या मैं VPN के साथ एक समर्पित IP प्राप्त कर सकता हूँ?**

विशेषताएँ

हाँ, कुछ वीपीएन प्रदाता अतिरिक्त शुल्क पर समर्पित/स्थिर आईपी पते प्रदान करते हैं। इससे आपको हर बार कनेक्ट होने पर एक ही आईपी पता मिलता है, जो आईपी-प्रतिबंधित सेवाओं तक पहुँचने या कैप्चा से बचने के लिए उपयोगी हो सकता है।

**मैं कैसे जांचूं कि मेरा VPN काम कर रहा है या नहीं?**

परीक्षण

कनेक्ट होने से पहले और बाद में अपने आईपी पते की जाँच करें ताकि यह सुनिश्चित हो सके कि वह बदल रहा है। ऑनलाइन टूल का उपयोग करके DNS लीक की जाँच करें, सत्यापित करें कि आपका स्थान VPN सर्वर स्थान के रूप में दिखाई दे रहा है, और VPN को डिस्कनेक्ट करके किल स्विच के काम करने की पुष्टि करें।

**यदि मैं अपना VPN चालू करना भूल जाऊं तो क्या होगा?**

प्रयोग

आपका असली आईपी पता और लोकेशन दिखाई देगा, आपका आईएसपी आपका ट्रैफ़िक देख सकेगा, और आपको वीपीएन सुरक्षा नहीं मिलेगी। कुछ वीपीएन ऑटो-कनेक्ट सुविधाएँ प्रदान करते हैं जो इंटरनेट या अविश्वसनीय नेटवर्क से कनेक्ट होने पर वीपीएन को स्वचालित रूप से शुरू कर देती हैं।

**क्या नियोक्ता VPN के माध्यम से मेरी इंटरनेट गतिविधि देख सकते हैं?**

गोपनीयता

अगर आप कंपनी के उपकरण या नेटवर्क का इस्तेमाल कर रहे हैं, तो नियोक्ता आपकी गतिविधियों पर एंडपॉइंट मॉनिटरिंग सॉफ़्टवेयर जैसे अन्य तरीकों से नज़र रख सकते हैं, यहाँ तक कि VPN के साथ भी। निजी उपकरणों पर पर्सनल VPN, नियोक्ता की निगरानी से बेहतर गोपनीयता प्रदान करते हैं।

**यदि मेरे पास VPN है तो क्या मुझे एंटीवायरस की आवश्यकता है?**

सुरक्षा

वीपीएन और एंटीवायरस अलग-अलग उद्देश्यों की पूर्ति करते हैं। वीपीएन गोपनीयता और डेटा की सुरक्षा करते हैं, जबकि एंटीवायरस मैलवेयर और दुर्भावनापूर्ण फ़ाइलों से सुरक्षा प्रदान करते हैं। व्यापक सुरक्षा के लिए आपको दोनों का उपयोग करना चाहिए - ये एक-दूसरे के पूरक हैं।

**डबल वीपीएन या मल्टी-हॉप क्या है?**

विकसित

डबल वीपीएन आपके ट्रैफ़िक को एक के बजाय दो वीपीएन सर्वरों के ज़रिए रूट करता है, जिससे एन्क्रिप्शन की एक अतिरिक्त परत जुड़ जाती है और आपकी ऑनलाइन गतिविधि का पता लगाना बेहद मुश्किल हो जाता है। हालाँकि, इससे स्पीड काफ़ी कम हो जाती है और ज़्यादातर यूज़र्स के लिए यह ज़रूरत से ज़्यादा हो जाता है।

**क्या मैं स्मार्ट टीवी के साथ VPN का उपयोग कर सकता हूँ?**

उपकरण

हाँ, आप अपने राउटर पर वीपीएन इंस्टॉल करके, अपने कंप्यूटर से वीपीएन कनेक्शन शेयर करके, या वीपीएन-सक्षम फायर स्टिक/ऐप्पल टीवी का इस्तेमाल करके स्मार्ट टीवी के साथ वीपीएन का इस्तेमाल कर सकते हैं। कुछ स्मार्ट टीवी सीधे वीपीएन ऐप्स को भी सपोर्ट करते हैं।

**वीपीएन में अस्पष्टीकरण क्या है?**

विकसित

ऑबफस्केशन वीपीएन ट्रैफ़िक को छिपाकर उसे सामान्य HTTPS ट्रैफ़िक जैसा बना देता है, जिससे प्रतिबंधित देशों या नेटवर्क में वीपीएन ब्लॉक को बायपास करने में मदद मिलती है। इसे स्टील्थ मोड भी कहा जाता है और यह इंटरनेट सेंसरशिप वाले देशों में उपयोगी है।

**मुझे कितनी बार VPN सर्वर बदलना चाहिए?**

प्रयोग

कोई निश्चित नियम नहीं है, लेकिन अगर आपको धीमी गति का अनुभव हो रहा है, या जिस सेवा तक आप पहुँचने का प्रयास कर रहे हैं, उसके कारण सर्वर अवरुद्ध है, या अतिरिक्त गोपनीयता के लिए समय-समय पर आपको सर्वर बदलना पड़ सकता है। कई उपयोगकर्ता कुछ पसंदीदा सर्वर चुन लेते हैं और उन्हीं पर टिके रहते हैं।

**क्या मैं गेमिंग के लिए VPN का उपयोग कर सकता हूँ?**

जुआ

गेमिंग के लिए VPN का इस्तेमाल कुछ सर्वरों पर पिंग कम करने, भौगोलिक प्रतिबंधों को दरकिनार करने, DDoS हमलों से बचने, या अलग-अलग क्षेत्रों में गेम को जल्दी एक्सेस करने के लिए किया जा सकता है। हालाँकि, VPN से विलंबता बढ़ सकती है, इसलिए गेम सर्वर के पास वाले सर्वर चुनें।

**DNS लीक क्या है और मैं इसे कैसे रोक सकता हूँ?**

सुरक्षा

DNS लीक तब होता है जब आपके DNS अनुरोध VPN टनल को बायपास कर देते हैं, जिससे आपकी ब्राउज़िंग गतिविधि आपके ISP को पता चल जाती है। अंतर्निहित DNS लीक सुरक्षा वाले VPN का उपयोग करके, अपनी DNS सेटिंग्स बदलकर, या VPN के DNS सर्वर का उपयोग करके इसे रोकें।

**क्या विशेष रूप से व्यवसायों के लिए VPN उपलब्ध हैं?**

व्यापार

हाँ, बिज़नेस वीपीएन केंद्रीकृत प्रबंधन, समर्पित आईपी पते, टीम खाते, एक साथ कनेक्शन में वृद्धि और एंटरप्राइज़-स्तरीय सुरक्षा जैसी सुविधाएँ प्रदान करते हैं। इनकी कीमत आमतौर पर ज़्यादा होती है, लेकिन ये बेहतर नियंत्रण और समर्थन प्रदान करते हैं।

**IPv6 क्या है और क्या VPN इसका समर्थन करते हैं?**

तकनीकी

IPv6, IPv4 की जगह लेने वाला नया इंटरनेट प्रोटोकॉल है। सभी VPN IPv6 का समर्थन नहीं करते, जिससे IPv6 लीक हो सकता है। ऐसे VPN खोजें जो या तो IPv6 का समर्थन करते हों या लीक को रोकने के लिए IPv6 ट्रैफ़िक को ब्लॉक करते हों, क्योंकि अधिकांश उपयोगकर्ता अभी भी मुख्य रूप से IPv4 का ही उपयोग करते हैं।

**क्या मैं अपना स्वयं का VPN सर्वर स्थापित कर सकता हूँ?**

DIY

हाँ, आप AWS या DigitalOcean जैसी क्लाउड सेवाओं का उपयोग करके, या अपने होम राउटर पर एक निजी VPN सर्वर स्थापित कर सकते हैं। हालाँकि, इससे आपको ISP से गोपनीयता मिलती है, लेकिन गुमनामी नहीं, क्योंकि सर्वर आपसे जुड़ा होता है। व्यावसायिक VPN बेहतर गुमनामी प्रदान करते हैं।

**वायरगार्ड क्या है और यह लोकप्रिय क्यों है?**

तकनीकी

वायरगार्ड एक आधुनिक वीपीएन प्रोटोकॉल है जो ओपनवीपीएन जैसे पुराने प्रोटोकॉल की तुलना में तेज़, ज़्यादा सुरक्षित और कम बैटरी खपत करता है। इसका कोड सरल है (जिससे ऑडिट करना आसान हो जाता है), बेहतर प्रदर्शन है, और यह कई वीपीएन प्रदाताओं के लिए पसंदीदा विकल्प बनता जा रहा है।

**क्या VPN मैलवेयर से सुरक्षा प्रदान करते हैं?**

सुरक्षा

वीपीएन मुख्य रूप से एन्क्रिप्शन के ज़रिए ट्रांज़िट के दौरान डेटा की सुरक्षा करते हैं, मैलवेयर से नहीं। हालाँकि, कुछ वीपीएन में विज्ञापन अवरोधक, मैलवेयर सुरक्षा और खतरनाक वेबसाइट ब्लॉकिंग जैसी अतिरिक्त सुरक्षा सुविधाएँ भी शामिल होती हैं। आपको अलग से एंटीवायरस सुरक्षा की भी आवश्यकता होगी।

**क्या मैं सस्ती ऑनलाइन कीमतें पाने के लिए वीपीएन का उपयोग कर सकता हूं?**

खरीदारी

कुछ ऑनलाइन सेवाएँ स्थान के आधार पर अलग-अलग कीमतें दिखाती हैं, इसलिए अपना वीपीएन सर्वर बदलने पर अलग कीमतें दिखाई दे सकती हैं। हालाँकि, यह सेवा की शर्तों का उल्लंघन हो सकता है, और भुगतान विधियाँ अक्सर आपके वास्तविक स्थान का ही खुलासा करती हैं।

**शुरुआती लोगों के लिए सबसे अच्छा वीपीएन कौन सा है?**

सिफारिशों

शुरुआती लोगों के लिए उपयुक्त वीपीएन में इस्तेमाल में आसान ऐप्स, विश्वसनीय कनेक्शन, अच्छा ग्राहक समर्थन और स्पष्ट गोपनीयता नीतियाँ होनी चाहिए। एक्सप्रेसवीपीएन, नॉर्डवीपीएन और सर्फशार्क अपने उपयोगकर्ता-अनुकूल इंटरफेस के कारण शुरुआती लोगों के लिए लोकप्रिय विकल्प हैं।

**मैं अपनी VPN सदस्यता कैसे रद्द करूं?**

खाता

रद्दीकरण के तरीके प्रदाता के अनुसार अलग-अलग होते हैं। ज़्यादातर प्रदाता आपके खाते के डैशबोर्ड के माध्यम से रद्दीकरण की अनुमति देते हैं, जबकि कुछ के लिए ग्राहक सहायता से संपर्क करना आवश्यक होता है। सदस्यता लेने से पहले रद्दीकरण नीति और धन-वापसी गारंटी की शर्तों की जाँच करें। अपने रद्दीकरण का रिकॉर्ड रखें।

**वीपीएन में पोर्ट फ़ॉरवर्डिंग क्या है?**

विकसित

पोर्ट फ़ॉरवर्डिंग बाहरी कनेक्शनों को VPN कनेक्शन के ज़रिए आपके डिवाइस के विशिष्ट पोर्ट तक पहुँचने की अनुमति देता है। यह सर्वर होस्ट करने, P2P कनेक्शन बेहतर बनाने, या डिवाइस को दूर से एक्सेस करने के लिए उपयोगी है। सभी VPN पोर्ट फ़ॉरवर्डिंग का समर्थन नहीं करते हैं।

**क्या मैं एक साथ कई VPN का उपयोग कर सकता हूँ?**

विकसित

तकनीकी रूप से संभव होते हुए भी, एक साथ कई वीपीएन का उपयोग (वीपीएन चेनिंग) जटिल है, गति को काफ़ी कम कर देता है, और आमतौर पर अनावश्यक भी होता है। अधिकांश उपयोगकर्ताओं की गोपनीयता संबंधी ज़रूरतें एक ही गुणवत्तापूर्ण वीपीएन सेवा से पूरी हो जाती हैं।

**वीपीएन किस बैंडविड्थ का उपयोग करते हैं?**

प्रदर्शन

वीपीएन एन्क्रिप्शन ओवरहेड बढ़ाते हैं, जिससे आमतौर पर बैंडविड्थ उपयोग 5-15% तक बढ़ जाता है। यह सटीक मात्रा इस्तेमाल किए गए प्रोटोकॉल और एन्क्रिप्शन स्तर पर निर्भर करती है। वायरगार्ड का ओवरहेड आमतौर पर ओपनवीपीएन से कम होता है। यदि लागू हो, तो डेटा कैप में इसे शामिल करें।

**क्या ऐसे VPN हैं जिनके लिए पंजीकरण की आवश्यकता नहीं है?**

गोपनीयता

कुछ वीपीएन प्रदाता केवल ईमेल पतों का उपयोग करके गुमनाम पंजीकरण या व्यक्तिगत जानकारी के बिना क्रिप्टोकरेंसी भुगतान की अनुमति देते हैं। हालाँकि, पूरी तरह से पंजीकरण-मुक्त वीपीएन दुर्लभ हैं और इनमें सीमित सुविधाएँ या सुरक्षा हो सकती है।

**वीपीएन ऑडिट क्या है और यह क्यों महत्वपूर्ण है?**

विश्वास

वीपीएन ऑडिट, किसी वीपीएन प्रदाता के सिस्टम, कोड और गोपनीयता प्रथाओं की तृतीय-पक्ष सुरक्षा फर्मों द्वारा की जाने वाली एक स्वतंत्र सुरक्षा समीक्षा है। ऑडिट किए गए वीपीएन अपने सुरक्षा दावों और नो-लॉग्स नीतियों के बारे में अधिक विश्वसनीय आश्वासन प्रदान करते हैं।

**क्या मैं अपने होम नेटवर्क तक दूरस्थ रूप से पहुंचने के लिए VPN का उपयोग कर सकता हूं?**

दूरदराज का उपयोग

हाँ, आप अपने होम राउटर पर एक वीपीएन सर्वर सेट अप कर सकते हैं ताकि आप कहीं से भी अपने होम नेटवर्क को सुरक्षित रूप से एक्सेस कर सकें। यह व्यावसायिक वीपीएन सेवाओं से अलग है और मुख्य रूप से गोपनीयता या गुमनामी के बजाय रिमोट एक्सेस के लिए है।

**यदि कंपनी का कारोबार बंद हो जाए तो मेरे VPN का क्या होगा?**

व्यापार

अगर कोई वीपीएन कंपनी बंद हो जाती है, तो आप तुरंत उसकी सेवाओं का उपयोग खो देंगे। पारदर्शी स्वामित्व और वित्तपोषण वाले स्थापित प्रदाताओं को चुनें। ऐसे वीपीएन चुनें जो लंबी मनी-बैक गारंटी प्रदान करते हों और बहुत लंबी सदस्यता प्रतिबद्धताओं से बचते हों।

**क्या मुझे अलग-अलग गतिविधियों के लिए अलग-अलग VPN की आवश्यकता है?**

प्रयोग

आम तौर पर, एक अच्छा वीपीएन आपकी सभी ज़रूरतों को पूरा कर सकता है। हालाँकि, कुछ उपयोगकर्ता विशिष्ट उद्देश्यों के लिए अलग-अलग वीपीएन चुनते हैं - जैसे कि एक स्ट्रीमिंग के लिए अनुकूलित और दूसरा अधिकतम गोपनीयता के लिए। यह आपकी विशिष्ट आवश्यकताओं और बजट पर निर्भर करता है।

**RAM-only सर्वर आर्किटेक्चर क्या है?**

गोपनीयता

केवल RAM वाले सर्वर हार्ड ड्राइव पर कोई डेटा संग्रहीत नहीं करते - सब कुछ मेमोरी से चलता है जो सर्वर के पुनः आरंभ होने पर साफ़ हो जाती है। यह गोपनीयता सुरक्षा की एक अतिरिक्त परत प्रदान करता है क्योंकि सर्वर पर कोई स्थायी लॉग या डेटा संग्रहीत नहीं किया जा सकता है।

**क्या मैं सार्वजनिक वाई-फाई पर वीपीएन का उपयोग कर सकता हूं?**

सुरक्षा

हाँ, सार्वजनिक वाई-फ़ाई पर VPN का इस्तेमाल करना बेहद ज़रूरी है। सार्वजनिक नेटवर्क अक्सर असुरक्षित होते हैं, जिससे दूसरे लोग आपका डेटा चुरा सकते हैं। VPN आपके कनेक्शन को एन्क्रिप्ट करता है और पासवर्ड और निजी डेटा जैसी संवेदनशील जानकारी को हैकर्स से सुरक्षित रखता है।

संबंधित मार्गदर्शिकाएँ:

[सार्वजनिक वाई-फाई सुरक्षा गाइड](https://bestvpn.digital/guides/public-wifi-security)

[सार्वजनिक वायरलेस नेटवर्क पर सुरक्षित रहने के लिए संपूर्ण मार्गदर्शिका](https://bestvpn.digital/guides/public-wifi-security)

[मोबाइल वीपीएन सुरक्षा](https://bestvpn.digital/guides/mobile-vpn-security)

[मोबाइल उपकरणों पर VPN का उपयोग करने के सर्वोत्तम तरीके](https://bestvpn.digital/guides/mobile-vpn-security)

**साझा और समर्पित आईपी पते के बीच क्या अंतर है?**

विशेषताएँ

साझा आईपी पते कई वीपीएन उपयोगकर्ताओं द्वारा एक साथ उपयोग किए जाते हैं, जिससे बेहतर गुमनामी मिलती है, लेकिन सेवा अवरोधों का सामना करना पड़ सकता है। समर्पित आईपी पते केवल आपको ही दिए जाते हैं, जिससे अवरोध और कैप्चा कम होते हैं, लेकिन गुमनामी कम होती है।

**मैं VPN कनेक्शन समस्याओं का निवारण कैसे करूँ?**

समस्या निवारण

सामान्य समाधानों में सर्वर बदलना, VPN प्रोटोकॉल बदलना, ऐप को पुनः आरंभ करना, फ़ायरवॉल सेटिंग्स की जाँच करना, VPN ऐप को अपडेट करना या ग्राहक सहायता से संपर्क करना शामिल है। कई कनेक्शन समस्याएँ विभिन्न सर्वर या प्रोटोकॉल आज़माकर हल की जाती हैं।

**सुरक्षा वीपीएन उपयोग के लिए मुझे राउटर के बारे में क्या पता होना चाहिए?**

सुरक्षा

VPN का इस्तेमाल करते समय सुरक्षा के लिए राउटर कॉन्फ़िगरेशन बेहद ज़रूरी है। अपने राउटर पर VPN सेट अप करने से सभी कनेक्टेड डिवाइस अपने आप सुरक्षित हो जाते हैं। ऐसे राउटर चुनें जो VPN क्लाइंट सपोर्ट करते हों, फ़र्मवेयर अपडेट होना सुनिश्चित करें और उचित फ़ायरवॉल सेटिंग्स कॉन्फ़िगर करें। हमारी सुझाई गई VPN सेवाएँ राउटर सेटअप गाइड और सहायता प्रदान करती हैं।

**VPN के माध्यम से प्रोटोकॉल को बढ़ाने में WebRTC की क्या भूमिका है?**

तकनीकी

VPN प्रोटोकॉल का उपयोग करते समय WebRTC आपके ऑनलाइन अनुभव को महत्वपूर्ण रूप से प्रभावित कर सकता है। WebRTC का उचित प्रबंधन सेंसरशिप को बायपास करने, आपके डेटा को सुरक्षित रखने और बेहतर गति का आनंद लेने में मदद करता है। शीर्ष VPN में उन्नत WebRTC लीक सुरक्षा सुविधाएँ शामिल होती हैं जो ब्राउज़र WebRTC अनुरोधों के माध्यम से आपके वास्तविक IP को उजागर होने से रोकती हैं।

**वीपीएन के माध्यम से बेसिक्स को बढ़ाने में लॉगिंग की क्या भूमिका है?**

गोपनीयता

वीपीएन चुनते समय लॉगिंग नीतियों को समझना ज़रूरी है। नो-लॉग्स नीतियाँ यह सुनिश्चित करती हैं कि आपका ब्राउज़िंग इतिहास, कनेक्शन समय और आईपी पते रिकॉर्ड न किए जाएँ। यह महत्वपूर्ण गोपनीयता सुरक्षा प्रदान करता है और डेटा को तीसरे पक्ष या अधिकारियों के साथ साझा होने से रोकता है।

**स्ट्रीमिंग वीपीएन सेटअप में आईपी लीक से संबंधित सामान्य गलतियाँ क्या हैं?**

स्ट्रीमिंग

आईपी लीक आपके स्ट्रीमिंग अनुभव और गोपनीयता को खतरे में डाल सकते हैं। आम गलतियों में DNS लीक, WebRTC लीक या IPv6 लीक की जाँच न करना शामिल है। किल स्विच और लीक प्रोटेक्शन के साथ सही तरीके से कॉन्फ़िगर किए गए VPN यह सुनिश्चित करते हैं कि भू-प्रतिबंधित सामग्री स्ट्रीम करते समय आपका असली आईपी छिपा रहे।

संबंधित मार्गदर्शिकाएँ:

[वीपीएन लीक परीक्षण गाइड](https://bestvpn.digital/guides/vpn-leak-test)

[DNS, WebRTC और IP लीक के लिए अपने VPN का परीक्षण कैसे करें](https://bestvpn.digital/guides/vpn-leak-test)

[स्ट्रीमिंग वीपीएन सेटअप](https://bestvpn.digital/guides/streaming-vpn-setup)

[स्ट्रीमिंग सेवाओं के लिए इष्टतम VPN कॉन्फ़िगरेशन](https://bestvpn.digital/guides/streaming-vpn-setup)

**वीपीएन के माध्यम से मूलभूत सुविधाओं को बढ़ाने में डीएनएस की क्या भूमिका है?**

तकनीकी

DNS कॉन्फ़िगरेशन VPN कार्यक्षमता के लिए मूलभूत है। अपने VPN प्रदाता के DNS सर्वर का उपयोग करने से DNS लीक को रोका जा सकता है और यह सुनिश्चित होता है कि आपका सारा ट्रैफ़िक VPN टनल के माध्यम से ठीक से रूट हो। यह गोपनीयता बनाए रखते हुए सुरक्षा और प्रदर्शन दोनों को बढ़ाता है।

**क्या पोर्ट फ़ॉरवर्डिंग VPN उपयोगकर्ताओं के लिए बेसिक्स में प्रदर्शन को प्रभावित करता है?**

प्रदर्शन

पोर्ट फ़ॉरवर्डिंग वीपीएन के प्रदर्शन और कार्यक्षमता को काफ़ी प्रभावित कर सकता है। यह पी2पी गतिविधियों, गेमिंग और सर्वर चलाने के लिए ज़रूरी है। हालाँकि, सभी वीपीएन प्रदाता पोर्ट फ़ॉरवर्डिंग का समर्थन नहीं करते हैं, और यह विशिष्ट पोर्ट खोलकर सुरक्षा को थोड़ा कम कर सकता है।

**उपयोग युक्तियाँ वीपीएन उपयोग के लिए मुझे कैटापुल्ट हाइड्रा के बारे में क्या पता होना चाहिए?**

प्रोटोकॉल

कैटापल्ट हाइड्रा एक मालिकाना वीपीएन प्रोटोकॉल है जो बेहतर गति और सुरक्षा प्रदान करता है। इसे पारंपरिक प्रोटोकॉल की तुलना में बेहतर प्रदर्शन प्रदान करने और मज़बूत एन्क्रिप्शन बनाए रखने के लिए डिज़ाइन किया गया है। यह प्रोटोकॉल स्ट्रीमिंग और सामान्य ब्राउज़िंग के लिए विशेष रूप से प्रभावी है।

**क्या लैग VPN उपयोगकर्ताओं के लिए सुरक्षा में प्रदर्शन को प्रभावित करता है?**

प्रदर्शन

VPN का इस्तेमाल करते समय विलंबता (लैग) सुरक्षा और प्रदर्शन दोनों को प्रभावित कर सकती है। ज़्यादा विलंबता कनेक्शन या सर्वर संबंधी समस्याओं का संकेत हो सकती है। अपने स्थान के नज़दीक VPN सर्वर चुनें और सुरक्षा बनाए रखते हुए विलंबता को कम करने के लिए WireGuard जैसे तेज़ प्रोटोकॉल का इस्तेमाल करें।

**वीपीएन के माध्यम से बेसिक्स को बढ़ाने में कुंजी एक्सचेंज की क्या भूमिका है?**

सुरक्षा

वीपीएन कनेक्शन में कुंजी विनिमय एक मूलभूत सुरक्षा प्रक्रिया है। यह आपके डिवाइस और वीपीएन सर्वर के बीच सुरक्षित एन्क्रिप्शन कुंजियाँ स्थापित करता है। आधुनिक प्रोटोकॉल बेहतर सुरक्षा और प्रदर्शन के लिए एलिप्टिक कर्व डिफी-हेलमैन जैसी उन्नत कुंजी विनिमय विधियों का उपयोग करते हैं।

**वीपीएन के माध्यम से उपयोग युक्तियाँ बढ़ाने में गेटवे की क्या भूमिका है?**

तकनीकी

उचित ट्रैफ़िक रूटिंग के लिए VPN गेटवे बेहद ज़रूरी है। यह तय करता है कि आपका इंटरनेट ट्रैफ़िक VPN टनल के ज़रिए कैसे निर्देशित होगा। उचित गेटवे कॉन्फ़िगरेशन DNS लीक को रोकता है, स्ट्रीमिंग क्वालिटी में सुधार करता है और यह सुनिश्चित करता है कि सभी ट्रैफ़िक सुरक्षित रहें।

**क्या VPN के साथ बेहतर उन्नत सुविधाओं के लिए गेटवे आवश्यक है?**

विकसित

उन्नत VPN सुविधाओं के लिए गेटवे कॉन्फ़िगरेशन आवश्यक है। यह उचित ट्रैफ़िक रूटिंग को सक्षम बनाता है, स्प्लिट टनलिंग को सपोर्ट करता है, और विशिष्ट सर्वरों के साथ संगतता सुनिश्चित करता है। उन्नत उपयोगकर्ताओं को सर्वोत्तम प्रदर्शन के लिए गेटवे सेटिंग्स को समझने से लाभ होता है।

**वीपीएन के माध्यम से बेसिक्स को बढ़ाने में जियो-ब्लॉकिंग की क्या भूमिका है?**

स्ट्रीमिंग

वीपीएन के इस्तेमाल के लिए जियो-ब्लॉकिंग को समझना बेहद ज़रूरी है। वीपीएन आपके स्थान को छिपाकर भौगोलिक प्रतिबंधों को दरकिनार करने में मदद करते हैं। इससे गोपनीयता और सुरक्षा बनाए रखते हुए क्षेत्र-लॉक की गई सामग्री, वेबसाइटों और सेवाओं तक पहुँच मिलती है।

संबंधित मार्गदर्शिकाएँ:

[जियो-ब्लॉकिंग गाइड को बायपास करें](https://bestvpn.digital/guides/bypass-geo-blocking)

[VPN के साथ भू-प्रतिबंधित सामग्री तक कैसे पहुँचें](https://bestvpn.digital/guides/bypass-geo-blocking)

[वैश्विक सामग्री पहुँच](https://bestvpn.digital/guides/global-content-access)

[वीपीएन के साथ अंतर्राष्ट्रीय सामग्री और सेवाओं तक पहुँच](https://bestvpn.digital/guides/global-content-access)

**मुझे डिवाइसों में एक साथ कनेक्शनों की परवाह क्यों करनी चाहिए?**

उपकरण

एक साथ कनेक्शन यह तय करते हैं कि आप एक VPN अकाउंट से कितने डिवाइस सुरक्षित रख सकते हैं। यह उन घरों के लिए ज़रूरी है जहाँ कई डिवाइस हैं। ऐसे VPN खोजें जो आपकी ज़रूरतों के हिसाब से असीमित कनेक्शन या पर्याप्त डिवाइस लिमिट प्रदान करते हों।

**डिवाइस VPN उपयोग के ऑडिट के बारे में मुझे क्या पता होना चाहिए?**

विश्वास

वीपीएन ऑडिट सुरक्षा दावों और गोपनीयता नीतियों का स्वतंत्र सत्यापन प्रदान करते हैं। कई उपकरणों के लिए वीपीएन चुनते समय, ऑडिट किए गए प्रदाता अधिक विश्वसनीयता प्रदान करते हैं। हाल ही में किए गए तृतीय-पक्ष सुरक्षा ऑडिट और पारदर्शिता रिपोर्ट देखें।

**मुझे उन्नत सुविधाओं में लैग की परवाह क्यों करनी चाहिए?**

जुआ

विलंबता गेमिंग, वीडियो कॉल और रीयल-टाइम एप्लिकेशन जैसी उन्नत VPN सुविधाओं को प्रभावित करती है। उन्नत उपयोगकर्ताओं को कम पिंग वाले सर्वर चुनने चाहिए, अनुकूलित प्रोटोकॉल का उपयोग करना चाहिए और सर्वोत्तम अनुभव के लिए समर्पित गेमिंग सर्वर पर विचार करना चाहिए।

**पी2पी और टोरेंटिंग वीपीएन सेटअप में ऑडिट के साथ आम गलतियाँ क्या हैं?**

पी2पी

टोरेंटिंग करते समय, प्रमाणित नो-लॉग्स नीतियों वाले ऑडिटेड वीपीएन प्रदाता चुनें। आम गलतियों में अनऑडिटेड वीपीएन का इस्तेमाल करना, किल स्विच सुविधाओं को नज़रअंदाज़ करना और पी2पी सपोर्ट की पुष्टि न करना शामिल है। ऑडिटेड वीपीएन पी2पी गतिविधियों के लिए बेहतर सुरक्षा प्रदान करते हैं।

**वीपीएन के माध्यम से व्यवसाय को बढ़ाने में पिंग की क्या भूमिका है?**

व्यापार

व्यावसायिक VPN उपयोग के लिए कम पिंग बेहद ज़रूरी है, खासकर वीडियो कॉन्फ्रेंसिंग, VoIP कॉल और रीयल-टाइम सहयोग के लिए। न्यूनतम विलंबता के लिए अनुकूलित सर्वर और समर्पित व्यावसायिक सुविधाओं वाले व्यावसायिक VPN प्रदाता चुनें।

**डिवाइस वीपीएन सेटअप में वीपीएन ऐप्स के साथ आम गलतियाँ क्या हैं?**

उपकरण

वीपीएन ऐप से जुड़ी आम गलतियों में पुराने ऐप्स का इस्तेमाल करना, ऑटो-कनेक्ट सुविधाओं को कॉन्फ़िगर न करना, किल स्विच सेटिंग्स को नज़रअंदाज़ करना और नकली वीपीएन ऐप डाउनलोड करना शामिल है। हमेशा विश्वसनीय स्रोतों से आधिकारिक ऐप डाउनलोड करें और उन्हें अपडेट रखें।

**क्या VPN के साथ बेहतर प्रोटोकॉल के लिए लैग आवश्यक है?**

प्रोटोकॉल

हालाँकि लैग वांछनीय नहीं है, लेकिन लेटेंसी को समझने से सही VPN प्रोटोकॉल चुनने में मदद मिलती है। WireGuard आमतौर पर OpenVPN की तुलना में कम लेटेंसी प्रदान करता है, जबकि IKEv2 मोबाइल कनेक्शन के लिए अनुकूलित है। अपनी गति और सुरक्षा आवश्यकताओं के आधार पर प्रोटोकॉल चुनें।

**उन्नत सुविधाओं में मुझे WebRTC की परवाह क्यों करनी चाहिए?**

गोपनीयता

VPN का इस्तेमाल करते समय भी WebRTC आपका असली IP पता लीक कर सकता है। अनुभवी उपयोगकर्ताओं को ब्राउज़र में WebRTC को अक्षम कर देना चाहिए या अंतर्निहित WebRTC लीक सुरक्षा वाले VPN का उपयोग करना चाहिए। यह वीडियो कॉल और पीयर-टू-पीयर कनेक्शन के दौरान गोपनीयता भंग होने से बचाता है।

**2025 में कौन सा VPN Netflix USA के साथ काम करेगा?**

स्ट्रीमिंग

हमारे नवीनतम परीक्षणों के अनुसार, एक्सप्रेसवीपीएन का न्यू जर्सी 3 सर्वर, नॉर्डवीपीएन का अटलांटा सर्वर, और सर्फशार्क का लॉस एंजिल्स सर्वर नेटफ्लिक्स यूएसए को 4K में अनब्लॉक करते हैं। मुफ़्त वीपीएन 100% बार विफल होते हैं।

**यूके के बाहर बीबीसी आईप्लेयर कैसे देखें?**

स्ट्रीमिंग

NordVPN के UK#1847 सर्वर से कनेक्ट करें, ब्राउज़र कुकीज़ साफ़ करें, और किसी भी UK पोस्टकोड (जैसे, SW1A 1AA) के साथ रजिस्टर करें। स्मार्ट टीवी सहित सभी डिवाइस पर काम करता है।

**क्या मैं एप्पल टीवी पर VPN का उपयोग कर सकता हूँ?**

उपकरण

Apple TV सीधे VPN ऐप्स को सपोर्ट नहीं करता। इसके बजाय, अपने राउटर पर VPN सेटअप करें या SmartDNS का इस्तेमाल करें (ExpressVPN का MediaStreamer बिना किसी समस्या के काम करता है)।

**डिज्नी+ के लिए कौन सा वीपीएन सबसे अच्छा है?**

स्ट्रीमिंग

Surfshark 15+ Disney+ लाइब्रेरीज़ (अमेरिका, यूके, जापान, आदि) को सबसे कम कीमत पर अनब्लॉक करता है। दैनिक परीक्षण किया गया—हमारा Disney+ VPN स्कोरकार्ड देखें।

**नेटफ्लिक्स प्रॉक्सी त्रुटि कैसे ठीक करें?**

समस्या निवारण

किसी दूसरे सर्वर पर स्विच करें, कैश साफ़ करें, या गुप्त मोड का इस्तेमाल करें। अगर अभी भी ब्लॉक है, तो नवीनतम कार्यशील सर्वर के लिए लाइव चैट से संपर्क करें—एक्सप्रेसवीपीएन हर घंटे अपना सर्वर अपडेट करता है।

**डबल वीपीएन क्या है?**

विकसित

अतिरिक्त एन्क्रिप्शन के लिए ट्रैफ़िक को दो सर्वरों से होकर रूट करता है। नॉर्डवीपीएन का डबल वीपीएन 2048-बिट एन्क्रिप्शन प्रदान करता है—जो पत्रकारों या कार्यकर्ताओं के लिए आदर्श है।

**राउटर पर VPN कैसे सेट करें?**

तकनीकी

FlashRouters से एक प्री-फ्लैश्ड राउटर खरीदें या DD-WRT फ़र्मवेयर इंस्टॉल करें। हमारी गाइड में Asus, Netgear और Linksys सेटअप शामिल हैं—इसमें 10 मिनट लगते हैं।

**IPv6 रिसाव संरक्षण क्या है?**

सुरक्षा

लीक रोकने के लिए IPv6 ट्रैफ़िक को अक्षम करता है। NordVPN की सेटिंग में सक्षम करें—99% VPN इसे अनदेखा करते हैं, जिससे IPv6-सक्षम नेटवर्क पर लीक होता है।

**VPN कनेक्ट न होने की समस्या को कैसे ठीक करें?**

समस्या निवारण

इन चरणों का प्रयास करें: प्रोटोकॉल बदलें (वायरगार्ड → ओपनवीपीएन), DNS को 8.8.8.8 में बदलें, एंटीवायरस/फ़ायरवॉल को अस्थायी रूप से अक्षम करें, सर्वर स्थिति के लिए 24/7 लाइव चैट से संपर्क करें।

**ExpressVPN निःशुल्क कैसे प्राप्त करें?**

मूल्य निर्धारण

30-दिन की मनी-बैक गारंटी का लाभ उठाएँ—बिना किसी सवाल के। साइन अप करें, 29 दिनों तक इस्तेमाल करें, लाइव चैट के ज़रिए रद्द करें और पूरा रिफ़ंड पाएँ। नए ईमेल के ज़रिए दोबारा पुष्टि करें।

**क्या VPN पर आजीवन सौदे होते हैं?**

मूल्य निर्धारण

'लाइफटाइम' VPN से बचें—ये डेटा बंद कर देते हैं या बेच देते हैं। इसके बजाय, Surfshark का 2-वर्षीय प्लान $1.99/माह पर लें—जो 90% की छूट के बराबर है।

**क्या एफबीआई वीपीएन को ट्रैक कर सकती है?**

गोपनीयता

अगर VPN शून्य लॉग रखता है (जैसे ExpressVPN के RAM-ओनली सर्वर), तो FBI भी डेटा पुनर्प्राप्त नहीं कर सकता। अदालत में साबित हुआ—ExpressVPN 2017 में लॉग नहीं सौंप सका।

**वारंट कैनरी क्या है?**

गोपनीयता

पारदर्शिता विवरण मासिक रूप से अपडेट किया जाता है। अगर इसे हटा दिया जाता है, तो यह एक गुप्त सम्मन का संकेत देता है। PIA और NordVPN अपने विवरण सार्वजनिक रूप से प्रकाशित करते हैं।

**2025 में iPhone के लिए सर्वश्रेष्ठ VPN?**

गतिमान

नॉर्डवीपीएन के आईओएस ऐप में वायरगार्ड, किल स्विच और सिरी शॉर्टकट शामिल हैं। ऐप स्टोर पर 4.9/5 रेटिंग प्राप्त - हमारे लिंक से 3 महीने के लिए मुफ़्त डाउनलोड करें।

**एंड्रॉइड टीवी पर वीपीएन का उपयोग कैसे करें?**

उपकरण

Surfshark APK को उनकी वेबसाइट से इंस्टॉल करें (Google Play कुछ क्षेत्रों को ब्लॉक करता है)। 1-क्लिक एक्सेस के लिए 'क्विक कनेक्ट' टाइल का उपयोग करें।

**क्या VPN का उपयोग करना कानूनी है?**

कानूनी

ज़्यादातर देशों में, वीपीएन पूरी तरह से कानूनी हैं। हालाँकि, अवैध गतिविधियों (जैसे कॉपीराइट सामग्री को हैक करना या टोरेंट करना) के लिए इनका इस्तेमाल करना अभी भी गैरकानूनी है। कुछ देश (जैसे, चीन, रूस, यूएई) वीपीएन पर प्रतिबंध लगाते हैं, इसलिए यात्रा से पहले हमेशा स्थानीय कानूनों की जाँच करें।

**क्या VPN मुझे ऑनलाइन गुमनाम बना सकता है?**

गोपनीयता

एक वीपीएन आपकी गोपनीयता को काफ़ी हद तक बढ़ाता है, लेकिन आपको 100% गुमनाम नहीं बनाता। पूरी तरह से गुमनाम रहने के लिए, नो-लॉग्स वीपीएन को टोर, सुरक्षित ब्राउज़र और टेल्स जैसे गोपनीयता-केंद्रित ऑपरेटिंग सिस्टम के साथ मिलाएँ।

**वीपीएन और प्रॉक्सी में क्या अंतर है?**

तुलना

एक वीपीएन आपके सभी इंटरनेट ट्रैफ़िक को ऑपरेटिंग सिस्टम स्तर पर एन्क्रिप्ट करता है, जबकि एक प्रॉक्सी केवल विशिष्ट ऐप्स (जैसे आपके ब्राउज़र) से ट्रैफ़िक को रीरूट करता है। प्रॉक्सी डेटा को एन्क्रिप्ट नहीं करते, जिससे वीपीएन कहीं अधिक सुरक्षित हो जाते हैं।

**क्या VPN इंटरनेट की गति को धीमा कर देते हैं?**

प्रदर्शन

हाँ, लेकिन बहुत कम। वायरगार्ड जैसे आधुनिक प्रोटोकॉल वाला एक प्रीमियम वीपीएन स्पीड को 5-10% तक कम कर सकता है, जबकि मुफ़्त या भीड़-भाड़ वाले वीपीएन स्पीड को 50% या उससे ज़्यादा तक कम कर सकते हैं। पास का सर्वर चुनने से मदद मिलती है।

**क्या मैं एकाधिक डिवाइस पर VPN का उपयोग कर सकता हूँ?**

उपकरण

शीर्ष वीपीएन प्रति खाते 5-10 एक साथ कनेक्शन प्रदान करते हैं। कुछ (जैसे सर्फशार्क) असीमित डिवाइस की अनुमति देते हैं। यह देखने के लिए कि कौन से वीपीएन आपके फ़ोन, लैपटॉप, राउटर और स्मार्ट टीवी को सपोर्ट करते हैं, हमारा तुलना चार्ट देखें।

**क्या VPN हैकर्स से सुरक्षा प्रदान करता है?**

सुरक्षा

हाँ, खासकर सार्वजनिक वाई-फ़ाई पर। एक वीपीएन आपके डेटा को एन्क्रिप्ट करता है, जिससे मैन-इन-द-मिडल हमलों को रोका जा सकता है। हालाँकि, यह मैलवेयर या फ़िशिंग से सुरक्षा नहीं देगा—अपने वीपीएन के साथ एंटीवायरस और 2FA का इस्तेमाल करें।

**नो-लॉग्स वीपीएन क्या है?**

गोपनीयता

नो-लॉग्स वीपीएन आपकी ऑनलाइन गतिविधि से संबंधित कोई भी डेटा संग्रहीत नहीं करता है। ऐसे प्रदाताओं की तलाश करें जिनका ऑडिट तृतीय पक्षों (जैसे PwC या Cure53) द्वारा किया गया हो और जो गोपनीयता-अनुकूल क्षेत्राधिकारों (जैसे, पनामा, स्विट्ज़रलैंड) में स्थित हों।

**यदि मैं VPN का उपयोग करता हूं तो क्या मुझे ट्रैक किया जा सकता है?**

गोपनीयता

अगर आपके वीपीएन की नो-लॉग्स नीति सख्त है और वह DNS/WebRTC लीक नहीं करता, तो ट्रैकिंग बेहद मुश्किल है। हालाँकि, Google या Facebook में लॉग इन करने पर भी आपकी पहचान हो जाती है—गुप्त मोड और गोपनीयता-केंद्रित सेवाओं का इस्तेमाल करें।

**किल स्विच क्या है?**

सुरक्षा

अगर VPN डिस्कनेक्ट हो जाता है, तो एक किल स्विच आपके इंटरनेट कनेक्शन को बंद कर देता है, जिससे IP लीक को रोका जा सकता है। टोरेंटिंग या संवेदनशील सामग्री एक्सेस करते समय हमेशा इस सुविधा को सक्षम रखें।

**क्या मुफ्त वीपीएन सुरक्षित हैं?**

मूल्य निर्धारण

99% मुफ़्त VPN खतरनाक होते हैं। ये आपका डेटा बेचते हैं, विज्ञापन डालते हैं या मैलवेयर रखते हैं। प्रोटॉन VPN का मुफ़्त टियर (सीमित सर्वर, कोई लॉग नहीं) अपवाद है। सुरक्षा के लिए, मनी-बैक गारंटी वाले पेड VPN ही चुनें।

**स्प्लिट टनलिंग क्या है?**

विशेषताएँ

स्प्लिट टनलिंग आपको यह चुनने की सुविधा देती है कि कौन से ऐप्स VPN का इस्तेमाल करें और कौन से आपके नियमित कनेक्शन का। यह उन बैंकिंग ऐप्स के लिए बेहतरीन है जो सुरक्षित रूप से टोरेंटिंग करते समय VPN को ब्लॉक कर देते हैं।

**क्या VPN नेटफ्लिक्स जियो-ब्लॉक को बायपास कर सकता है?**

स्ट्रीमिंग

हाँ, लेकिन केवल ExpressVPN, NordVPN, या Surfshark जैसे प्रीमियम VPN ही Netflix, BBC iPlayer और Disney+ को लगातार अनब्लॉक करते हैं। हमारे दैनिक-परीक्षणित कार्यशील सर्वरों की सूची देखें।

**वायरगार्ड क्या है?**

तकनीकी

वायरगार्ड सबसे नया वीपीएन प्रोटोकॉल है, जो ओपनवीपीएन की तुलना में तेज़ गति और मज़बूत एन्क्रिप्शन प्रदान करता है। अधिकांश शीर्ष वीपीएन अब इसका समर्थन करते हैं (उदाहरण के लिए, नॉर्डवीपीएन का नॉर्डलिंक्स)।

**मैं कैसे जानूं कि मेरा VPN काम कर रहा है?**

परीक्षण

कनेक्ट करने से पहले और बाद में ipleak.net पर जाएँ। अगर आपका IP और DNS बदल जाता है, तो इसका मतलब है कि यह काम कर रहा है। अपने ब्राउज़र में WebRTC लीक की भी जाँच करें।

**क्या मैं गेमिंग के लिए VPN का उपयोग कर सकता हूँ?**

जुआ

हाँ! एक VPN DDoS हमलों को कम करता है, IP प्रतिबंधों को दरकिनार करता है, और आपको जियो-लॉक्ड गेम्स को जल्दी एक्सेस करने की सुविधा देता है। ExpressVPN या CyberGhost जैसे कम पिंग सर्वर वाले VPN चुनें।

**अस्पष्टीकरण क्या है?**

विकसित

अस्पष्टीकरण (obfuscation) वीपीएन ट्रैफ़िक को सामान्य HTTPS के रूप में छिपा देता है, चीन या ईरान जैसे देशों में वीपीएन ब्लॉक को दरकिनार कर देता है। 'स्टील्थ मोड' या 'ओपनवीपीएन स्क्रैम्बल' सुविधाओं पर ध्यान दें।

**क्या चीन में VPN काम करते हैं?**

सेंसरशिप

डीप पैकेट इंस्पेक्शन के कारण केवल कुछ ही वीपीएन (जैसे, एक्सप्रेसवीपीएन, एस्ट्रिल, नॉर्डवीपीएन) चीन में विश्वसनीय रूप से काम करते हैं। यात्रा से पहले हमेशा वीपीएन डाउनलोड करें।

**क्या मैं VPN के साथ टोरेंट कर सकता हूँ?**

पी2पी

हाँ, लेकिन केवल किल स्विच सक्षम वाले P2P-अनुकूलित सर्वर का ही उपयोग करें। हमारी शीर्ष पसंद: नॉर्डवीपीएन, सर्फशार्क और प्राइवेट इंटरनेट एक्सेस—सभी पोर्ट फ़ॉरवर्डिंग और बिना किसी बैंडविड्थ सीमा के।

**समर्पित आईपी क्या है?**

विशेषताएँ

एक समर्पित आईपी पता केवल आपके द्वारा उपयोग किया जाने वाला आईपी पता होता है, जिससे कैप्चा और ब्लैकलिस्टिंग कम होती है। बैंकिंग या दूरस्थ कार्य के लिए उपयोगी। नॉर्डवीपीएन, साइबरघोस्ट और प्योरवीपीएन के साथ ऐड-ऑन के रूप में उपलब्ध।

**वीपीएन की लागत कितनी है?**

मूल्य निर्धारण

प्रीमियम वीपीएन की कीमत प्लान की अवधि के आधार पर $2 से $12/माह तक होती है। हमारे विशेष ऑफर के तहत कीमतें $1.99/माह (सर्फशार्क 2-वर्षीय प्लान) तक कम हो जाती हैं, जिसमें 3 महीने मुफ़्त मिलते हैं।

**क्या मैं गुमनाम रूप से VPN के लिए भुगतान कर सकता हूँ?**

गोपनीयता

हाँ, शीर्ष वीपीएन बिटकॉइन, मोनेरो या नकद स्वीकार करते हैं। मुल्लवड एक खाता संख्या भी जनरेट करता है—ईमेल की आवश्यकता नहीं।

**पांच/नौ/चौदह आंखें गठबंधन क्या है?**

गोपनीयता

ये देशों के बीच खुफिया जानकारी साझा करने के समझौते हैं। इन अधिकार क्षेत्रों (जैसे, अमेरिका, ब्रिटेन) में स्थित VPN से बचें, जब तक कि उनके पास प्रमाणित नो-लॉग्स नीति (जैसे PIA) न हो।

**क्या VPN, ISP थ्रॉटलिंग को बायपास कर सकता है?**

प्रदर्शन

हाँ, अगर आपका ISP स्ट्रीमिंग (जैसे, Netflix) को धीमा कर देता है, तो VPN आपके ट्रैफ़िक को छिपा देता है और पूरी स्पीड बहाल कर देता है। पुष्टि के लिए VPN के साथ और उसके बिना परीक्षण करें।

**शुरुआती लोगों के लिए सबसे अच्छा वीपीएन कौन सा है?**

सिफारिशों

साइबरघोस्ट और एक्सप्रेसवीपीएन में 1-क्लिक ऐप्स, 24/7 सपोर्ट और किसी सेटअप की ज़रूरत नहीं है। गैर-तकनीकी उपयोगकर्ताओं के लिए बिल्कुल सही।

**किसी को रोजमर्रा की ब्राउज़िंग के लिए वीपीएन का उपयोग क्यों करना चाहिए?**

सामान्य वीपीएन जानकारी

दैनिक ब्राउज़िंग के लिए VPN का उपयोग आपकी ऑनलाइन गोपनीयता और सुरक्षा को बढ़ाता है। यह आपके इंटरनेट ट्रैफ़िक को एन्क्रिप्ट करता है, जिससे ISP, विज्ञापनदाता या हैकर आपकी गतिविधियों पर नज़र नहीं रख पाते। यह कैफ़े या हवाई अड्डों के सार्वजनिक वाई-फ़ाई जैसे असुरक्षित नेटवर्क पर विशेष रूप से महत्वपूर्ण है, जहाँ डेटा चोरी का जोखिम होता है। VPN आपको भौगोलिक प्रतिबंधों को दरकिनार करके, क्षेत्र-लॉक YouTube वीडियो या समाचार साइटों जैसी सामग्री तक पहुँचने की सुविधा भी देता है। उदाहरण के लिए, आप गुमनाम रूप से ब्राउज़ कर सकते हैं, सस्ती उड़ानों की खरीदारी कर सकते हैं, या अंतर्राष्ट्रीय टीवी शो स्ट्रीम कर सकते हैं। 2025 में, डेटा उल्लंघनों में वृद्धि के साथ, VPN सुरक्षा की एक और परत जोड़ता है। ExpressVPN, जो अपनी गति और विश्वसनीयता के लिए जाना जाता है, सभी डिवाइस पर निर्बाध ब्राउज़िंग के लिए एक बेहतरीन विकल्प है। इसका सहज इंटरफ़ेस सभी उपयोगकर्ताओं के लिए उपयुक्त है।

**वीपीएन शुरुआती लोगों के लिए ऑनलाइन सुरक्षा कैसे बेहतर बनाता है?**

सामान्य वीपीएन जानकारी

शुरुआती लोगों के लिए, एक वीपीएन आपके इंटरनेट कनेक्शन को एन्क्रिप्ट करके ऑनलाइन सुरक्षा को आसान बनाता है, जो पासवर्ड या क्रेडिट कार्ड विवरण जैसे संवेदनशील डेटा को हैकर्स से सुरक्षित रखता है। यह आपके आईपी एड्रेस को छुपाता है, जिससे वेबसाइटों या ट्रैकर्स के लिए आपकी पहचान करना मुश्किल हो जाता है। यह सार्वजनिक वाई-फाई पर विशेष रूप से उपयोगी है, जहाँ साइबर हमले आम हैं। एक वीपीएन घुसपैठिया विज्ञापनों और ट्रैकर्स को भी ब्लॉक करता है, जिससे ब्राउज़िंग का अनुभव और भी बेहतर हो जाता है। 2025 में, जब साइबर अपराध की लागत सालाना अरबों डॉलर होगी, तो आम उपयोगकर्ता भी इस सुरक्षा का लाभ उठा सकेंगे। साइबरघोस्ट एक आसान-से-उपयोग इंटरफ़ेस प्रदान करता है जिसमें पहले से कॉन्फ़िगर की गई सुरक्षा सेटिंग्स हैं, जो नए उपयोगकर्ताओं के लिए आदर्श है। इसकी नो-लॉग्स नीति सुनिश्चित करती है कि आपका डेटा निजी रहे। साइबरघोस्ट जैसे विकल्पों को आज़माकर, आप बिना किसी तकनीकी विशेषज्ञता के अपनी ऑनलाइन गतिविधियों को सुरक्षित करना शुरू कर सकते हैं।

**वीपीएन और प्रॉक्सी सर्वर में क्या अंतर है?**

सामान्य वीपीएन जानकारी

एक वीपीएन और एक प्रॉक्सी सर्वर दोनों आपके आईपी पते को छिपाते हैं, लेकिन उनमें काफ़ी अंतर होता है। एक वीपीएन आपके सभी इंटरनेट ट्रैफ़िक को एन्क्रिप्ट करता है, उसे एक सुरक्षित सर्वर के माध्यम से रूट करता है, जिससे ऐप्स और वेबसाइटों पर गोपनीयता और सुरक्षा सुनिश्चित होती है। प्रॉक्सी केवल विशिष्ट ट्रैफ़िक (जैसे, ब्राउज़र डेटा) को बिना एन्क्रिप्शन के रीडायरेक्ट करते हैं, जिससे आप जासूसी के शिकार हो सकते हैं। वीपीएन बैंकिंग या भौगोलिक प्रतिबंधों को दरकिनार करने जैसे संवेदनशील कार्यों के लिए आदर्श होते हैं, जबकि प्रॉक्सी ब्लॉक की गई साइटों तक त्वरित, गैर-संवेदनशील पहुँच के लिए बेहतर होते हैं। उदाहरण के लिए, एक वीपीएन आपको नेटफ्लिक्स को सुरक्षित रूप से स्ट्रीम करने देता है, जबकि एक प्रॉक्सी ऐसा नहीं कर सकता। PureVPN 70 से ज़्यादा देशों में सर्वर के साथ किफ़ायती, एन्क्रिप्टेड कनेक्शन प्रदान करता है, जो इसे प्रॉक्सी की तुलना में एक बेहतर विकल्प बनाता है।

**क्या VPN मेरे ISP से मेरा ब्राउज़िंग इतिहास छुपा सकता है?**

सामान्य वीपीएन जानकारी

हाँ, एक वीपीएन आपके ट्रैफ़िक को एन्क्रिप्ट करके और उसे एक रिमोट सर्वर के ज़रिए रूट करके आपके ब्राउज़िंग इतिहास को आपके आईएसपी से छुपाता है। यह आपके आईएसपी को यह देखने से रोकता है कि आप किन वेबसाइटों पर जाते हैं या ऑनलाइन क्या करते हैं, जिससे आपकी गोपनीयता सुरक्षित रहती है। उदाहरण के लिए, अगर आप स्ट्रीमिंग कर रहे हैं या संवेदनशील विषयों पर शोध कर रहे हैं, तो एक वीपीएन आपकी गतिविधि को निजी रखता है। 2025 में, जब आईएसपी उपयोगकर्ता डेटा का तेज़ी से मुद्रीकरण कर रहे हैं, तो यह एक प्रमुख लाभ है। नॉर्डवीपीएन, अपनी ऑडिटेड नो-लॉग्स नीति के साथ, यह सुनिश्चित करता है कि वीपीएन प्रदाता भी आपकी गतिविधि न देख सके। इसके 5,500 से ज़्यादा सर्वर निजी ब्राउज़िंग की सुविधा प्रदान करते हैं। नॉर्डवीपीएन जैसी सेवा चुनकर, आप अपने डिजिटल फ़ुटप्रिंट पर नियंत्रण बनाए रख सकते हैं और चिंतामुक्त होकर ब्राउज़ कर सकते हैं।

**क्या मुझे अपने घर के वाई-फाई का उपयोग करते समय वीपीएन की आवश्यकता है?**

सामान्य वीपीएन जानकारी

हालाँकि घरेलू वाई-फ़ाई आम तौर पर सार्वजनिक नेटवर्क से ज़्यादा सुरक्षित होता है, फिर भी एक VPN मूल्यवान सुरक्षा प्रदान करता है। यह आपके डेटा को एन्क्रिप्ट करता है, जिससे हैकर्स कमज़ोर राउटर सुरक्षा का फ़ायदा उठाने या लॉगिन क्रेडेंशियल जैसी संवेदनशील जानकारी को इंटरसेप्ट करने से बच जाते हैं। यह ISP को लक्षित विज्ञापनों के लिए आपकी ब्राउज़िंग आदतों पर नज़र रखने से भी रोकता है। उदाहरण के लिए, अगर आप घर पर ऑनलाइन खरीदारी करते हैं या वित्तीय प्रबंधन करते हैं, तो एक VPN सुनिश्चित करता है कि आपका डेटा सुरक्षित रहे। इसके अलावा, यह अंतरराष्ट्रीय स्ट्रीमिंग प्लेटफ़ॉर्म जैसी भौगोलिक रूप से प्रतिबंधित सामग्री को भी अनलॉक करता है। ExpressVPN राउटर और उपकरणों के लिए ऐप्स के साथ, घरेलू उपयोग के लिए तेज़ और विश्वसनीय कनेक्शन प्रदान करता है। इसका उपयोगकर्ता-अनुकूल सेटअप आपके पूरे नेटवर्क को सुरक्षित करना आसान बनाता है।

114 में से 114 अक्सर पूछे जाने वाले प्रश्न दिखाए जा रहे हैं