नाम: _____ दिनांक: _____ अंक: _____

चेकपॉइंट 10

बुनियादी VPN FAQ

इंटरैक्टिव वर्कशीट और अध्ययन मार्गदर्शिका

आधारित: VPN.com VPN गाइड: **https://www.vpn.com/hi/vpn/**

VPN क्या है वर्कशीट

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग A)

वर्चुअल प्राइवेट नेटवर्क के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q1: VPN क्या है और यह कैसे काम करता है?

वर्चुअल प्राइवेट नेटवर्क (VPN) आपके इंटरनेट कनेक्शन को एन्क्रिप्ट करता है और आपके ट्रैफ़िक को एक सुरक्षित रिमोट सर्वर से भेजता है। इससे आपका सार्वजनिक IP पता छिप जाता है और VPN टनल से गुज़रने वाले ट्रैफ़िक के बारे में स्थानीय नेटवर्क पर नज़र रखने वाले और आपका ISP जो देख सकते हैं, वह सीमित हो जाता है।

Q2: मुझे VPN का उपयोग क्यों करना चाहिए?

VPN आपकी डिजिटल गोपनीयता की रक्षा करता है, सार्वजनिक Wi-Fi नेटवर्क (जैसे कैफ़े या हवाई अड्डे) पर आपके कनेक्शन को सुरक्षित करता है, जब ISP एन्क्रिप्टेड ट्रैफ़िक का प्रकार पहचान नहीं पाता तब गतिविधि-आधारित थ्रॉटलिंग को घटा सकता है, वैश्विक सामग्री तक पहुँचने के लिए भौगोलिक प्रतिबंधों को बायपास करता है, और दूरस्थ कार्य के संसाधनों को सुरक्षित करने में मदद करता है।

Q3: क्या VPN मुझे ऑनलाइन पूरी तरह गुमनाम बना देता है?

नहीं। VPN आपका IP पता छिपाता है और ट्रैफ़िक एन्क्रिप्ट करता है, फिर भी आपको ब्राउज़र कुकी, सक्रिय खातों (जैसे Google या Facebook), ब्राउज़र फ़िंगरप्रिंटिंग, या VPN प्रदाता द्वारा आपका डेटा लॉग करने से ट्रैक किया जा सकता है।

Q4: क्या VPN मेरी इंटरनेट स्पीड धीमी कर देगा?

हाँ, थोड़ी। एन्क्रिप्शन प्रक्रिया और VPN सर्वर की भौतिक दूरी लेटेंसी और ओवरहेड बढ़ाती है। असर प्रोवाइडर, प्रोटोकॉल, सर्वर की दूरी, डिवाइस और नेटवर्क की स्थिति के अनुसार बदलता है।

Q5: क्या VPN का उपयोग क़ानूनी है?

कई देशों में VPN का उपयोग कानूनी है, लेकिन कुछ क्षेत्राधिकार VPN सेवाओं को प्रतिबंधित, विनियमित या ब्लॉक करते हैं। उपयोग से पहले उपयोगकर्ताओं को वर्तमान स्थानीय कानून जाँच लेने चाहिए। अधिक जानकारी के लिए VPN.com पर वैधता गाइड देखें।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

वर्चुअल प्राइवेट नेटवर्क के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q6: क्या मैं मुफ़्त VPN उपयोग कर सकता हूँ?

मुफ़्त VPN विज्ञापन, सीमित सुविधाओं, उपयोग विश्लेषण, डेटा सीमा या कमाई के अन्य मॉडलों पर निर्भर हो सकते हैं। उपयोग से पहले उपयोगकर्ताओं को प्रदाता की गोपनीयता नीति, स्वामित्व, ऑडिट और बिज़नेस मॉडल की समीक्षा करनी चाहिए।

Q7: "नो-लॉग्स" नीति क्या है?

नो-लॉग्स नीति बताती है कि प्रदाता के अनुसार वह कौन-सी गतिविधि और कनेक्शन डेटा नहीं रखता। सटीक दायरा अलग-अलग होता है, इसलिए पाठकों को नीति और स्वतंत्र ऑडिट के निष्कर्ष देखने चाहिए।

Q8: मैं सबसे अच्छा VPN कैसे चुनूँ?

ऑडिट की गई नो-लॉग्स नीतियाँ, मज़बूत प्रोटोकॉल (WireGuard, OpenVPN), सुरक्षित सर्वर स्थान, तेज़ गति, केवल-RAM सर्वर, किल स्विच सुविधा और खुफ़िया-साझाकरण गठबंधनों (जैसे 5/9/14 Eyes) से बाहर का क्षेत्राधिकार देखें।

Q9: क्या मैं अपने फ़ोन और स्मार्ट TV पर VPN उपयोग कर सकता हूँ?

हाँ। आधुनिक VPN प्रोवाइडर iOS, Android, macOS, Windows, Linux और स्मार्ट टीवी के लिए समर्पित ऐप्स, साथ ही आपके घर के नेटवर्क के सभी डिवाइस की सुरक्षा के लिए राउटर सेटअप देते हैं।

Q10: Kill Switch क्या है?

Kill Switch एक सुरक्षा सुविधा है जो VPN कनेक्शन टूटने पर आपके उपकरण को इंटरनेट से अपने-आप डिस्कनेक्ट कर देती है। इससे आपका बिना एन्क्रिप्शन वाला डेटा या असली IP पता लीक होने से बचता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q1: WireGuard, OpenVPN और IKEv2 में क्या अंतर है?

WireGuard एक आधुनिक, हल्का प्रोटोकॉल है (केवल ~4,000 कोड लाइनें) जो तेज़ गति और जल्दी कनेक्शन समय देता है। OpenVPN एक अत्यंत सुरक्षित, कसौटी पर परखा हुआ ओपन-सोर्स प्रोटोकॉल है। IKEv2 नेटवर्क बदलते समय जल्दी फिर से कनेक्ट होने की क्षमता के कारण मोबाइल डिवाइस के लिए उत्कृष्ट है। [4]

Q2: डबल VPN या Multi-Hop रूटिंग क्या है?

मल्टी-हॉप आपके ट्रैफ़िक को क्रम में दो या अधिक VPN सर्वरों से रूट करता है। इससे एन्क्रिप्शन की दूसरी परत जुड़ती है और अगर एक सर्वर से समझौता हो जाए, तो आपके असली IP पते को दूसरे हॉप से छिपाए रखने में मदद मिलती है।

Q3: WebRTC लीकिंग क्या है और VPN इसे कैसे रोकता है?

WebRTC एक ब्राउज़र प्रोटोकॉल है जो VPN सक्रिय होने पर भी आपके असली लोकल और सार्वजनिक IP पते उजागर कर सकता है। प्रीमियम VPN अपने डेस्कटॉप/मोबाइल ऐप और ब्राउज़र एक्सटेंशन में WebRTC अनुरोधों को ब्लॉक या स्पूफ़ करते हैं।

Q4: RAM-only सर्वर क्या हैं और वे क्यों मायने रखते हैं?

पारंपरिक सर्वर डेटा हार्ड ड्राइव पर लिखते हैं, जिन्हें ज़ब्त या समझौता किया जा सकता है। केवल-RAM (बिना डिस्क वाले) सर्वर पूरी तरह वोलेटाइल मेमोरी (RAM) में चलते हैं। सर्वर के रीबूट या बंद होने पर मेमोरी में रखा डेटा मिट जाता है।

Q5: ऑब्फ़स्केशन VPN ब्लॉक को कैसे बायपास करता है?

ऑब्फ़स्केशन (या "Stealth VPN") VPN ट्रैफ़िक को ऐसा रूप देता है कि वह सामान्य HTTPS ट्रैफ़िक (पोर्ट 443) जैसा दिखे। इससे सरकारों या स्कूल/ऑफ़िस नेटवर्क द्वारा VPN रोकने के लिए इस्तेमाल की जाने वाली डीप पैकेट इंस्पेक्शन (DPI) को पार करने में मदद मिल सकती है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q6: स्प्लिट टनलिंग क्या है और इसका उपयोग कब करना चाहिए?

स्प्लिट टनलिंग आपको चुनने देती है कि कौन से ऐप एन्क्रिप्टेड VPN टनल से जाएँ और कौन सीधे इंटरनेट से जुड़ें। संवेदनशील बैंकिंग ऐप को VPN से भेजने और स्थानीय गेम को सीधे जोड़ने के लिए इसका उपयोग करें, जिससे VPN से जुड़ी लेटेंसी से बचा जा सके।

Q7: फ़ॉरवर्ड सीक्रेसी (परफ़ेक्ट फ़ॉरवर्ड सीक्रेसी) कैसे काम करती है?

PFS यह सुनिश्चित करता है कि हर सत्र के लिए एक अनूठी, अस्थायी एन्क्रिप्शन कुंजी बने। भविष्य में प्राइवेट कुंजी से छेड़छाड़ हो भी जाए, तो उससे पिछले या भविष्य के सत्र डिक्रिप्ट नहीं किए जा सकते क्योंकि उनमें स्वतंत्र कुंजियाँ इस्तेमाल हुई थीं।

Q8: 5/9/14 Eyes गठबंधन क्या हैं और मुझे इनकी परवाह क्यों करनी चाहिए?

क्षेत्राधिकार उस कानूनी प्रक्रिया को प्रभावित कर सकता है जिसका सामना कोई प्रदाता कर सकता है, लेकिन व्यावहारिक गोपनीयता जोखिम इस पर भी निर्भर करता है कि प्रदाता कौन-सा डेटा रखता है, उसका तकनीकी ढाँचा, स्वामित्व, पारदर्शिता रिपोर्टिंग और ऑडिट का इतिहास क्या है।

Q9: DNS Leak सुरक्षा क्या है?

DNS लीक सुरक्षा आपके डिवाइस को वेबसाइट लुकअप क्वेरी (DNS क्वेरी) अपने ISP के सर्वरों के बजाय VPN के निजी, एन्क्रिप्टेड DNS सर्वरों से भेजने के लिए बाध्य करती है। इससे आपका ISP यह ट्रैक नहीं कर पाता कि आप कौन-सी साइटें देखते हैं।

Q10: क्या VPN ISP इंटरनेट थ्रॉटलिंग को बायपास कर सकता है?

कभी-कभी। जब ISP चुनिंदा पहचान योग्य गतिविधियों की स्पीड घटाता है, तब VPN मदद कर सकता है, लेकिन वह भीड़, डेटा सीमा, खाता-स्तर की स्पीड सीमा या खराब नेटवर्क गुणवत्ता को दूर नहीं करेगा।

तकनीकी संदर्भ और स्रोत

इस वर्कशीट में उपयोग किए गए उद्धृत प्रकाशन, क्रिप्टोग्राफ़िक विनिर्देश और आधिकारिक दस्तावेज़ मानक।

शैक्षणिक और उद्योग संदर्भ

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637