Nimi: _____ Päivämäärä: _____ Pisteet: _____

TARKISTUSPISTE 10

Usein kysytyt kysymykset VPN:stä

Interaktiivinen tehtävämoniste ja opiskeluopas

Pohjana: VPN.comin VPN-opas: **https://www.vpn.com/fi/vpn/**

Mikä on VPN -tehtävämoniste

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa A)

Tutustu yleisimpiin kysymyksiin ja vastauksiin, joita mahdolliset asiakkaat esittävät virtuaalisten yksityisverkkojen käytöstä.

Q1: Mikä on VPN ja miten se toimii?

Virtuaalinen yksityisverkko (VPN) salaa internetyhteytesi ja reitittää liikenteesi suojatun etäpalvelimen kautta. Tämä peittää julkisen IP-osoitteesi ja rajoittaa sitä, mitä paikallisverkon tarkkailijat ja internetoperaattorisi näkevät VPN-tunnelin kautta kulkevasta liikenteestä.

Q2: Miksi minun pitäisi käyttää VPN:ää?

VPN suojaa digitaalista yksityisyyttäsi, turvaa yhteytesi julkisissa Wi-Fi-verkoissa (kuten kahviloissa tai lentokentillä), voi vähentää toimintaan perustuvaa kuristusta, kun operaattori ei pysty tunnistamaan salatun liikenteen tyyppiä, ohittaa maantieteelliset rajoitukset globaalin sisällön käyttämiseksi ja auttaa suojaamaan etätyön resursseja.

Q3: Tekeekö VPN minusta täysin nimettömän verkossa?

Ei. Vaikka VPN piilottaa IP-osoitteesi ja salaa liikenteen, sinua voidaan silti seurata selainevästeillä, aktiivisilla tileillä (kuten Google tai Facebook), selaimen sormenjäljillä tai jos VPN-palveluntarjoajasi kirjaa tietosi.

Q4: Hidastaako VPN internet-yhteyteni nopeutta?

Kyllä, hieman. Salausprosessi ja fyysinen etäisyys VPN-palvelimeen lisäävät viivettä ja kuormaa. Vaikutus vaihtelee palveluntarjoajan, protokollan, palvelimen etäisyyden, laitteen ja verkko-olosuhteiden mukaan.

Q5: Onko VPN:n käyttö laillista?

VPN:n käyttö on laillista monissa maissa, mutta jotkin lainkäyttöalueet rajoittavat, sääntelevät tai estävät VPN-palveluja. Käyttäjien tulisi tarkistaa voimassa olevat paikalliset lait ennen käyttöä. Lisätietoja saat VPN.comin laillisuusoppaista.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa B)

Tutustu yleisimpiin kysymyksiin ja vastauksiin, joita mahdolliset asiakkaat esittävät virtuaalisten yksityisverkkojen käytöstä.

Q6: Voinko käyttää ilmaista VPN:ää?

Ilmaiset VPN:t voivat perustua mainontaan, rajoitettuihin ominaisuuksiin, käyttöanalytiikkaan, datakattoihin tai muihin tulonhankintamalleihin. Käyttäjien tulisi tarkistaa palveluntarjoajan tietosuojakäytäntö, omistus, auditoinnit ja liiketoimintamalli ennen käyttöä.

Q7: Mikä on "ei lokeja" -käytäntö?

Lokittomuuskäytäntö kuvaa, mitä toiminta- ja yhteystietoja palveluntarjoaja ilmoittaa olevansa säilyttämättä. Tarkka laajuus vaihtelee, joten lukijoiden tulisi tarkistaa käytäntö ja riippumattomien auditointien havainnot.

Q8: Miten valitsen parhaan VPN:n?

Etsi auditoituja lokittomuuskäytäntöjä, vahvoja protokollia (WireGuard, OpenVPN), turvallisia palvelinsijainteja, nopeita yhteyksiä, vain RAM-muistia käyttäviä palvelimia, kill switch -toiminto ja lainkäyttöalue tiedusteluyhteistyöliittoumien (kuten 5/9/14 Eyes) ulkopuolella.

Q9: Voinko käyttää VPN:ää puhelimessani ja älytelevisiossani?

Kyllä. Nykyaikaiset VPN-palveluntarjoajat tarjoavat omat sovellukset iOS:lle, Androidille, macOS:lle, Windowsille, Linuxille ja älytelevisioille sekä reititinasennuksia, jotka suojaavat kaikkia kotiverkkosi laitteita.

Q10: Mikä on kill switch?

Kill Switch on tietoturvaominaisuus, joka katkaisee laitteesi internetyhteyden automaattisesti, jos VPN-yhteys katkeaa. Tämä estää salaamattomien tietojesi tai todellisen IP-osoitteesi vuotamisen.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa C)

Tutustu virtuaalisten yksityisverkkojen ja suojattujen tunnelointiprotokollien teknisiin ja rakenteellisiin puoliin.

Q1: Mikä ero on WireGuardilla, OpenVPN:llä ja IKEv2:lla?

WireGuard on nykyaikainen, kevyt protokolla (vain noin 4 000 koodiriviä), joka tarjoaa nopeat nopeudet ja lyhyet yhteysajat. OpenVPN on erittäin turvallinen, käytännössä koeteltu avoimen lähdekoodin protokolla. IKEv2 sopii erinomaisesti mobiililaitteille, koska se osaa yhdistää nopeasti uudelleen verkkoa vaihdettaessa. [4]

Q2: Mitä on kaksois-VPN tai Multi-Hop-reititys?

Multi-Hop reitittää liikenteesi kahden tai useamman VPN-palvelimen kautta peräkkäin. Tämä lisää toisen salauskerroksen ja auttaa pitämään todellisen IP-osoitteesi piilossa toiselta hypyltä, jos yksi palvelin vaarantuu.

Q3: Mitä WebRTC-vuoto on ja miten VPN estää sen?

WebRTC on selainprotokolla, joka voi paljastaa oikeat paikalliset ja julkiset IP-osoitteesi, vaikka VPN olisi käytössä. Premium-VPN:t estävät tai väärentävät WebRTC-pyyntöjä pöytäkone- ja mobiilisovelluksissaan sekä selainlaajennuksissaan.

Q4: Mitä pelkkää RAM-muistia käyttävät palvelimet ovat ja miksi niillä on merkitystä?

Perinteiset palvelimet kirjoittavat dataa kiintolevyille, jotka voidaan takavarikoida tai vaarantaa. Pelkkää RAM-muistia käyttävät (levyttömät) palvelimet toimivat kokonaan haihtuvassa muistissa (RAM). Kun palvelin käynnistetään uudelleen tai sammutetaan, muistissa oleva data pyyhkiytyy.

Q5: Miten obfuskointi ohittaa VPN-estot?

Hämäys (eli "Stealth VPN") naamioi VPN-liikenteen tavalliseksi HTTPS-liikenteeksi (portti 443). Tämä voi auttaa pääsemään ohi syväpakettitarkastuksen (DPI), jota hallitukset tai koulu- ja toimistoverkot käyttävät VPN-yhteyksien estämiseen.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa D)

Tutustu virtuaalisten yksityisverkkojen ja suojattujen tunnelointiprotokollien teknisiin ja rakenteellisiin puoliin.

Q6: Mitä jaettu tunnelointi on ja milloin sitä kannattaa käyttää?

Jaetun tunneloinnin avulla voit valita, mitkä sovellukset reitittyvät salatun VPN-tunnelin kautta ja mitkä yhdistävät suoraan internetiin. Käytä sitä reitittääksesi arkaluonteiset pankkisovellukset VPN:n kautta, kun paikalliset pelit yhdistävät suoraan, jolloin vältät VPN:n aiheuttaman viiveen.

Q7: Miten eteenpäin salassapito (Perfect Forward Secrecy) toimii?

PFS varmistaa, että jokaiselle istunnolle luodaan yksilöllinen, väliaikainen salausavain. Vaikka yksityinen avain vaarantuisi tulevaisuudessa, sitä ei voi käyttää menneiden tai tulevien istuntojen purkamiseen, koska ne käyttivät toisistaan riippumattomia avaimia.

Q8: Mitä 5/9/14 Eyes -liittoumat ovat ja miksi minun pitäisi välittää niistä?

Lainkäyttövalta voi vaikuttaa oikeudelliseen menettelyyn, jonka palveluntarjoaja voi kohdata, mutta käytännön yksityisyysriski riippuu myös siitä, mitä tietoja palveluntarjoaja säilyttää, sen teknisestä arkkitehtuurista, omistuksesta, läpinäkyvyysraportoinnista ja auditointihistoriasta.

Q9: Mitä DNS-vuotosuoja on?

DNS-vuodonesto pakottaa laitteesi lähettämään verkkosivujen hakukyselyt (DNS-kyselyt) VPN:n yksityisten, salattujen DNS-palvelimien kautta internetpalveluntarjoajasi palvelimien sijaan. Tämä estää internetpalveluntarjoajaasi seuraamasta, mitä sivustoja vierailet.

Q10: Voiko VPN ohittaa internetpalveluntarjoajan nopeuden rajoituksen?

Joskus. VPN voi auttaa, kun internetpalveluntarjoaja hidastaa valikoiden tunnistettavia toimintoja, mutta se ei ratkaise verkon ruuhkaa, datarajoituksia, tilikohtaisia nopeusrajoituksia tai heikkoa verkon laatua.

Tekniset viitteet ja lähteet

Tässä tehtävämonisteessa käytetyt lainatut julkaisut, salausmääritykset ja viralliset asiakirjastandardit.

TIETEELLISET JA ALAN VIITTEET

[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