Digikurssi osa 3

- Miten puhdistan tietokoneen evästeistä ja muista haittaavista ja hidastavista tiedostoista?
- Miten VPN toimii ja mitä siitä on hyötyä?
- Wifi-verkon turvallisuus

Porvoon Kansalliset Seniorit
Olli Holopainen kevät 2024

Miten puhdistan tietokoneen evästeistä ja muista haittaavista ja hidastavista tiedostoista?

1.Selaimen evästeiden (cookies) poistaminen: Useimmissa verkkoselaimissa on sisäänrakennettu toiminto evästeiden poistamiseksi. Yleensä tämä löytyy selaimen asetuksista tai historiatiedostojen hallinnasta. Voit poistaa evästeet valitsemalla "Tyhjennä evästeet" tai vastaavan toiminnon.

2.Väliaikaistiedostojen (temperary files) poistaminen: Tietokone kerää väliaikaistiedostoja käytön aikana, ja nämä tiedostot voivat hidastaa sitä ajan mittaan. Voit poistaa nämä tiedostot manuaalisesti tai käyttää erilaisia puhdistusohjelmia, kuten CCleaner, joka on suosittu vaihtoehto Windowsille.

3.Haittaohjelmien (malwares) skannaus ja poisto: Suorita säännöllisesti virustarkistus tietokoneellasi, jotta voit havaita ja poistaa mahdolliset haittaohjelmat, kuten virukset, troijalaiset ja vakoiluohjelmat. Käytä luotettavaa virustorjuntaohjelmistoa ja varmista, että sen virustietokanta on ajan tasalla.

Miten puhdistan tietokoneen evästeistä ja muista haittaavista ja hidastavista tiedostoista?

4. Tarpeettomien ohjelmien poistaminen: Poista tarpeettomat tai käyttämättömät ohjelmat tietokoneeltasi. Voit tehdä tämän ohjauspaneelin tai sovellusten asennuksenhallinnan kautta. Varmista, ettet poista mitään ohjelmia, joita tarvitset, ja ole varovainen, ettet poista järjestelmäohjelmia.

5. Levyn eheytys (defrag): Jos käytössäsi on kiintolevy (HDD), sen eheytys voi auttaa parantamaan suorituskykyä poistamalla tiedostojen hajautumisen. Tämä voidaan tehdä käyttöjärjestelmän sisäisillä työkaluilla, kuten Windowsin Levyn eheytys -työkalulla.

6. Päivitä ohjaimet ja käyttöjärjestelmä: Varmista, että tietokoneesi käyttöjärjestelmä ja laitteiston ohjaimet ovat ajan tasalla. Päivitykset voivat korjata turvallisuusongelmia ja parantaa suorituskykyä.

Miten puhdistan tietokoneen evästeistä ja muista haittaavista ja hidastavista tiedostoista?

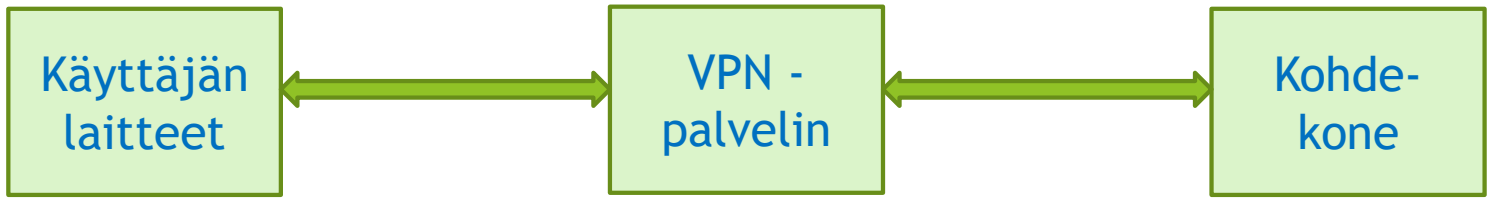
7. Tiedostojen järjestäminen ja siivoaminen: Järjestä tiedostosi kansioihin ja poista tarpeettomat tai vanhentuneet tiedostot säännöllisesti. Tämä auttaa pitämään tietokoneesi järjestyksessä ja vapauttamaan tilaa levyltä.

8. Käytä automaattisia puhdistusohjelmia: Monet ohjelmat, kuten mainitsemani CCleaner, tarjoavat automaattisen puhdistusominaisuuden, jonka avulla voit aikatauluttaa säännölliset puhdistukset ja optimoinnit.

Muista tehdä varmuuskopioita tärkeistä tiedostoista ennen kuin teet suuria muutoksia tietokoneellesi, kuten ohjelmien poistamisen tai rekisterin muokkaamisen. Näin varmistat, että et menetä tärkeitä tietoja vahingossa.

Miten VPN toimii ja mitä siitä on hyötyä?

VPN (Virtual Private Network eli virtuaalinen yksityisverkko) on teknologia, joka mahdollistaa turvallisen ja yksityisen internet-yhteyden luomisen julkisen verkoston kautta. Se toimii salaten internet-liikenteen ja ohjaamalla sen läpi VPN-palvelimen ennen sen saapumista määränpäähän.



Salattu tiedonsiirto

Salattu tunneli

Salattu tiedonsiirto

Salattu tunneli

Miten VPN toimii?

Toiminta:

Salaus: VPN salaa internet-liikenteen, jolloin ulkopuoliset eivät voi helposti seurata tai tarkastella sitä. Tämä suojelee henkilökohtaisia tietoja, kuten käyttäjätunnukset, salasanat ja selaushistorian.

Anonymiteetti: VPN-palvelin toimii välimaastossa käyttäjän ja internetin välillä, piilottaen käyttäjän todellisen IP-osoitteen. Tämä auttaa säilyttämään käyttäjän anonymiteetin verkossa.

Maantieteellisten esto-ohitukset: VPN-palvelinten sijoittaminen eri maantieteellisiin sijainteihin mahdollistaa sen, että käyttäjät voivat ohittaa maantieteelliset esto- tai rajoitukset. Esimerkiksi käyttäjä voi käyttää VPN:ää muuttamaan IP-osoitteensa Yhdysvaltoihin, jolloin hän voi käyttää Yhdysvalloissa saatavilla olevia verkkosisältöjä, jotka muuten eivät olisi saatavilla hänen sijaintimaassaan.

Mitä hyötyä VPN antaa

Turvallisuus: VPN suojaa käyttäjän tietoja kolmansilta osapuolilta, kuten hakkerilta, hallituksilta ja internet-palveluntarjoajilta.

Yksityisyys: VPN auttaa säilyttämään käyttäjän yksityisyyden verkossa piilottamalla IP-osoitteen ja estämällä selaustietojen seurannan.

Sisällön saatavuus: VPN mahdollistaa pääsyn rajoitettuihin tai estettyihin verkkosivustoihin ja palveluihin, jotka saattavat olla estettyjä käyttäjän maantieteellisen sijainnin perusteella.

Turvallinen etätyö: VPN tarjoaa turvallisen yhteyden etätyöntekijöille organisaation verkkoon, mikä on erityisen tärkeää, kun käsitellään arkaluonteisia tietoja.

On tärkeää huomata, että vaikka VPN tarjoaa lisäturvaa ja yksityisyyttä verkossa, se ei kuitenkaan ole täydellinen ratkaisu. Käyttäjien tulisi edelleen noudattaa hyviä tietoturvakäytäntöjä ja varmistaa, että heidän laitteensa ja ohjelmistonsa ovat ajan tasalla. Lisäksi on tärkeää valita luotettava VPN-palveluntarjoaja, jolla on hyvä maine ja joka tarjoaa asianmukaiset tietoturvaominaisuudet.

Mitä hyötyä VPN antaa / Copilot

IP-osoitteen piilottaminen: VPN salaa internet-liikenteesi ja piilottaa IP-osoitteesi. Näin voit selata verkkoa anonyymisti ja suojata henkilöllisyytesi verkkosivustoilta, sovelluksilta ja palveluilta, jotka haluavat tarkkailla toimiasi.

Suoratoistopalvelujen maarajoitusten poisto: VPN mahdollistaa pääsyn suoratoistopalveluihin, kuten Netflix, sijainnistasi riippumatta. Voit vaihtaa IP-osoitteesi ja käyttää palveluita kuin olisit toisessa maassa.

Turvallisempi ja yksityisempi selaus: VPN suojaa sinua turvallisuusuhilta, kuten datapakettien nuuskinnalta, vaarallisilta Wi-Fi-verkoilta ja väliintulohyökkäyksiltä. Erityisesti matkailijat ja etätyöntekijät hyötyvät VPN:n käytöstä.

Valtioiden sensuurin ohittaminen: Jos olet alueella, jossa internetin käyttöä rajoitetaan, VPN auttaa kiertämään sensuuria ja tarjoaa vapaamman internetin.

Mitä hyötyä VPN antaa / Copilot

Halvemmat lentojen hinnat: VPN:n avulla voit vaihtaa sijaintiasi ja saada parempia hintoja esimerkiksi lentolippuihin ja hotelleihin.
Yhteenvetona: VPN on tehokas työkalu yksityisyyden suojaamiseen, maantieteellisten rajoitusten kiertämiseen ja turvallisen verkkoselailun takaamiseen. Kokeile VPN-palvelua ja nauti sen monista eduista!

Mikä on paras VPN-palvelu? / Copilot

ExpressVPN: Se on nopein saatavilla oleva VPN, erittäin turvallinen, helppokäyttöinen ja soveltuu loistavasti suoratoistoon. ExpressVPN tarjoaa myös 30 päivän tyytyväisyystakuun.

CyberGhost: Tämä VPN-palvelu on optimoitu sujuvaan suoratoistoon, nopeaan torrent-lataamiseen ja viiveettömään pelaamiseen.

Private Internet Access (PIA): PIA tarjoaa laajan valikoiman mukautettavia asetuksia, joiden avulla voit tasapainottaa nopeutta ja turvallisuutta.

NordVPN: NordVPN sisältää uhkien suojausominaisuuden, joka estää mainoksia, seurantaa ja haitallisia verkkosivuja.

Surfshark: Surfshark tarjoaa vaihtuvia IP-osoitteita, CleanWebin ja muita ominaisuuksia yhteyden suojaamiseen.

Valitse näistä palveluista se, joka parhaiten vastaa tarpeitasi ja tarjoaa sinulle haluamasi ominaisuudet. Muista myös hyödyntää mahdollisia ilmaisia kokeilujaksoja tai tyytyväisyystakuuta, jotta voit testata palvelua ennen sitoutumista.

Voiko hakkeri höykätä wifi-verkon kautta tietokoneeseen?

Kyllä, hakkeri voi hyökkäyksen avulla päästä tietokoneeseen Wi-Fi-verkon kautta useilla eri tavoilla:

1.Salasanahyökkäykset: Hakkeri voi käyttää erilaisia menetelmiä, kuten brute force -hyökkäyksiä tai sanakirjapohjaisia hyökkäyksiä, murtaakseen Wi-Fi-verkon salasanan. Kun hänellä on verkon salasana, hän voi päästä verkon sisäiseen tietoliikenteeseen ja mahdollisesti hyökätä tietokoneisiin, jotka ovat verkon takana.

2.Verkkoliikenteen vakoilu: Hakkeri voi käyttää verkon liikenteen vakoilua ja hyödyntää mahdollisia heikkouksia tietokoneissa tai käyttäjissä, jotka ovat yhteydessä Wi-Fi-verkkoon. Tämä voi sisältää esimerkiksi salausprotokollien murtamisen tai tietojen urkinnan.

3.Palomuurihyökkäykset: Hyökkääjä voi kohdistaa tietokoneisiin, jotka ovat Wi-Fi-verkon takana, hyökkäyksiä suoraan verkkotasolla. Tällaiset hyökkäykset voivat kiertää palomuurit tai muiden turvallisuustoimenpiteiden tarjoaman suojauksen.

Voiko hakkeri höykätä wifi-verkon kautta tietokoneeseen?

4. Phishing-hyökkäykset: Hyökkääjä voi lähettää houkuttelevia väärennettyjä viestejä Wi-Fi-verkon käyttäjille, joissa pyydetään heitä avaamaan haitallisia linkkejä tai antamaan arkaluontoisia tietoja, jotka voivat antaa hyökkääjälle pääsyn tietokoneisiin.

On tärkeää pitää Wi-Fi-verkot suojattuina käyttämällä vahvoja salasanoja, päivittämällä laitteiden ohjelmistoja säännöllisesti ja varmistamalla, että käytössä on asianmukaiset tietoturvaohjelmat. Lisäksi varovaisuus verkossa toimittaessa ja epäilyttävien viestien ja linkkien välttäminen voi auttaa vähentämään riskiä Wi-Fi-verkon kautta tapahtuvilta hyökkäyksiltä.