

**Pysy
turvassa
jo tänään!**

NÄIN VÄLTYT NÄKYMÄSTÄ:

Piiloudu it-rikollisilta

Tietokoneet ja puhelimet ovat nykyään alttiina monille uhille. Tässä on kaksitoista vinkkiä, joilla voit välttää rikollisten huomion verkossa.



Toimittaja
Henning Rasmussen

Jopa it-asiantuntijoiden ja tietokonelehtien toimittajien voi olla vaikeaa tunnistaa kaikkia nykyisin leviäviä kehittyneitä huijausyrityksiä.

Haitalliset, tuntemattomilta verkkosivustoilta peräisin olevat evästeet voivat seurata liikkeitäsi verkossa. Hakkerit yrittävät päästä tietokoneellesi hyökkäämällä henkilökohtaiseen IP-osoitteeseesi, jonka tietokoneesi paljastaa, kun vieraillet verkkosivustoilla tai napsautat haitallisten sähköpostiviestien linkkejä. Identiteettivarkaat varastavat kuvasi ja tietosi Facebookista ja luovat sitten uusia profiileja nimelläsi – hyödyntääkseen ystäväsi hyväuskoisuutta.

Uhkia on jonoksi asti

Kaikkien verkossa vaanivien vaarojen lisäksi olet alttiina myös monille

riskeille lähistölläsi. Rikolliset voivat yrittää päästä käsiksi kotisi langattomaan verkkoon. Sitten he pääsisivät kaikille laitteillesi ja voisivat varastaa rahaa ja tietoja – tai saatat huomata, että lentokentän ilmainen Wi-Fi ei olekaan niin turvallinen kuin luulisi. Huonolla onnella voit jopa joutua tilanteeseen, jossa huijarit yrittävät murtautua tietokoneellesi langattomalla bluetooth-yhteydellä, kun luulet olevasi turvallisessa paikassa, kuten kahvilassa tai kokouksessa.

Puhelin voi olla vaarallinen

On olemassa monia uhkia, jotka altistavat tietokoneesi ja sinut jatkuvasti vaaroille, mutta lisäksi useimmilla meistä on tietoturvassa vielä yksi lisäaukko, jota huijarit voivat hyödyntää. Aivan kuten tietokoneesi, myös puhelimesi voi altistua vaarallisille verkkosivustoille, viruksille ja hyökkäyksille puhelimesi IP-osoitteen kautta. Lisäksi huijarit saattavat soit-

taa sinulle, vaikka puhelinnumerosi ei olisi julkisesti saatavilla, koska huijarit soittavat usein summamutikassa satunnaisiin numeroihin.

Tämäntyyppiset huijauspuhelut ovat voimakkaassa kasvussa. Tekoälyä hyödyntämällä sekä näkemällä vaivaa huijarit ovat tulleet paljon paremmiksi siinä, että heidän huijauksensa näyttävät aidolta.

Pysy pois rikollisten tutkista

Emme voi taata, ettei enää koskaan joutu huijauksen uhriksi luettuasi tämän artikkelin. Mutta saat ainakin kaksitoista hyvää vinkkiä siihen, miten voit tehdä hakkereiden ja rikollisten tihutöistä mahdollisimman hankalia.

Tärkeintä on, että yrität tehdä itsestäsi, koneestasi ja puhelimestasi mahdollisimman näkymättömiä – sekä verkossa että todellisessa elämässä. Näytämme kaksitoista tapaa, joilla voit vaikeuttaa rikollisten työtä.



Piiloudu tehokkaasti verkossa

Haluatko välttää joutumasta yhdeksi uhriksi tietoverkkorikollisuuden tilastoihin? Silloin kannattaa piiloutua mahdollisimman hyvin, kun hakkerit ja muut rikolliset etsivät uusia uhreja huijattavikseen.

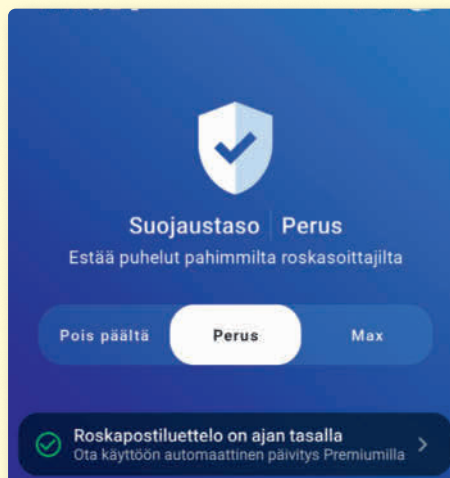
- | | | |
|---|---|-----------------------------------|
| ✓ Suojaudu huijareiden puheluilta | ✓ Tarkista, oletko ehkä jäljitettävissä | ✓ Älä käytä ilmaisia hotspoteja |
| ✓ Piiloudu vieraillessasi tietokoneilla | ✓ Poista tuntemattomat ohjelmat puhelimesta | ✓ Piilota tietosi Facebookissa |
| ✓ Estä näkymisesi ilmaisella VPN:llä | ✓ Käytä aina vahvaa tunnistustaa | ✓ Luo toissijainen sähköpostitili |
| ✓ Piilota langattoman verkkosi nimi | ✓ Ota Wi-Fi ja bluetooth pois käytöstä | ✓ Suojaa tiedostosi salauksella |

Suojaudu huijareiden puheluilta

Monet saavat puheluita Microsoftin työntekijöinä esiintyviltä, epäilyttäviltä sähköyhtiöiltä ja kuvitteellisten tuotteiden myyjiltä. Näin voit suojautua.

Roskapuhelut ovat ärsyttäviä ja pahimmillaan vaarallisia. Tunnistat ne siitä, että soittaja yrittää usein puutteellisella englannilla saada sinut suostumaan tilaamaan jotain tai asentamaan apuohjelman tietokoneellesi. He voivat myös esittäytyä erinomaisella suomen kielellä esimerkiksi pankkisi työntekijöinä.

Useimmissa älypuhelimissa on nykyään toimintoja, jotka tunnistavat ja estävät epäilyttävät numerot. Voit myös ladata Truecaller-sovelluksen Android-puhelimeesi tai iPhoneen ja suojautua siten huijauspuheluilta.



Voit ladata Android- ja iOS-laitteille Truecaller-sovelluksen, joka tarkistaa saapuvat puhelut laajasta huijausnumeroitten luettelosta. Siten saat ajoissa varoituksen rikollisten soitoista.



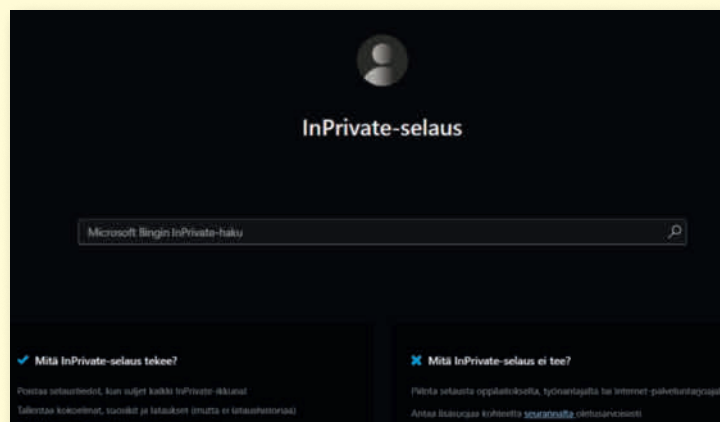
Tämä on tärkeää

• Huijauspuhelut

Joku soittaa ja esittää olevansa esimerkiksi pankista ja yrittää saada sinut siirtämään rahaa tai luovuttamaan tilitietojasi.

• Kalliit puhelut

Sinua pyydetään painamaan näppäintä, jolloin sinut yhdistetään tietämättäsi minuuttihinnaltaan kalliiseen palvelunumeroon.



Käyttämällä InPrivate-toimintoa Edgessä tai Incognito-toimintoa Chromessa tietojasi toiminnastasi tietokoneella verkossa ei tallenneta.



Tämä on tärkeää

• Muut näkevät historian

Jakaessasi tietokoneen muiden kanssa he voivat nähdä, millä sivustoilla olet käynyt: kuten verkkopankit, terveys-tiedot tai etsimiäsi lahjoja.

• Mainokset seuraavat

Ilman incognito-tilaa verkkosivustot voivat tallentaa tietoja tietokoneellesi ja näyttää sitten mainoksia kaikista hakemistasi asioista.

Piiloudu vieraillessasi tietokoneilla

Mikäli käytät tietokonetta kirjastossa tai muussa julkisessa paikassa, varmista, että kone ei tallenna tietojasi toiminnastasi.

Avaamalla uudet ikkunat incognito-tilassa Chromessa selain ei tallenna selaushistoriaasi, hakujasi tai luetteloa kotisivuista, joilla olet käynyt. Tämä on kätevää, jos muut käyttävät samaa tietokonetta ja haluat pitää asiat yksityisinä. Chromessa toiminto on nimeltään Incognito-sivu, Firefoxissa Yksityinen ikkuna ja Edgessä InPrivate-ikkuna. Toiminto piilottaa kuitenkin vain jälkesi tietokoneelta. Internetin palveluntarjoajasi ja vierailemasi verkkosivustot voivat edelleen nähdä, mitä teet. Se ei siis ole täydellinen suojaus.



Estä näkymisesi ilmaisella VPN:llä

VPN tarkoittaa virtuaalista erillisverkkoa. Se suojaaa yhteyttä käyttäessäsi nettiä puhelimella tai tietokoneella. Käytännössä VPN toimii niin, että asennat pienen ohjelman, jonka on kehittänyt VPN-palveluntarjoaja. Palveluntarjoajalla on useita palvelimia eri maissa, ja kun muodostat yhteyden johonkin niistä ohjelman avulla, kaikki tietosi lähetetään eräänlaisen suojatun tunnelin kautta. Tämä tar-

koittaa, ettei kukaan voi nähdä, millä verkkosivustoilla käyt, mitä kirjoitat tai missä olet, koska myös IP-osoiteesi on piilotettu tyystin. Tämä on erityisen hyödyllistä, jos käytät langatonta internetiä kahviloissa, hotelleissa tai ulkomailla. VPN-palvelu, kuten esimerkiksi ilmainen Proton VPN, jonka voit tuki ladata verkkosivustoltamme, suojaa sinua samalla myös hakkereilta.

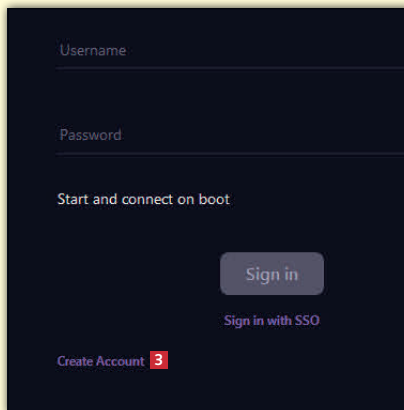


Tämä on tärkeää

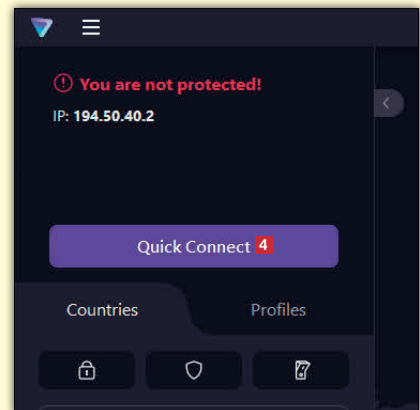
- **Muut näkevät toimintasi**
Julkisissa verkoissa muut voivat nähdä, mitä teet, esimerkiksi kun käytät verkkopankkia tai luet sähköposteja.
- **Sinua seurataan**
Verkkosivustot ja yritykset voivat seurata, mitä katsot verkossa, ja tallentaa sinua koskevia tietoja.



1 Lataa Proton VPN sivustoltamme ja aloita asennus. Asennuksen aikana voit merkitä ehdotettuja ohjelmia **1**. Napsauta vielä lopuksi **Asenna**-painiketta **2**.



2 Ohjelman käynnistyessä ensimmäisen kerran sinun on kirjaututtava sisään ilmaisella tilillä. Tee tili napsauttamalla kohtaa **Create Account** **3**. Kirjaudu tälle tilille.



3 Napsauta ohjelmassa **Quick Connect** -painiketta **4**. Tietokoneesi yhdistyy ensimmäiseen käytettävissä olevaan VPN-palvelimeen, mikä suojaa sen hakkereilta.



Tämä on tärkeää

- **Ei-toivotut vieraat**
Jos verkkosi näkyy muille, lähellä olevat voivat yrittää arvata salasanasasi ja päästä verkkoon.
- **Helppo pääsy hakkereille**
Hakkerit voivat löytää helpommin ulos näkyvän verkon ja yrittää murtautua siihen. Onnistuessaan he voivat nuuskaa tiedostoja, varastaa salasanoja ja häiritä laitteiden toimintaa.

Piilota langattoman verkkosi nimi

Langattomalla verkollasi on nimi, joka näkyy, kun sinä tai naapurisi etsit lähellä olevia Wi-Fi-verkkoja. Piilottamalla ssid-nimen estät verkkoa näkymästä muille.

Piilotettu verkko ei näy muille, joten ei-toivottujen vieraiden on vaikeampi yrittää murtautua Wi-Fi-verkkoosi. Voit edelleen käyttää verkkoa itse, mutta sinun on tiedettävä sen

nimi sekä salasana ja syötettävä ne manuaalisesti ensimmäisellä kerralla, kun haluat yhdistää tietokoneesi tai puhelimesi verkkoon. Voit piilottaa verkon ssid-tunnuksen kirjautumalla reitittimeen selaimella. Etsi langattoman verkon asetukset ja poista valinta kohdasta Näytä verkon nimi tai vastaavasta. Lue lisää reitittimen käyttöohjeesta.

Tarkista oletko jäljitettävissä

Cover Your Tracks -verkkosivustolla voit katsoa, kuinka paljon tietokoneesi paljastaa sinusta, kun olet verkossa. Verkkosivustot voivat tietämättäsi saada tietoja tietokoneesi näytön koosta, käyttöjärjestelmästäsi ja käyttämistäsi ohjelmista. Näitä kutsutaan sormenjäljiksi, ja niitä voidaan käyttää seuraamaan sinua verkossa, vaikka et käyttäisi omaa nimeäsi verkkosivustoilla.

Sivusto testaa selaimesi ja kertoo, kuinka helposti olet tunnistettavissa. Saat myös tietää, kuinka hyvin olet suojattu ja kuinka voit parantaa yksityisyyttäsi verkossa. Kun testi on valmis, saat tietää, kuinka ainutlaatuisia sormenjäljeksi ovat ja kuinka helposti verkkosivustot voivat niiden perusteella tunnistaa sinut ja seurata sinua verkossa. Voit tarvittaessa muuttaa selaimesi asetuksia.



Tämä on tärkeää

• Heikompi yksityisyys

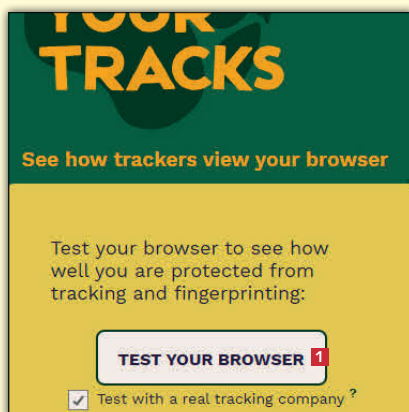
Sivustot voivat tietämättäsi seurata, millä sivuilla käyt, mitä napsautat ja mistä olet kiinnostunut.

• Kohdennettu mainonta

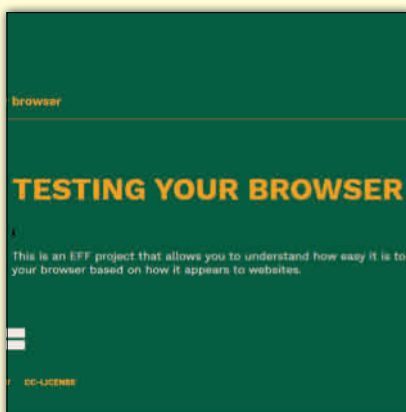
Saat mainoksia verkossa tottumuksesi perusteella.

• Tietojen väärinkäyttö

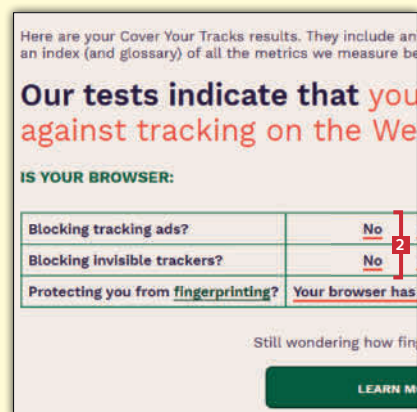
Tietojasi voidaan vuotaa tai myydä ja pahimmassa tapauksessa niitä voidaan käyttää petoksiin.



1 Avaa selaimesi ja siirry sivustolle coveryourtracks.eff.org. Napsauta seuraavaksi kohtaa **TEST YOUR BROWSER** **1**.



2 Verkkosivusto tarkistaa nyt, kuinka alttiina tietokoneesi on jäljittämiseksi verkossa. Tämä kestää 10–20 sekuntia.



3 Mikäli kahdessa kentässä on **No** **2** et ole suojassa seurannalta. Sivustollamme osoitteessa kotimikro.fi/2516 on ohjeet, kuinka suojaat selaimesi seurannalta.



Tämä on tärkeää

• Tietojesi varastaminen

Mikäli olet antanut liikaa käyttöoikeuksia, tuntemattomat sovellukset voivat nuuskaa yhteystietojasi, viestejasi tai kuvia ja lähettää niitä eteenpäin.

• Puhelimen kallis käyttö

Piilotetut sovellukset voivat käyttää saatavilla olevia tietojasi, kuluttaa akkua ja lähettää kalliita tekstiviestejä tietämättäsi.

Poista tuntemattomat ohjelmat puhelimesta

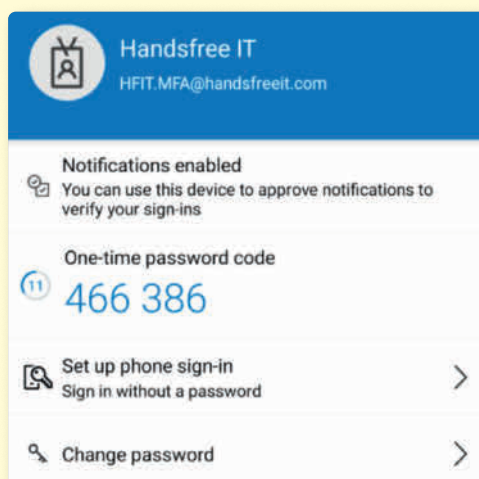
On erittäin suositeltavaa tarkistaa säännöllisesti, mitä sovelluksia puhelimesi on. Luulet ehkä tuntevasi kaikki sovelluksesi, mutta jotkut sovellukset ovat saattaneet asentua huomaamattasi tai niitä on saattanut tulla jonkin muun ladatun sovelluksen mukana. Ellet tunnista jotakin sovellusta puhelimesi sovellusluettelossa, sen tarpeellisuus kannattaa

arvioida tai poistaa se kokonaan. Jotkut sovellukset voivat käyttää yhteystietojasi, sijaintiasi, kameraasi tai mikrofonia ilman, että olet antanut siihen suostumusta. Tämä tarkoittaa, että epäilyttävät sovellukset saattavat tietää sinusta enemmän kuin haluat. Siksi kannattaa ajoittain käydä läpi sovellusten luettelo ja poistaa ne, joita et käytä.

Käytä aina vahvaa tunnistusta

Pelkällä salasanalla suojautuminen on nykyään liian epävarmaa. Siksi kannattaa käyttää myös turvallisia kertakäyttöisiä salasanoja.

Kaksivaiheinen todennus on lisäsuojaus, jonka voit ottaa käyttöön useimmissa verkkopalveluissa. Valitsemasi salasanan lisäksi sinun on käytettävä kertakäyttöistä salasanaa, joka lähetetään tekstiviestinä puhelimeesi tai toimitetaan tähän tarkoitettuun sovelluksella. Vaikka joku arvaisi salasanasi, hän ei voi kirjautua sisään ilman kertakäyttöistä salasanaa. Kaksivaiheinen todennus otetaan yleensä käyttöön käyttämäsi palvelun asetuksissa. Sen määrittäminen vie vain hetken, mutta se vaikeuttaa huomattavasti tietoihisi pääsyä.



Sovelluksella, kuten Microsoftin ilmaisella Authenticatorilla, saat turvallisia kertakäyttöisiä salasanoja.



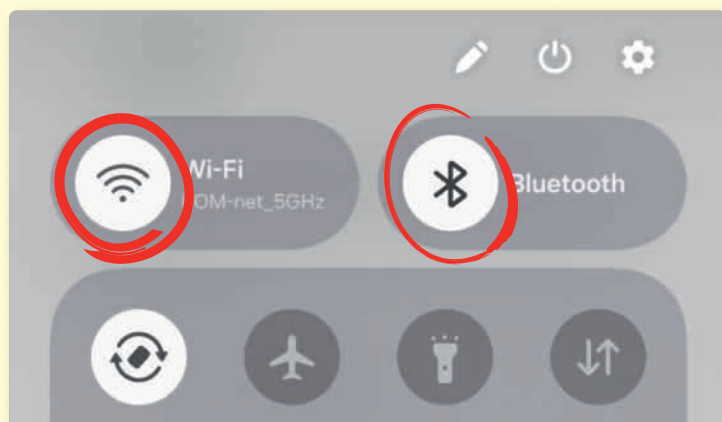
Tämä on tärkeää

• Tilisi hakkerointi

Jos joku arvaa tai varastaa verkkopalvelun salasanasi, hän voi päästä käsiksi esimerkiksi sähköpostiisi, kalenteriisi tai Facebook-tiliisi.

• Tietojen väärinkäyttö

Tiillesi päässyt hakkeri voi lukea viestejasi, lähettää sähköposteja nimelläsi tai vaikka varastaa henkilökoh-
taisia tietojasi.



Useimmissa puhelimissa bluetoothin ja Wi-Fi:n saa helposti pois päältä vetämällä kahdella sormella näytöllä. Napsauta niiden kuvakkeita.



Tämä on tärkeää

• Sinua voidaan seurata

Wi-Fi- ja bluetooth-yhteyksien ollessa päällä puhelimesi voi lähettää signaaleja, joiden avulla muut voivat seurata liikkeitäsä.

• Hakkerit voivat käyttää

Avoimet signaalit, kuten bluetooth ja Wi-Fi, voivat antaa huijareille helpon pääsyn puhelimeesi tai käyttämään yksityisiä tietojasi.

Ota Wi-Fi ja bluetooth pois käytöstä

Langattomat tekniikat, kuten Wi-Fi, NFC ja bluetooth, ovat lähes välttämättömiä, mutta ne voivat myös altistaa sinut hyökkäyksille.

Wi-Fi- ja bluetooth-yhteydet kannattaa ottaa pois käytöstä puhelimesta silloin, kun niitä ei tarvita – etenkin kun olet ulkona. Langattomien teknologioiden ollessa päällä puhelin etsii jatkuvasti verkkoja ja laitteita, mikä voi altistaa sinut vaaroille. Tuntemattomat henkilöt saattavat yrittää muodostaa yhteyden puhelimeesi tai seurata tietämättäsi liikkeitäsä langattomien signaalien kautta. Sammuttamalla Wi-Fi- ja bluetooth-yhteydet – kun et käytä niitä – säästät akkua ja vaikeutat ulkopuolisten henkilöiden mahdollisuuksia nuuskaa tietojasi.

Vältä ilmaisia hotspoteja

Voi tuntua keitaalta autiomaassa, kun näet ilmaisen langattoman verkon kahvilassa tai lentokentällä, mutta verkko voi vaarantaa turvallisuutesi.

Ilmainen Wi-Fi ravintoloissa, hoteleissa tai lentokentillä voi olla houkutteleva, kun ha-
luat lukea sähköpostisi tai uutiset, mutta se ei ole aina turvallista. Jos muodostat yhteyden avoimeen verkkoon, muut samassa verkossa olevat henkilöt voivat seurata, mitä teet – esimerkiksi nähdä salasanasi, sähköpostisi tai muita yksityisiä tietojasi. Joskus taitavat huijarit luovat jopa väärennetyjä hotspoteja, jotka näyttävät oikealta verkolta, jolloin tietokoneesi onkin yhteydessä suoraan rikollisten verkkoon. Siksi kannattaa välttää avoimia verkkoja.



Mikään ei ole niin houkuttelevaa kuin ilmainen, mutta joissakin tapauksissa riskinä on henkilökohtaisten tietojen vaarantuminen.



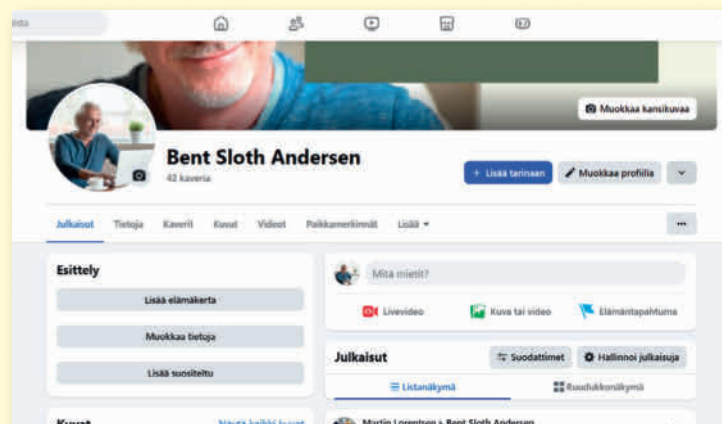
Tämä on tärkeää

• Tietojen paljastuminen

Saman verkon käyttäjät voivat saada käsiinsä henkilökohtaiset salasanasi, sähköpostisi ja samalla muita yksityisiä tietojasi.

• Väärennetyt hotspotit

Kokenut hakkeri voi luoda aidolta näyttävän langattoman verkon ja päästä sitä kautta käsiksi puhelimeesi tai tietokoneeseesi.



Tällä Facebook-tilillä henkilökohtaiset tiedot, merkinnät ja kuvat on piilotettu muilta kuin kavereilta, joten kukaan ulkopuolinen ei voi nähdä niitä.



Tämä on tärkeää

• Identiteettivarkaus

Huijarit voivat väärinkäyttää tietojasi, julkaisuja ja kuvia luodakseen vääriä profileja tai huijatakseen muita sinun nimissäsi.

• Murrot ja petokset

Esimerkiksi lomaan liittyvien tietojen jakaminen Facebookissa voi antaa murtovarkaalle vihjeen siitä, ettet ole kotona vähään aikaan.

Piilota Facebookin tietosi

Ystäviini on mukavaa pitää yhteyttä Facebookissa, mutta väärinkäytösten estämiseksi varmista, että jaat kuvia ja tietoja vain kavereille, jotka tunnet.

Facebookissa kannattaa piilottaa henkilökohtaiset tiedot ja kuvat. Sitten ne eivät näy tuntemattomille. Vaikka tiedot asuinpaikastasi, puoliosastasi tai etelänlomastasi saattavat tuntua harmittomilta, ne voivat helposti joutua rikollisten käsiin. Pahimmassa tapauksessa tietoja voidaan käyttää petoksiin tai identiteettivarkauksiin, ja myös murtovarkaatt voivat päätellä tiedoista, milloin et ole kotona. Facebookin asetuksissa voit valita, että vain kaverisi voivat nähdä jakamasi sisällön, jotta tuntemattomat eivät näe yksityiselämäsi kuuluvia tietoja.



Tämä on tärkeää

• Hukut roskapostiin

Vain yhtä sähköpostiosoitetta käytettäessä postilaatikko täyttyy nopeasti uutiskirjeistä ja turhista viesteistä, jolloin tärkeät sähköpostit voivat jäädä huomaamatta.

• Suurempi petosriski

Jos osoitteesi leviää verkossa, se voi päätyä väärin käsiin ja sitä voidaan käyttää huijauksiin tai identiteettivarkauteen.

Luo toissijainen sähköpostitili

Yksityisen sähköpostiosoitteen lisäksi kannattaa luoda toinen osoite toissijaisiin tarkoituksiin. Voit käyttää yksityistä tiliä henkilökohtaisiin asioihin, kuten verkkopankkiin, sähköiseen postilaatikkoon, lääkäriin sekä yhteydenpitoon perheen ja ystävien kanssa. Toisen osoitteen voi helposti luoda esimerkiksi osoitteessa **gmail.com**. Sitä voi käyttää uutiskir-

jeisiin, kilpailuihin, verkkokaupoissa ja silloin kun on vain annettava osoite. Tämä suojaa sinua lukuisilta mainoksilta ja ei-toivotuilta sähköposteilta, jotka muuten täyttäisivät nopeasti postilaatikkosi. Samalla vähenee petosten riski, koska et jaa tärkeää sähköpostiosoitettasi joka paikkaan. Jos toinen osoitteesi täyttyy roskapostista, voit poistaa sen ja luoda uuden.

Lataa Guardian Of Data sivulta kotimikro.fi/2516



Suojaa tiedostosi salauksella

Tietokoneesi kiintolevyllä kaikki tiedostosi ovat yleensä täysin suojamattomia, joten varkaat tai muut ulkopuoliset henkilöt voivat esimerkiksi lukea asiakirjojasi tai katsella valokuviasi. Jos kuitenkin salaat tiedostosi, ne lukitaan digitaalisella avaimella, jolloin vain sinä voit avata ne. Tämä koskee erityisesti arkaluontoisia tietoja, kuten kirjeitä, tilittietoja tai yksityisiä valokuvia. Sa-

lauksella ne muuttuvat täysin lukekelvottomiksi niille, joille et ole myöntänyt käyttöoikeutta. Jos koneessasi on Windows 11 Pro, se sisältää jo salausohjelman BitLocker-toiminnon muodossa. Muussa tapauksessa tiedostot voidaan suojata ilmaisella Guardian Of Data -ohjelmalla, jonka voit ladata verkkosivuiltamme. Salaus suojaa siis muistosi ja kaikki henkilökohtaiset tietosi.



Tämä on tärkeää

• Tietojen vuotaminen

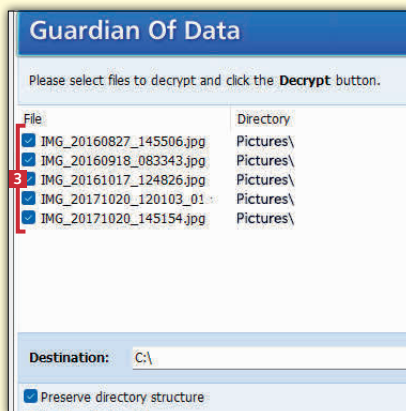
Jos joku pääsee käsiksi tietokoneeseen, hän voi nähdä asiakirjasi, kuvasi ja muut tiedot.

• Identiteettivarkaus

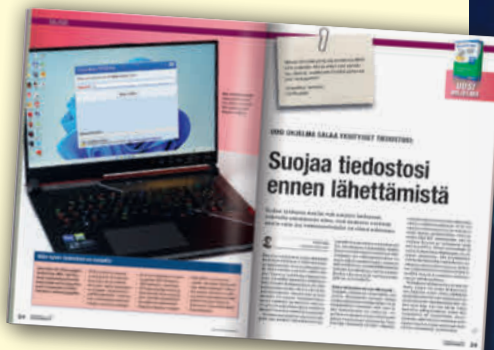
Huijarit voivat käyttää henkilökohtaisia tietojasi, kuten henkilötunnusta ja pankkitietoja, esiintyäkseen sinuna.



1 Lataa ohjelma verkkosivuiltamme ja asenna se. Napsauta **Encrypt**-painiketta **1** salataksesi tiedot, kun ohjelma käynnistyy. Tiedot avataan valitsemalla **Decrypt** **2**.



2 Valittuasi **Decrypt**-toiminnon voit valita, mitkä tiedot **3** avataan. Siten sinun ei tarvitse avata kaikkia tietoja vain yhden tiedoston hakemista varten.



Voit hakea verkkosivuiltamme Guardian Of Data -ohjelman täydelliset ohjeet. Täältä löydät kaikki tiedot siitä, miten voit suojata tiedostosi ohjelmalla.