



tehokasta tietoturvavinkkiä

Internetissä, puhelimella ja tietokoneella toimiminen on täynnä tuntemattomia sudenkuoppia. Annamme sata huolellisesti valittua turvallisuusvinkkiä, jotka tekevät digitaalisesta elämästäsi heti paljon turvallisempaa.



Toimittajat
Martin Lorentsen
Henning Rasmussen

Valitettavasti huonoja uutisia riittää, kun kyse on digitaalisten viestintävälineiden, kuten tietokoneen ja puhelimen käytöstä. Sitä mukaa kun olemme tulleet yhä riippuvaisemmiksi elektronisista laitteista, huijarit ovat yrittäneet hyödyntää kyseistä asiaa erilaisissa petoksissa.

Kyberhyökkäykset ovat nykyään suurempi uhka jokapäiväiselle elämällemme kuin koskaan aiemmin. Ja tekoälyn yleistyessä suuntaus on vain pahentunut – ammattimaiset huijarit

kun ovat saaneet käyttöönsä tehokkaan työkalun, jolla he voivat automatisoida rikollisia toimiaan.

Laajamittaisia petoksia

Olemme tähän mennessä nähneet jo lukuisia esimerkkejä siitä, kuinka tekoälyä käytetään väärennetyjen videoiden, äänien ja tekstien luomiseen. Tarkoituksena on huijata varomattomilta uhreilta arkaluontoisia tietoja, kuten salasanoja ja maksutietoja.

Vaikka huijarit hyödyntävät yhä enemmän uutta teknologiaa uusissa huijausmenetelmissä, myös vanhat menetelmät ovat edelleen käytössä. Identiteettivarkaudet, joissa Facebook-kuvia ja tietoja käytetään luo-

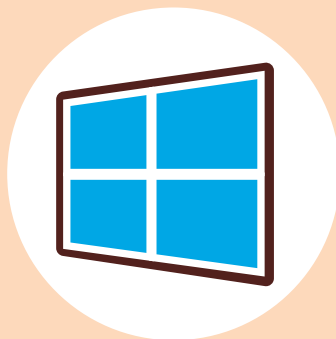
maan väärä henkilöllisyys jonkin toisen huijauksen osana, ovat edelleen yleisiä. Voit myös edelleen joutua huijatuksi ja ostaa niin sanotusti sian säkissä, kun teet ostoksia verkossa. Eivätkä huijarit ole suinkaan lopettaneet sähköpostilaatikkojen pommitamista tietojenkalasteluviesteillä.

Sata tehokasta turvavinkkiä

Valitettavasti kekseliäät rikolliset ovat lähes aina askeleen edellä uhrejaan. Voit kuitenkin tehdä paljon minimoidaksesi hyökkäysten riskin, mutta se edellyttää, että tiedät, mitä pitää tehdä. Annamme tässä sata tehokasta turvallisuusvinkkiä, jotka suojaavat sinua parhaiten nykypäivän uhilta.



Sähköposti



Windows



Verkko



Salasanat



Ohjelmat



Puhelin



Facebook



Selain



Verkkokauppa

1

Käytä vahvoja salasanoja

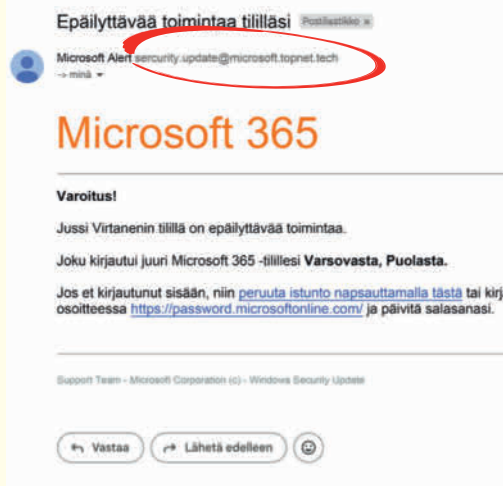
Tärkein suoja sähköpostitiliäsi väärinkäyttäviä rikollisia vastaan on suojata se vahvalla salasanalla. Hakkerit ja huijarit yrittävät jatkuvasti päästä käsiksi sähköpostitileihin kehittyneiden ohjelmien avulla, mutta joutuvat luopumaan, jos salasana on liian vaikea. Voit lukea tästä lisää verkkosivuiltamme osoitteesta kotimikro.fi/2513.

2

Tarkista sähköpostin lähettäjä

Väärennetyt sähköpostit ovat usein niin huolellisesti tehtyjä, että vain pienet yksityiskohdat paljastavat ne huijauksiksi. Tarkista siis erityisen huolellisesti lähettäjän osoite.

Kun katsot tarkemmin lähettäjän osoitetta, niin se on usein aivan eri kuin mitä pyritään esittämään.



3

Älä jaa kaikkea sähköpostitse

Tavalliset sähköpostit ovat turvattomia, koska niiden sisältöä ei ole salattu. Älä siis koskaan lähetä sähköpostitse arkaluonteisia henkilötietoja, kuten henkilötunnusta, passin kopiota tai vastaavia, vaan käytä sen sijaan turvallista ratkaisua.

4

Älä anna taitavien huijareiden hämätä

Sosiaalisen manipuloinnin tekniikalla rikolliset voivat huijata uhreja uskomaan, että he ovat saaneet sähköpostia lapseltaan, joka tarvitsee kiireellistä taloudellista apua ongelman ratkaisemiseksi. Huijarit ovat tulleet niin taitaviksi, että kannattaa aina ottaa suoraan yhteyttä pyytäjään, jos joku pyytää sinua siirtämään rahaa tai lähettämään henkilökohtaisia tietoja.

5

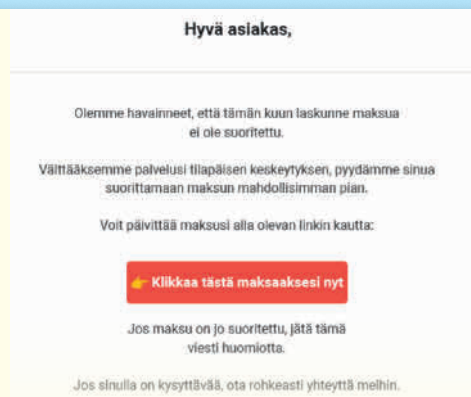
Salaa arkaluontoiset tiedot sähköposteissa

Emme suosittele henkilötietojen lähettämistä sähköpostitse, koska sähköpostitekniikka ei ole riittävän turvallinen tähän tarkoitukseen. Jos lähetät sähköpostia, joka sisältää tietoja, joiden joutumista väärin käsiin et halua riskeerata, tarkista sähköpostitilisi asetuksista, onko sisältö mahdollista salata S/MIME-tekniikalla. Vaihtoehtoisesti voit harkita sähköpostiohjelmasi suojaamista OpenPGP:llä tai vastaavalla palvelulla.

6

Älä avaa tuntemattomia linkkejä

Kun saat sähköposteja yrityksiltä, niissä olevat linkit on usein naamioitu painikkeiksi tai kuviksi, ja niiden napsauttaminen voi olla vaarallista. Voit selvittää, minne linkkipainike johtaa, kun viet hiiren osoittimen painikkeeseen päälle. Turvallisinta on kuitenkin olla napsauttamatta linkkejä.



Tässä väärennetyssä sähköpostissa olisi houkuttelevaa napsauttaa punaista painiketta, mutta se johtaa huijaussivustolle.

7

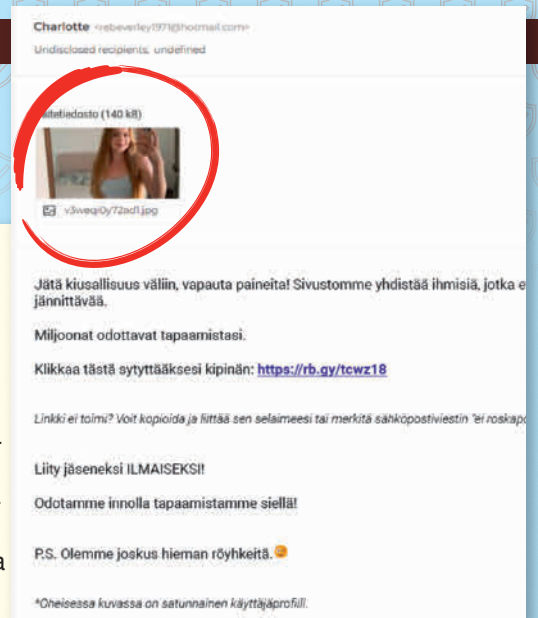
Käytä kaksivaiheista tunnistautumista

Useimmissa sähköpostipalveluissa voi käyttää uutta ja turvallista kirjautumismenetelmää, jota kutsutaan kaksivaiheiseksi tunnistautumiseksi. Kirjautumisen ensimmäisessä vaiheessa käytetään tavallista salasanaa. Sen jälkeen saat kertakäyttökoodin. Lue aiheesta lisää verkkosivuiltamme osoitteesta kotimikro.fi/2513.

8

Älä avaa viestien liitetiedostoja

Huijareilta tulevissa sähköpostiviesteissä on usein yksi tai useampi liitetiedosto. Exe-päätteiset ohjelmatiedostot ovat tunnetusti vaarallisia, mutta uhka koskee myös muita tiedostotyyppisiä. Rikollisista on tullut niin taitavia, että jopa kuvallitteet voivat olla vaarallisia, koska ne saattavat sisältää haitallista ohjelmakoodia.



Viesteihin liitettyjen kuvien avaaminen voi olla vaarallista.

9

Huomioi viestin kieli ja sävy

Jos ostat ajoittain tavaroita verkosta, saatat saada sähköpostiviestejä kuljetusyrityksiltä, kuten DAO tai GLS. Ennen kuin noudatat viestissä annettuja ohjeita, viestin kieliasu kannattaa tutkia huolellisesti. Se paljastaa usein huijareiden huonot käännökset.

10

DONATION

KRISTINE WELLENSTEIN <juanb@playcomia.com.ar>

13.2025 - 15.2025

Ti: Recipients

This is a reminder to claim a \$6,500,000 (6.5 million USD) donation from Kristine wellenstein the jackpot winner, Funds are donated to support individuals and companies. Your email has been selected as one of the lucky winners.

Send a claim request to (wellensteinkristine4@gmail.com)

Stay Blessed.
Kristine Wellenstein.

Vaikka voi olla houkuttelevaa saada viesti palkinnosta, siihen kannattaa aina suhtautua varauksella, ellet tunne lähettäjä.

Suhtaudu varauksella viesteihin, joiden lähettäjä et tunne

On täysin inhimillistä, että luontainen varovaisuutemme katoaa, kun meitä houkutellaan suurilla lupauksilla. Ainakin nigerilaiset huijarit ovat vuosien ajan menestyneet viesteillä, joissa he huijaavat uhreja uskomaan, että heitä odottaa suuri summa rahaa, koska he ovat – yllätys, yllätys – sukua kuolleelle varakkaalle henkilölle.

Tällainen lupaus voi tietysti houkutella monia, mutta jos lähettäjän nimi on sinulle täysin tuntematon, emme suosittele aloittamaan keskustelua. Jos vastaat jotain väärennettyihin sähköposteihin, voit nopeasti joutua vaaralliseen valheiden verkkoon, jossa päädyt kuitenkin luovuttamaan rahaa tai tietoja.

GLS.

Ilmoitus vireillä olevasta toimituksesta

Hyvä asiakas,

Ilmoitamme sinulle, että pakettisi odottaa toimitusta. Vahvista paketin vastaanotto klikkaamalla alla olevaa linkkiä 48 tunnin kuluessa, jotta lähetystyö voidaan jatkaa.

Paketin numero: FUD48515287362

Lähetetty: 20/02/2025

Vahvista vastaanotto klikkaamalla seuraavaa linkkiä: Vahvista vastaanotto.

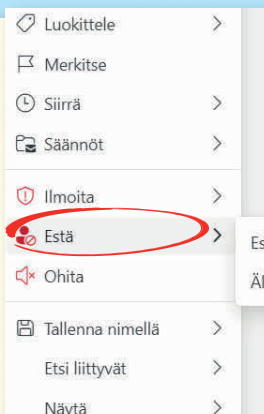
Jos sinulla on kysyttävää, ota rohkeasti yhteyttä sosiaalisessa mediassa tai asiakaspalvelussamme.

Huijausviestien kielenkäyttö paljastaa usein heikon konekäännöksen käytön.

11

Estä ei-toivotut sähköpostiviestit

Kaikki lailliset yritykset, jotka lähettävät sinulle uutiskirjeitä ja muita viestejä, antavat sinulle myös mahdollisuuden peruuttaa helposti viestien lähetys. Jos saat viestejä lähettäjiltä, joilta et niitä halua, voit estää ne luomalla suodattimen sähköpostipalveluissa, kuten Gmailissa. Katso ohjeet täältä: kotimikro.fi/2513.

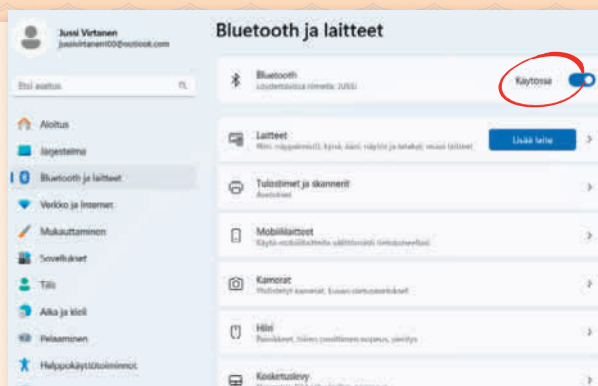


Jos lähettämistä ei voi peruuttaa, voit estää lähettäjän viestit.

12

Ota bluetooth pois päältä, kun et tarvitse sitä

Bluetooth on loistava langaton tekniikka, jolla voi yhdistää helposti esimerkiksi kuulokkeet tietokoneeseen. Myös rikolliset voivat kuitenkin hyödyntää sitä, joten katkaise yhteys, kun et käytä sitä.



Windowsin asetuksista voit helposti kytkeä bluetooth-yhteyden päälle ja pois päältä. Kun yhteys on pois päältä, muut laitteet eivät voi löytää laitettasi.

14

Päivitä Windows

Windows pyytää usein juuri huonolla hetkellä suorittamaan päivityksen ja käynnistämään tietokoneen uudelleen. Siitä huolimatta suosittelemme, että hyväksyt päivityksen, kun käyttöjärjestelmä pyytää asentamaan sen. Microsoft julkaisee nimittäin tärkeitä tietoturvapäivityksiä, jotka korjaavat nykyiset tietoturva-aukot, joita häikäilemättömät rikolliset voisivat muuten hyödyntää viipymättä.

15

Tee säännöllisesti varmuuskopioita

Vaikka voit estää useimmat onnettomuudet noudattamalla näitä vinkkejämme, huonolla onnella voit silti saada haittaohjelman tai kiristysohjelman, joka vahingoittaa tai salaa tiedostojasi. Jos näin tapahtuu, on vain yksi keino palauttaa tiedostot. Luo tiedostoista varmuuskopio, josta voit palauttaa ne. Lataa esimerkiksi Hasleo Backup Suite sivulta [kotimikro.fi/2513](https://www.kotimikro.fi/2513).

13

Suojaa tietokone hyökkäyksiltä

Windows 10:ssä ja 11:ssä on monia turvatoimia, jotka auttavat pitämään tietokoneesi suojatuna. Näihin kuuluu esimerkiksi **Hyökkäysten esto**, joka suojaa tietokoneesi haavoittuvuuksia haitalliselta koodilta.

Hyökkäysten esto

Perehdy järjestelmän ja ohjelmien hyökkäysten eston asetuksiin mukauttaaksesi haluamiasi asetuksia.

Järjestelmäasetukset Ohjelma-asetukset

Hallintavirran suojaus (CFG)

Varmistaa hallintavirran yhtenäisyyden epäsuorissa puheluissa.

Käytä oletusta (Käytössä)

Tietojen toteutuksen esto (DEP)

Estää koodin ajamisen vain-tiedot-muistisivuilta.

Käytä oletusta (Käytössä)

Pakota kuvien satunnaistaminen (pakollinen ASLR)

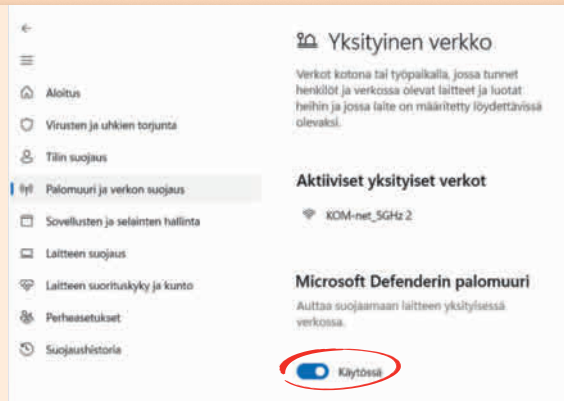
Pakota kuvien siirto, jos niitä ei ole koottu kohteella /DYNAMICBASE

Varmista Windowsin asetuksista, että kohdassa **Hyökkäysten esto** on käytössä **Hallintavirran suojaus**.

16

Suojaa liikenne palomuurilla

Palomuri on tärkeä osa tietokoneen tietoturvaa. Kaikki ohjelmat ja toiminnot, jotka käyttävät verkkoa tai internetiä, kulkevat ensin Windowsin palomuurin läpi, mikä parantaa tietoturvaa. Tarkista siis asetuksista, että tietokoneessa on varmasti käytössä palomuri.



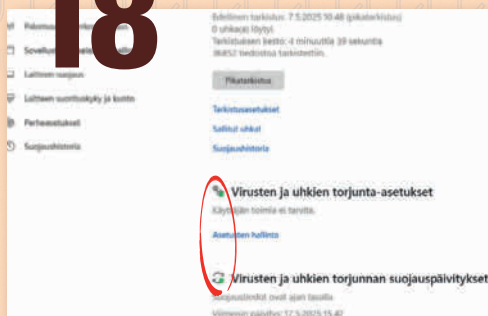
Windowsin asetuksissa on valikkokohta nimeltä **Windowsin suojaus**. Sieltä näet hetkessä, toimiiko tietokoneesi palomuri niin kuin pitää.

17

Vaihda paikalliseen tiliin

Jos olet huolissasi tietojen siirtämisestä tietokoneeltasi nettipalvelimille, voit käyttää paikallista käyttäjätiliä tietokoneellasi Microsoft-tilin sijaan. Microsoft-tilillä tietoja siirretään tietokoneesi ja Microsoftin palvelimien välillä, josta voit esimerkiksi synkronoida asetukset eri tietokoneiden välillä. Katso verkkosivustoltamme, miten paikallinen tili luodaan: [kotimikro.fi/2513](https://www.kotimikro.fi/2513).

18



Windowsin suojauksessa vihreällä merkityt kohdat merkitsevät, että virustorjuntaohjelma on päällä eikä laite ole uhattuna.

Varmista, että virustorjunta on käytössä

Tietokoneesi tärkein tietoturvaohjelma on virustorjuntaohjelma, joka valvoo jatkuvasti kaikkia verkosta lataamiasi tiedostoja ja tietokoneella käynnistettyjä ohjelmia. Siksi on myös erittäin tärkeää, että ohjelma on päivitetty uusimmilla virustunnisteilla, että se toimii ja suojaa sinua aktiivisesti taustalla.

Voit tarkistaa tämän Windowsin asetuksista kohdasta **Windowsin suojaus**. Napsauta vain kohtaa **Virusten ja uhkien torjunta-asetukset**.

19

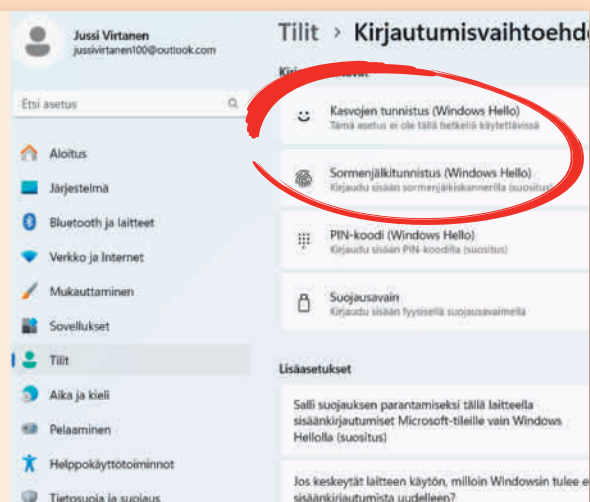
Älä käytä vanhentuneita ohjelmia

Tämä neuvo voi tuntua turhalta, jos olet juuri ladannut ohjelman uusimman version, mutta se on nimenomaan ratkaisevan tärkeää turvallisuuksesi kannalta. Rikolliset ovat taitavia löytämään uusia tietoturva-aukkoja tunnetuista ohjelmista. Voit välttää tämän pitämällä ohjelmat ajan tasalla valmistajan uusimmilla tietoturvapäivityksillä.

20

Kirjaudu biometrisillä tunnisteilla

Windowsin **Windows Hello** tarjoaa mahdollisuuden kirjautua tietokoneelle kasvojentunnistuksella tai sormenjäljellä. Niiden väärentäminen on paljon vaikeampaa kuin murtaa salasana.



Asetusten kohdassa **Kirjautumisvaihtoehdot** voit valita kasvojentunnistuksen tai sormenjälkitunnistuksen.

21

Katso mitä taustalla on käynnissä

Näet käynnissä olevat ohjelmat ja palvelut Windowsin **prosesseista**.

Täältä näet myös kaikki taustalla käynnissä olevat ohjelmat, joilla ei ole kuvaketta tehtäväpalkissa. Vaikka useimmat taustapalvelut ovat Windowsin omia ja niiden nimet eivät välttämättä sano juuri mitään, luettelo kannattaa silti tarkistaa ajoittain. Jos huomaat jotain epäilyttävää, skannaa tietokoneesi virusten ja haittaohjelmien varalta.

Sovellukset (3)	Käynnistetty	0%	0 Mi	0 Mi/s	0 Mi/s
Asiakaset					
Google Chrome (11)		0%	213.9 Mi	0.1 Mi/s	0 Mi/s
Tietävienväylä		4.6%	59.4 Mi	0.1 Mi/s	0 Mi/s
Taustaprosessit (50)					
Aloitus (2)					
AMD Crash Defender S...		0%	25.8 Mi	0 Mi/s	0 Mi/s
AMD External Events C...		0%	0.3 Mi	0 Mi/s	0 Mi/s
AMD External Events S...		0.1%	1.4 Mi	0 Mi/s	0 Mi/s
AMD Software (4)					
AMD Software		0%	0.6 Mi	0 Mi/s	0 Mi/s
Antimalware Core Servi...		0%	90.1 Mi	0 Mi/s	0 Mi/s
Antimalware Service Ex...		0%	7.2 Mi	0 Mi/s	0 Mi/s
Anybet Indexing Engine		0.4%	87.1 Mi	0.1 Mi/s	0 Mi/s
Application Frame Host		0%	4.7 Mi	0 Mi/s	0 Mi/s
		0%	9.9 Mi	0 Mi/s	0 Mi/s

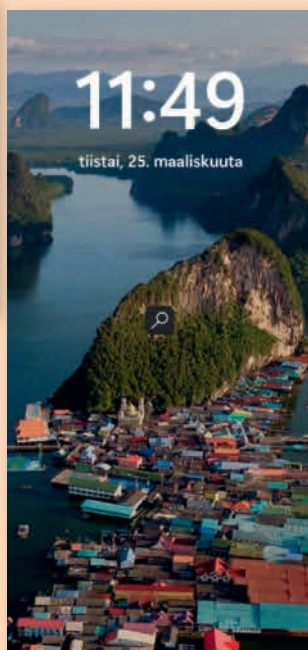
Voit avata **prosessit** näppäinyhdistelmällä **Ctrl + Vaihto + Esc**.

22

Lukitse tietokone, kun et käytä sitä

Käyttäessäsi tietokonetta kotonasi ei ole kovinkaan todennäköistä, että kukaan asiaankuulumaton tutkisi tiedostojasi. Matkoilla tai vaikkapa kahviloissa tietokone kannattaa kuitenkin lukita aina, kun poistut sen äärestä – myös silloin, kun olet pois vain hetken.

Windowsin voi lukita näppäinyhdistelmällä **Windows-painike + L**. Lukituksen avaamiseen tarvitaan salasana.



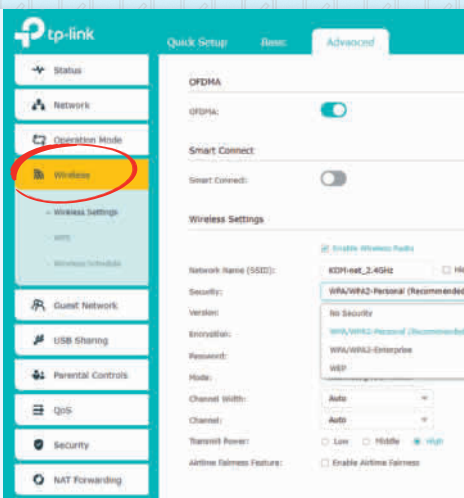


23

Käytä parasta mahdollista salausta

Reitittimen asetuksista voi valita langattoman signaalin salausmenetelmän. Suosittelemme käyttämään uusimpia WPA2- tai WPA3-standardeja. Lue reitittimesi käyttöohjeesta, miten pääset muuttamaan asetuksia.

TP-Linkin reitittimissä valitaan **Advanced**-välilehdeltä kohta **Wireless**.



24

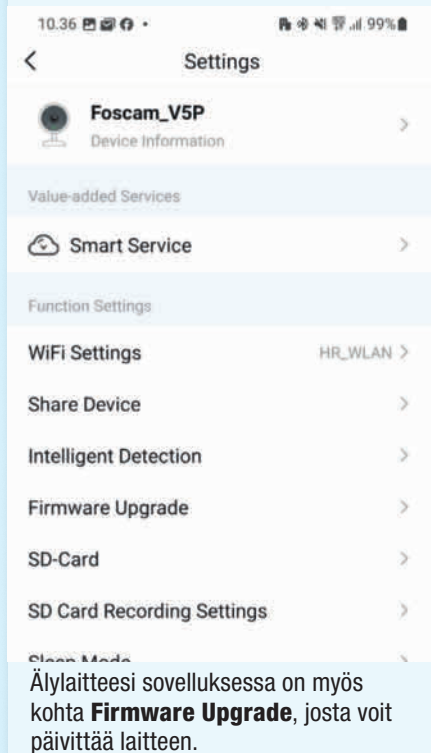
Sulje reitittimesi portit

Reitittimesi käyttämät portit varmistavat, että voit käyttää kotisi laitteita, kun et ole kotona. Jos et tarvitse tätä toimintoa, sulje portit. Katso reitittimesi käyttöohjeesta, miten voit kirjautua reitittimen asetuksiin ja etsiä avoimet portit.

26

Pidä älylaitteesi päivitettyinä

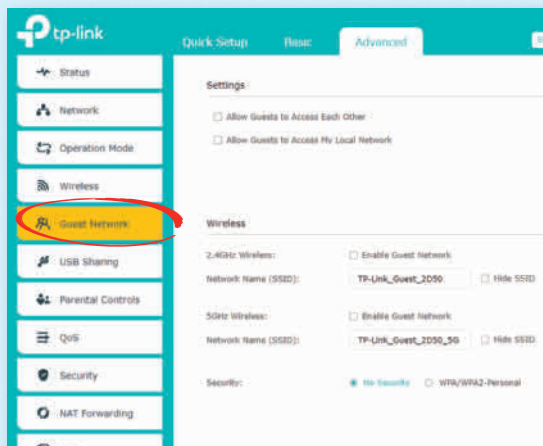
Älylaitteet, kuten pistorasiat ja kamerat, voivat olla turvallisuusriski kaikille verkossasi oleville laitteille. Voit välttää tämän pitämällä älylaitteet ajan tasalla firmware-päivityksillä. Voit tehdä tämän suoraan laitteiden omista sovelluksista.



25

Luo vieraille oma verkkonsa

Useimmat uudemmat reitittimet mahdollistavat ylimääräisen langattoman verkon luomisen, jota voit tarjota vieraiden käyttöön. Tästä vierasverkosta ei pääse muihin verkon laitteisiin, joten vierasverkko sopii hyvin internetyhteyden jakamiseen. Lue reitittimesi käyttöohjeesta, miten vierasverkko tehdään omassa mallissasi.

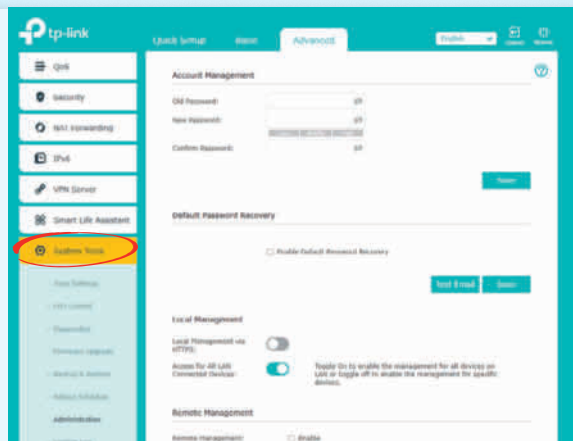


TP-Linkin reitittimissä valitaan **Advanced**-välilehdeltä kohta **Guest Network**.

27

Sulje reitittimen etäohjaus

Onko sinulla koskaan ollut tarvetta päästä käsiksi reitittimeesi, kun et ole ollut kotona? Mikäli ei, ei ole mitään syytä pitää tätä toimintoa päällä. Tarkista reitittimen käyttöohjeesta, miten etäohjauksen voi poistaa käytöstä.

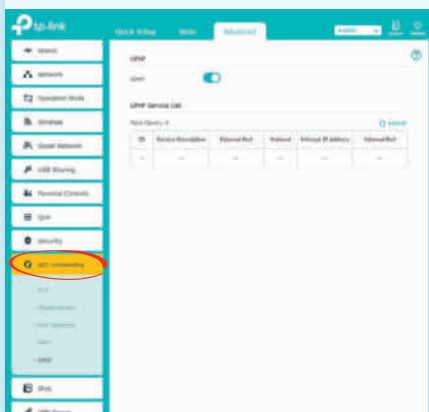


TP-Linkin reitittimissä voit ottaa etäohjauksen pois käytöstä **Advanced**-välilehden kohdasta **System Tools**.

28

Poista UPnP käytöstä reitittimessäsi

Voit lukea lisää reitittimen UPnP-toiminnosta osoitteesta kotimikro.fi/2513. Toiminto oli alun perin suunniteltu helpottamaan eri laitteiden yhdistämistä kotiverkkoon. Käytännössä on kuitenkin käynyt ilmi, että tämä toiminto helpottaa ikävä kyllä myös rikollisten pääsyä verkkoon. Siksi suosittelemme etsimään UPnP-toiminnon reitittimen käyttöohjeesta, kirjautumaan sisään reitittimen asetuksiin ja ottamaan sen kokonaan pois käytöstä.



UPnP-toiminto löytyy usein reitittimen Advanced-välilehdeeltä kohdasta **NAT Forwarding**.

29

Käytä vahvaa WiFi-salasanaa

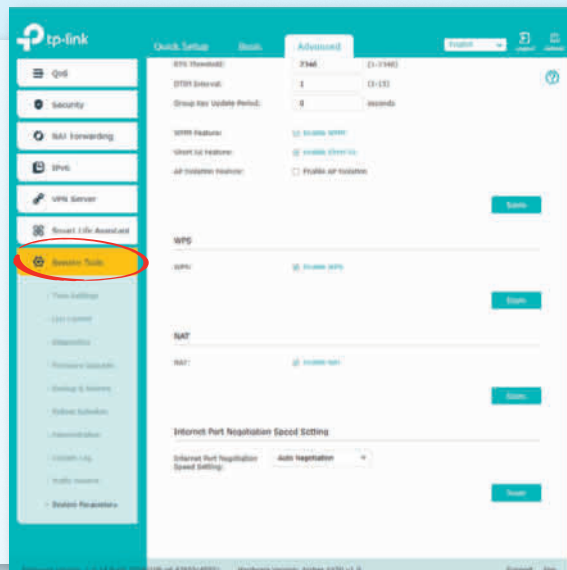
Yksinkertaisten ilmaisujen tai numerosarjojen käyttäminen langattoman verkon salasana on käytännössä kuin kutsu sisään ulkopuolisille. Sama pätee, ellei ole muuttanut valmistajan reitittimen mukana toimittamaa oletussalasanaa. Lue siis reitittimen käyttöohjeesta, miten langattoman verkon salasana vaihdetaan.

31

Sulje reitittimen WPS-toiminto

WPS löytyy sekä reitittimistä että langattomista laitteista, jotka voi liittää verkkoon. Sillä laitteet voi yhdistää painamalla yhtä painiketta, mutta sitä voidaan myös käyttää väärin. WPS:n voi poistaa käytöstä.

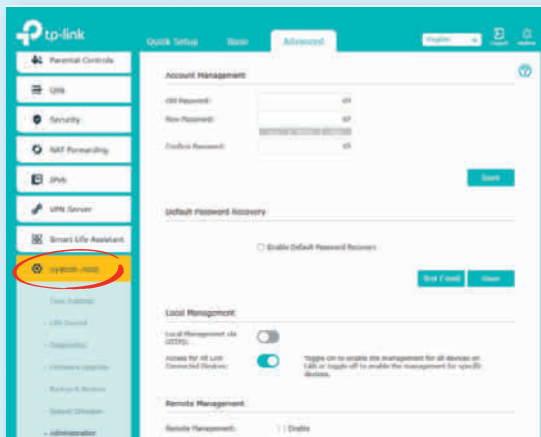
Reitittimen WPS-toiminnon voi mainiosti ottaa pois käytöstä, jos sitä ei tarvitse.



32

Älä pidä langatonta verkkoa aina päällä

Jos lähistöllä asuu muita, voitte nähdä toistenne langattomat verkot. Vaikka verkkoon pääsemisen edellyttää, että vierailija saa käyttöönsä salasanasasi, voit minimoida kutsumattomien vieraiden riskin sammuttamalla reitittimen kokonaan esimerkiksi yön ajaksi.



Yleensä reitittimeen kirjautumisen oletussalasana vaihdetaan **System**-valikosta.

30

Pidä reititin päivitettynä

On tärkeää pitää kaikki laitteet ajan tasalla – sekä tietokone, puhelin että kaikki kodin elektroniset laitteet. Sama koskee reititintä, joka saa usein turvallisuuspäivityksiä valmistajalta. Tarkista siksi säännöllisesti reitittimesi asetuksista, onko uusia päivityksiä saatavilla. Tämä tehdään yleensä Järjestelmä-valikosta.

33

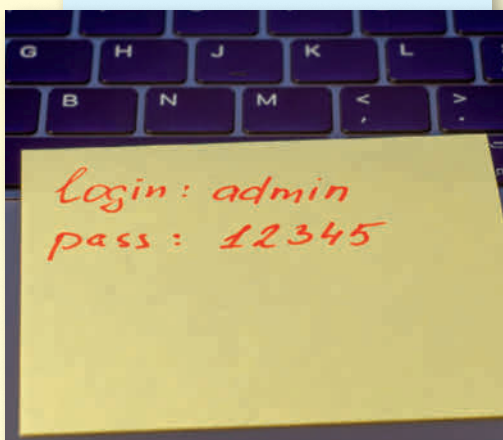
Vaihda reitittimen salasana

Salasana ja usein myös käyttäjätunnus on annettava ennen kuin voit muuttaa reitittimen asetuksia. Siksi on tärkeää, että salasana on juuri itse valitsemasi. Noudata parhaita ja ajantasaisia ohjeita turvallisista salasanoista ja vaihda se sitten reitittimen omista asetuksista.

34

Älä käytä liian ilmeisiä salasanonoja

On houkuttelevaa luoda helposti muistettavia salasanonoja, koska niitä käytetään useissa palveluissa. Aina on kuitenkin ihmisiä, jotka yrittävät päästä käsiksi muiden tileihin. Älä siis käytä salasanaa, joka on helppo arvata tai jonka kehittyneet ohjelmat voivat helposti avata. Vältä salasanonoja, joissa on loogisia numerosarjoja tai tavallisia sanoja. Voit lukea tästä aiheesta lisää verkkosivustoltamme kotimikro.fi/2513



Ilmeisimmät salasanat on turhan helppo arvata. Vältä numerosarjoja ja sanoja, jotka löytyvät helposti tavallisista sanakirjoista.

38

Älä käytä samoja salasanonoja

Älä koskaan käytä samaa salasanaa eri palveluissa, vaikka se helpottaisikin muistettavien salasanonojen määrän pienentämisessä. Pahimmassa tapauksessa rikolliset pääsevät käsiksi kaikkiin palveluihisi, jos he saavat selville yhden palvelun salasanan.

35



Looking for you...

Verkkokamera yhdessä Windows Hellon kanssa sallii turvallisen kirjautumisen kasvojen tunnistuksella.

Käytä sormenjäljen tai kasvojen tunnistusta

Voit vähentää muistettavien hankalien salasanonojen määrää käyttämällä niiden sijaan biometrisiä tunnistuksia, jos mahdollista. Windowsissa ja puhelimissa voit valita kasvojen tunnistuksen tai sormenjälkitunnistuksen vaihtoehtona perinteiselle salasanalle – ja se on itse asiassa turvallisempi vaihtoehto.

36

Käytä mahdollisimman pitkiä salasanonoja

Mitä pidempi salasana on, sitä kauemmin sen arvaaminen tai murtaminen tietokoneella kestää. Siksi useimmat tietoturva-asiantuntijat suosittelevat nykyään vähintään 12 merkin pituisia salasanonoja – mieluiten jopa pidempiä.

37

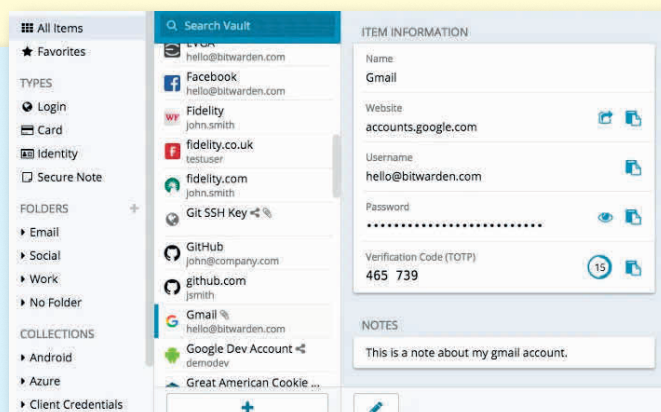
Keksi säkeitä

Voit helpottaa turvallisen ja pitkän salasanan muistamista yhdistämällä sen johonkin sinulle merkitykselliseen asiaan. Se voi olla esimerkiksi runo tai laulu, johon on sekoitettu merkkejä, numeroita ja isoja kirjaimia, kuten vaikkapa 1Ruusu!SenSulle\$uon.

39

Apuohjelma salasanonojen muistamiseen

Mikäli jo nyt on vaikeaa muistaa päivittäisiä salasanonoja, tilanne vain pahenee, kun salasanat pitenevät ja monimutkaistuvat. Tätä helpottaa niin sanottu salasanonojen hallintaohjelma. Se on kätevä ohjelma, jonka voi avata pääsalasanalla, ja ohjelma huolehtii sen jälkeen kaikkien vaikeiden yksittäisten salasanonojen muistamisesta. Voit käyttää esimerkiksi Bitwarden Free -ohjelmaa, jonka löydät turvallisuuksipaketistamme osoitteesta kotimikro.fi/2513.



Bitwarden Free on erinomainen salasanonojen hallinnointiohjelma, joka pitää tallessa kaikki turvalliset salasanasi.

40

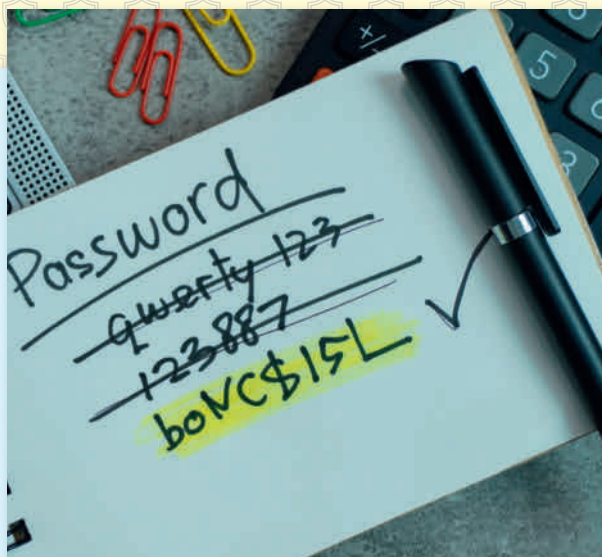
Onko salasanojasi vuotanut?

Toisinaan tapahtuu suuria tietovuotoja, joissa hakkerit kaappavat palveluihin rekisteröityneiden käyttäjien tietoja. Usein rikolliset pääsevät myös käsiksi ihmisten sähköpostiosoitteisiin ja salasanoihin, mikä on tietysti riskialtista, jos käytät samaa käyttäjätunnusta muissa palveluissa. Voit itse tarkistaa Chromen asetuksista, onko tietojasi vuotanut. Valitse **Yksityisyys ja turvallisuus** ja **Siirry turvatarkistukseen**.

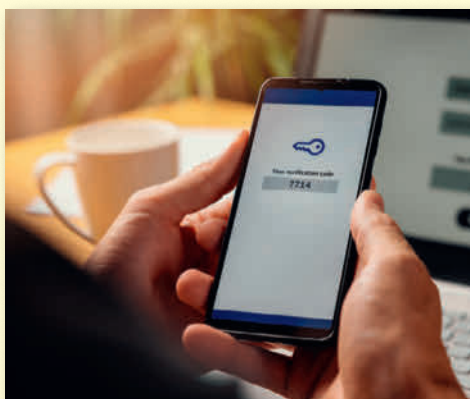
41

Käytä erikoismerkkejä

Hyvässä ja vahvassa salasanassa on vähintään neljä turvallisuustekijää. Salasanan tulee sisältää sekä isoja että pieniä kirjaimia, mieluiten satunnaisesti sijoitettuna. Lisäksi tulee käyttää erikoismerkkejä, kuten @, !, % ja vastaavia, sekä satunnaisia numeroita. Lue lisää osoitteesta kotimikro.fi/2513.



Älä käytä helposti arvattavia salasanvoja vaan satunnaisia kirjaimia ja erikoismerkkejä.



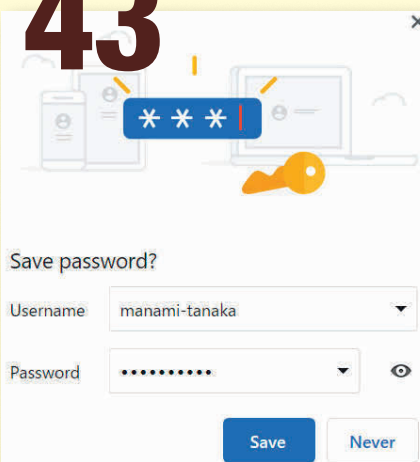
Kaksivaiheisessa tunnistautumisessa voidaan käyttää kertakäyttöistä koodia.

42

Käytä kaksivaiheista tunnistautumista

Kaksivaiheinen tunnistautuminen on turvallisuusmenetelmä, jossa tiiliin pääsy vaatii käyttäjältä kaksi eri tunnistautumistekijää. Tunnistautumiseen voidaan käyttää salasan lisäksi esimerkiksi puhelimeen tai vahvistussovellukseen lähetettävää koodia. Sormenjälkitunnistus tai puhelinnumeron käyttäminen estää hakkereiden pääsyn tilille.

43



Suosikkiselaimesi tarjoaa verkkosivustojen salasanoiden tallentamista, mutta se ei ole riskitöntä.

Selaimen ei saa antaa tallentaa salasanojasi

On houkuttelevaa hyväksyä, kun selaimet kuten Edge ja Chrome ehdottavat verkkosivuston salasan tallentamista, mutta se ei ole yhtä turvallista kuin oikean salasanoiden hallintaohjelman käyttö. Selaimen tallentamat salasanat näkyvät niille, joille lainaat tietokoneasi, eivätkä ne ole erityisen hyvin suojattuja hakkereilta.

44

Lemmikin nimeä ei kannata käyttää

Saatat ajatella, että vieraat ihmiset eivät voi arvata salasanasi, jos olet käyttänyt lemmikkisi tai lapsenlapsesi nimeä. Asiantuntijat eivät kuitenkaan suosittele tätä, koska nimet ja oikeat sanat voidaan helposti arvata käyttämällä sanakirjoja tai tähän erityisesti tarkoitettuja ohjelmia.



Lemmikin nimeä ei missään tapauksessa kannata käyttää salasanana, sillä se on aivan liian helppo arvata.



45

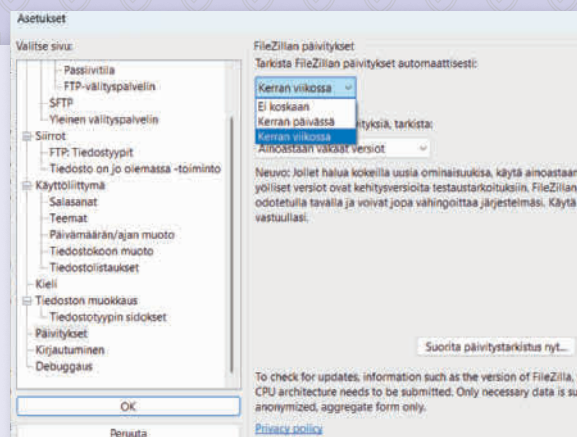
Vältä väärä lataussivustoja

Googlen ja muiden hakupalvelujen käyttäminen ohjelmien etsimiseen ja lataamiseen verkosta ei ole riskitöntä. Saatat päätyä väärennetyille lataussivuille, jossa luulet lataavasi oikean ohjelman, mutta saatkin viruksen tietokoneellesi. Siksi ohjelmat kannattaa ladata vain suoraan valmistajalta tai vaikkapa sivustoltamme kotimikro.fi, jossa skannaamme kaiken virusten varalta.

46

Anna ohjelmien päivittää itsensä

Ohjelmat, joita ei ole päivitetty aikoihin, ovat usein vaaravyöhykkeessä, koska hakkerit ovat jo ehtineet löytää niistä turvallisuusaukkoja. Voit välttää tämän pitämällä ohjelmiasi ajan tasalla. Useimmat ohjelmat voi myös määrittää etsimään ja asentamaan uusia päivityksiä automaattisesti.



Useimpien ohjelmien asetuksista voi ottaa käyttöön ohjelman automaattiset päivitykset. Voit myös määrittää päivitysten tarkistamisen aikavälin.



Tässä asennetaan doubleTwist-ohjelmaa, kun Delta Toolbar yllättäen tunkeutuu tarjolle.

47

Varo lisäosia asennuksissa

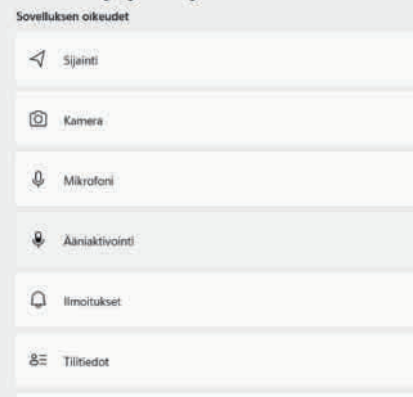
Ole varovainen, kun asennat ohjelmia tietokoneellesi. Etenkin ilmaiseksi saatavilla olevat ohjelmat lisäävät usein lisäosia asennuksen yhteydessä, koska se tuo valmistajalle pientä lisätuloa. Lue siis huolellisesti, mitä hyväksyt asennuksen aikana, ja hylkää heti kaikki lisäosat, joita et tunne.

48

Tarkista, mitä ohjelmat saavat tehdä

Haluatko, että pienen valmistajan ohjelma voi nähdä sijaintisi tai käynnistää verkkokamerasi? Ellet halua, voit tarkistaa ohjelmien käyttöoikeudet. Napsauta Windowsin aloituspainiketta hiiren oikealla ja valitse **Asetukset**. Napsauta kohtaa **Tietosuoja ja suojaus** ja valitse oikeus, esimerkiksi **Sijainti**. Katso, millä ohjelmilla on sijaintitietojen käyttöoikeus.

Tietosuoja ja suojaus



Asetusten kohdasta **Tietosuoja ja suojaus** voit katsoa, mitä käyttöoikeuksia asennetuilla ohjelmilla on.

49

Poista kaikki tarpeettomat ohjelmat

Mikäli olet käyttänyt tietokonettasi jo jonkin aikaa, olet todennäköisesti asentanut siihen monia ohjelmia, joita et enää käytä. Nämä ohjelmat voivat aiheuttaa turvallisuusriskin, joten kannattaa tarkistaa asia **Asetuksista** ja poistaa tarpeettomat ohjelmat. Lue tästä lisää verkkosivustoltamme osoitteesta kotimikro.fi/2513.

50

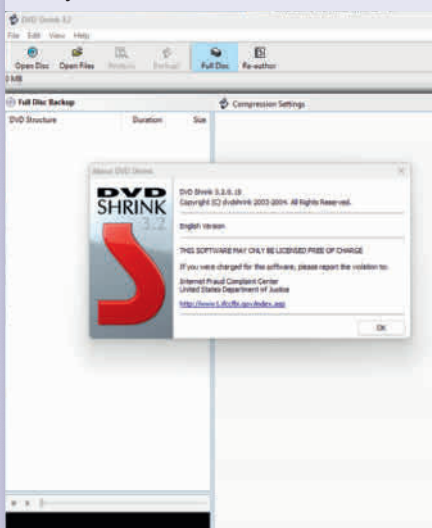
Onko tietokoneellasi haittaohjelmia?

Jos tietokone toimii tavallista hitaammin, siinä voi olla piilossa toimivia haittaohjelmia. Pelätyt haittaohjelmat vievät esimerkiksi paljon tilaa kiintolevyltä, kun ohjelmat salaavat tiedostosi lunnaiden vaatimiseksi. Voit tarkistaa asian tehtävienhallinnasta näppäinyhdistelmällä **Ctrl + Vaihto + Esc**. Tarkista kohta **Levy**.

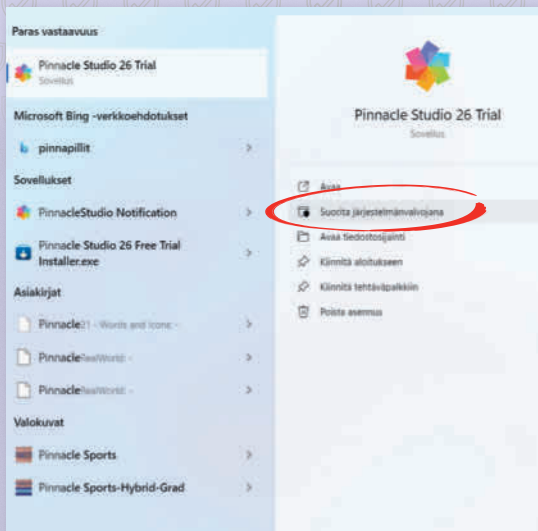
51

Saako ohjelmaan edelleen päivityksiä?

Valmistajat lopettavat toisinaan hyvien ohjelmien jakelun, jolloin myös päivitykset loppuvat. Tällöin et myöskään saa ohjelmiin tietoturva-aukkojen korjauksia, ja lopetettun ohjelman käyttö muuttuu riskialttiiksi. Siksi kannattaa tarkistaa myös se, milloin ohjelmat on päivitetty viimeksi.



DVD Shrink on hyvä ohjelma dvd-elokuvien tallentamiseen kiintolevyille, mutta se on päivitetty viimeksi vuonna 2004, joten sen käyttö on epävarmaa.



Aloitavalikon hakutuloksista ohjelmat voi suorittaa järjestelmänvalvojana.

52

Älä anna ohjelmille kaikkia oikeuksia

Hakiessasi ohjelmia aloitusvalikosta tai kun napsautat pikakuvaketta hiiren kakkospainikkeella, voit suorittaa ohjelmat järjestelmänvalvojana. Tätä ei kannata tehdä, ellei ohjelman toiminta edellytä tätä. Järjestelmänvalvojan oikeudet antavat ohjelmille paljon enemmän valtuuksia tietokoneellasi.

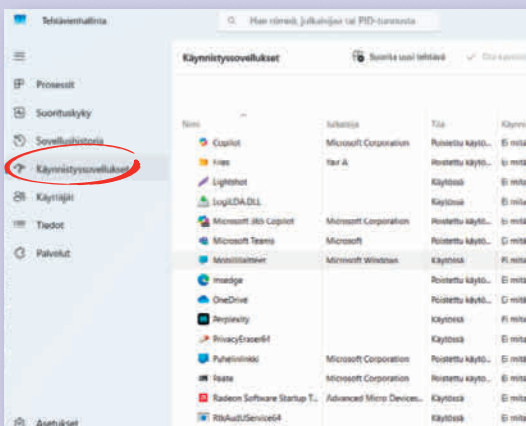
53

Tarkista tiedostot vielä kerran

Et voi aina luottaa täysin virus-torjuntaohjelmaasi, kun se hyväksyy ohjelman tai tiedoston. Jos haluat olla täysin varma, kannattaa käyttää toista tarkistusta. Suosittelemme [virustotal.com](https://www.virustotal.com)-sivustoa, jonne voit ladata tiedostoja ja nähdä vastauksena, miten kaikki markkinoiden johtavat turvallisuusohjelmat arvioivat ne.



VirusTotalissa tarvitsee vain valita **Choose file** ja hakea tiedosto kiintolevyiltä, niin saat heti ilmoituksen siitä, onko tiedosto vaarallinen.



Tehtävienhallinnan kohdasta **Käynnistyssovellukset** näet itse käynnistyvät ohjelmat.

54

Rajoita itse käynnistyviä ohjelmia

Pienet ohjelmat, jotka käynnistyvät automaattisesti Windowsin mukana, eivät ole vain rasite tietokoneen resursseille. Käynnistysohjelmien joukossa voi myös piillä haitallisia ohjelmia. Siksi kannattaa tarkistaa **Ctrl + Vaihto + Esc** -näppäinyhdistelmällä tehtävienhallinnasta **Käynnistyssovellukset**.

55

Rajoita ohjelmien pääsyä tietokoneen tiedostoihin

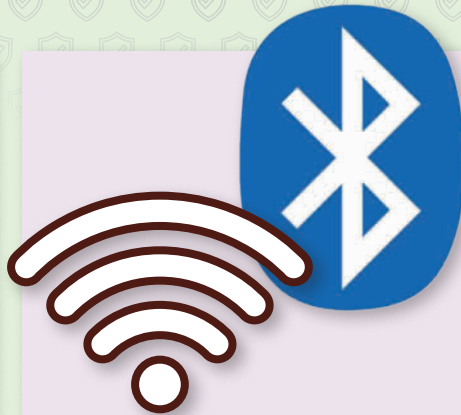
Lunnasohjelma on virustyyppi, joka salaa tiedostosi ja vaatii maksua niiden avaamisesta. Ohjelma ei kuitenkaan voi salata tiedostoja, jos se ei pääse niihin käsiksi. Kannattaa siis lukita pääsy kansioihin asetuksista käyttämällä **Kansioiden suojaus**-toimintoa.



56

Käytä virustorjuntaa

Mikäli käytät iPhonea, olet jo hyvin suojattu, mutta jos sinulla on Android-puhelin, on erittäin suositeltavaa suojata se virustorjuntaohjelmalla – aivan kuten tietokoneesikin. Sophos Intercept X for Mobile on paras ilmainen virustorjuntasovellus Androidille. Näytämme verkkosivuillamme, miten sitä käytetään. Artikkelin löytyy täältä: kotimikro.fi/2513.



Ei ole mitään syytä pitää Wi-Fi- tai bluetooth-yhteyksiä päällä silloin, kun niitä ei käytetä mihinkään.

57

Sulje bluetooth ja Wi-Fi

Wi-Fi ja bluetooth ovat käteviä langattomia yhteyksiä, mutta ne voivat myös mahdollistaa hakkerien pääsyn puhelimeesi. Pidä Wi-Fi-yhteys päällä vain luotettavissa langattomissa verkoissa. Bluetoothin pitäisi olla päällä vain langattomia kuulokkeita tai kaiuttimia varten. Nämä yhteydet voi helposti poistaa väliaikaisesti käytöstä puhelimen asetuksista.

58

Pidä puhelimesi päivitettyinä

Puhelimesi ohjelmistossa voi toisinaan ilmetä tietoturva-aukkoja, joita hakkerit voivat hyödyntää. Siksi kannattaa varmistaa, että puhelimesi käyttöjärjestelmä on päivitetty ajan tasalle. Voit tarkistaa milloin tahansa, onko päivityksiä saatavilla. Siirry vain iPhone- tai Android-puhelimesi asetuksissa kohtaan, joka koskee ohjelmistopäivityksiä tai puhelimen tietoja.

< **Ohjelmistopäivitys****Ohjelmistosi on ajan tasalla.****Päivitä tiedot**

- One UI -versio: 7.0
- Android-versio: 15
- Nykyinen versio: S921BXXU5BYD9 / S921BOXM5BYD9 / S921BXXU5BYD9
- Tietoturvakorjauksen taso: 1. huhtikuuta 2025

Puhelimen asetuksista voi katsoa käyttöjärjestelmän version ja onko se ajan tasalla.

59

Käytä hyvää hotspot-salasanaa

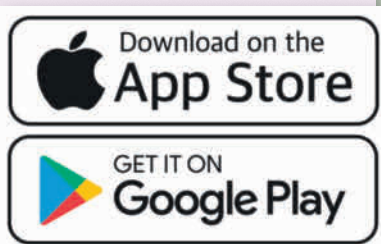
Voit jakaa puhelimesi tiedot ja kirjautua verkkoon toisella laitteella jakamalla puhelimen verkkoyhteyden. Tätä kutsutaan hotspotiksi. Jos jaat yhteyden, on tärkeää, että suojaat hotspotin hyvällä salasanalla. Voit vaihtaa salasanan asetuksissa, joissa hotspot otetaan käyttöön. Muista käyttää salasanaa pieniä ja isoja kirjaimia sekä erikoismerkkejä ja numeroita.

60

Lataa vain virallisista kaupoista

Hakkerit pääsevät puhelimeesi helpoimmin sovellusten kautta. Usein tyrkytetään myös vaarallisia, haittaohjelmia sisältäviä sovelluksia, jotka voivat esimerkiksi tyhjentää verkkopankkitiliä tai valvoa sinua. Lataamalla sovellukset virallisista sovelluskaupoista vähennät riskiä.

App Store on iPhone-sovelluskauppa. Androidille käytetään Google Playä.



61

Hakkerit pääsevät helpommin asentamaan haittaohjelmia päivittämättömiin sovelluksiin.

**Päivitä sovelluksesi**

Aivan kuten puhelimen käyttöjärjestelmä on pidettävä ajan tasalla, on myös muistettava päivittää puhelimen sovellukset säännöllisesti. Silloin voit käyttää sovelluksiasi huoletta. Lue täältä, miten sovellukset voi pitää päivitettyinä: kotimikro.fi/paivita-sovellukset.

62

Tee varmuuskopio kuvistasi

Nykyään useimmat meistä kuvaavat puhelimella, joten kuvat myös tallennetaan puhelimeen. Jos puhelimelle sattuu jotain, voit kuitenkin menettää täysosumasi, ellei ole tallentanut niitä myös muualle. Siksi ne kannattaa varmuuskopioida säännöllisesti. Lue verkkosivuiltamme, miten voit tehdä sen parhaiten: kotimikro.fi/2513.

[Postin tietoja]: Lahetus on saspunut jakeluasemalle, mutta sita ei voida toimittaa, koska pakkauspaallyksen tiedot ovat epäselvät.

Klikkaa nyt linkkia:

<http://is.gd/ByequFC?psg=olbgei>
Lahetämme uudelleen heti, kun tiedot on päivitetty.
Kitos

Tyypillisessä huijausviestissä on linkki, joka kehoitetaan avaamaan.

63

Varo tekstiviestihuijauksia

Voit saada huijausviestejä myös tekstiviesteinä. Se voi olla esimerkiksi tekstiviesti, jossa ilmoitetaan paketin toimituksen epäonnistumisesta, kuten viereisessä kuvassa. Ne voivat olla myös väärennetyjä viestejä viranomaisilta tai viestejä, joissa ilmoitetaan palkinnon voittamisesta.

64



Älä käytä julkisia usb-latauspisteitä

Voi olla houkuttelevaa kytkeä puhelimesi julkiseen usb-latauspisteeseen, mutta kannattaa olla varovainen. Hakkerit käyttävät nimittäin usb-liitäntöjä asentaakseen haittaohjelmia puhelimeesi. Menetelmän nimi on "juice jacking", ja tarkoituksena on varastaa tietojasi.

66

Lukitse puhelin biometrisesti

Biometrinen tunnistaminen, kuten sormenjälkitai kasvojentunnistus, sallii puhelimen nopean lukituksen ilman salasanaa. Se on myös taatusti turvallinen tapa suojata tietoja, sillä puhelimen lukituksen avaaminen edellyttää ihmisen yksilöllisiä fyysisiä piirteitä.



Puhelimen turva-asetuksista voi ottaa käyttöön biometriset tunnistustoiminnot.

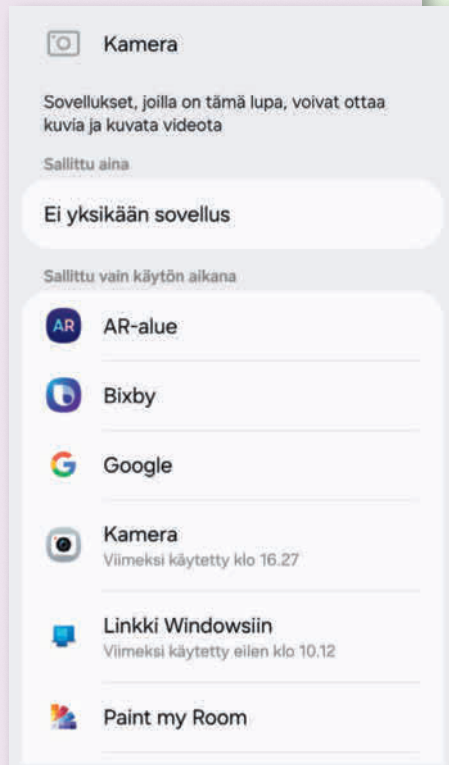
65

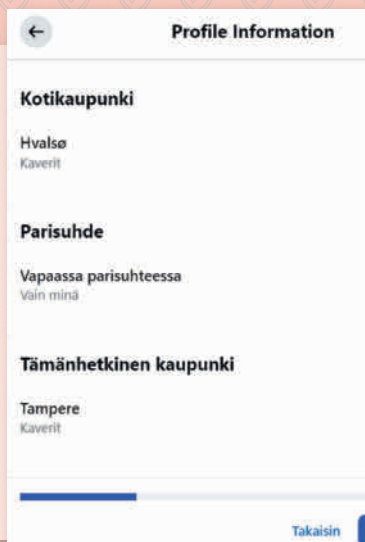
Tarkista sovellusten käyttöoikeudet

Kannattaa tarkistaa, mitkä sovellukset pääsevät käyttämään puhelimesi työkaluja. Samsung-puhelimesta löydät käyttöoikeuksien luettelon Sovellukset-kohdasta, jossa napautat kolmea pistettä ja valitset kohdan Käyttöoikeuksien hallinta. Menetelmä voi vaihdella hieman, jos sinulla on eri puhelin, mutta yleensä on mentävä sovellusten asetuksiin, josta löydät luettelon käyttöoikeuksista. Voit helposti poistaa ei-toivotut käyttöoikeudet.

Tarkista etenkin mikrofonin, GPS:n, kameran, puheluiden ja tekstiviestien käyttöoikeudet.

Millään sovelluksella ei tarvitse olla jatkuvasti esimerkiksi kameran käyttöoikeutta. Poista siis kaikki turhat käyttöoikeudet.





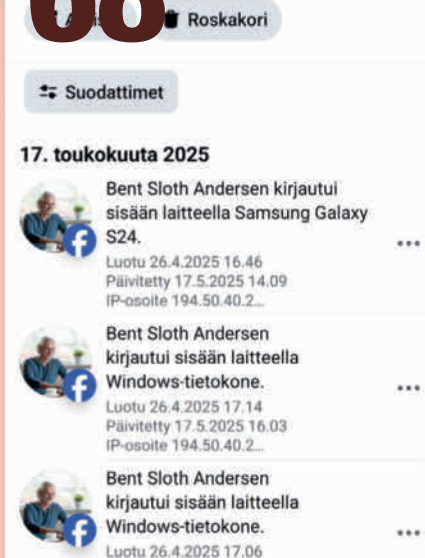
67

Tee profiillistasi yksityinen

Voit määrittää profiilisi yksityiseksi ja vähentää identiteettivarkauden riskiä napsauttamalla profiilikuvaasi Facebookin oikeassa yläkulmassa ja valitsemalla kohdan **Asetukset ja yksityisyys**. Valitse **Henkilökohtaiset tiedot** ja käy läpi sivuston tiedot.

Varmista helposti, että henkilökohtaiset tietosi näkyvät vain sinulle itsellesi ja mahdollisesti kavereillesi Facebookissa.

68



Jos näet kohteen, jota et tunnista, napsauta kohteen vieressä olevaa kolmea pistettä ja valitse **Kirjaudu ulos**.

Tarkista, mihin olet kirjautunut

Jos epäilet, että joku muu on päässyt käsiksi profiiliisi, voit tarkistaa asian. Napsauta profiilikuvaasi oikeassa yläkulmassa ja valitse **Asetukset ja yksityisyys**, sitten **Toimintaloki ja Turvallisuus ja sisäänkirjautuminen**. Täältä näet, mihin olet kirjautunut.

69

Varo väärrää sisältöä

Facebook on luopunut faktantarkistuksesta, joten siellä on nykyään runsaasti väärennettyä sisältöä. Valitettavasti väärennetty sisältö ei ole vain valheellisia tietoja, vaan napsauttaminen voi olla myös vaarallista. Esimerkiksi linkki väärennettyyn artikkeliin voi johtaa huijaussivustolle, jossa sinulta huijataan arkaluontoisia tietoja tai voit altistaa tietokoneesi viruksille. Ole varovainen sisällön suhteen.

70

Muista kirjautua ulos

Voi kuulostaa itsestään selvältä, mutta muista kirjautua ulos Facebookista, kun et käytä sitä. Tämä on tärkeää, jos olet kirjautunut sisään julkisella tietokoneella tai tietokoneella, jolla on muita käyttäjiä. Muuten saatat antaa muille pääsyn profiiliisi.

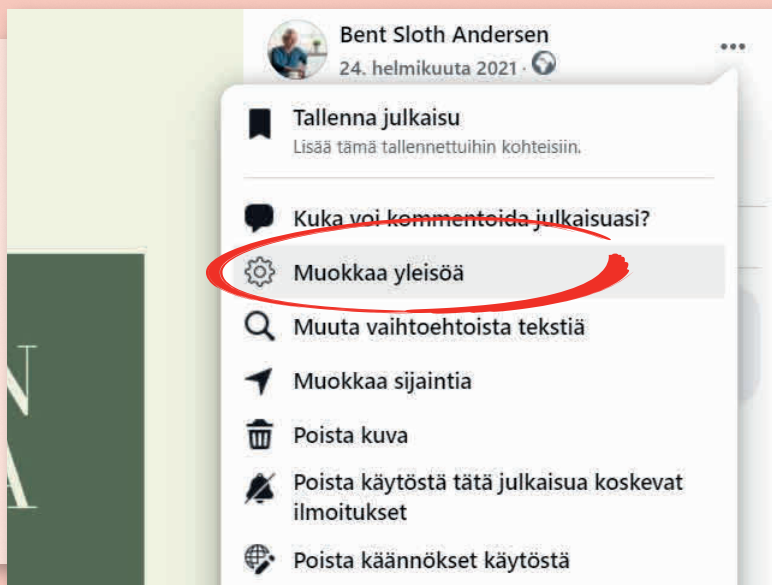
Kun olet kirjautunut ulos, tarkista, ettei selain ole tallentanut sähköpostiosoitettasi ja salasanaasi. Jos niin on, poista tiedot.

71

Aseta profiilikuva yksityiseksi

Huijarit voivat varastaa Facebookista satunnaisen uhrien identiteettejä ja käyttää niitä muiden huijaamiseen. Monissa Facebook-profiileissa profiilikuviin on vapaa pääsy, joten huijarit voivat helposti tallentaa ne tietokoneelleen ja käyttää niitä väärin. Voit estää tämän asettamalla profiilikuvaa yksityiseksi, jolloin vain sinä ja ystäväsi voivat avata kuvan. Muut näkevät vain pikkukuvan, jota hakkerit eivät voi juurikaan hyödyntää.

Avaa profiilikuvasi ja napsauta kolmea pistettä. Napsauta kohtaa **Muokkaa yleisöä** ja valitse yleiseksi Kaverit.

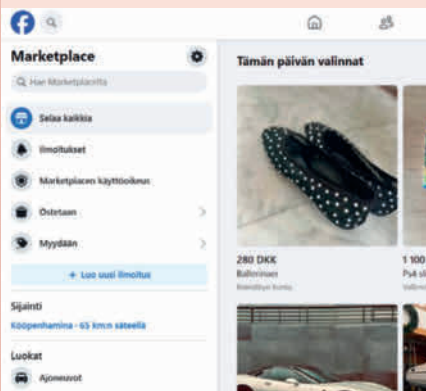


72

Ole varovainen markkinapaikalla

Facebook Marketplace on Facebookin markkinapaikka, jossa voi ostaa ja myydä käytettyjä tavaroita. Tiedossa on kuitenkin useita esimerkkejä siitä, kuinka sekä ostajia että myyjiä on tullut huijatuiksi.

Myyjä voi tarjota merkkituotteita, kuten Apple-tuotteita tai merkkiavusteita edullisesti, mutta todellisuudessa hän kauppaakin kopioita tai ei mitään. Toisaalta ostajat voivat sanoa maksavansa hämäreiden palvelujen kautta, jolloin et saa rahojasi. Liikkeellä on myös varastettuja tavaroita.



Facebook Marketplacella kannattaa noudattaa varovaisuutta.

73



Varo linkkejä Messengerissä

Facebookin Messenger-viestipalveluun yllättäen ilmaantuvien viesteihin, joissa kehoitetaan napsautamaan linkkiä, kannattaa suhtautua varauksella – etenkin jos viesti on tuntemattomalta lähettäjältä. Kannattaa varoa myös, vaikka lähettäjänä olisi joku Facebook-kaveristasi, sillä todellinen lähettäjä voi olla huijari, joka on hakeroitunut kaverisi profiiliin.

Kaveriin voi olla yhteydessä jollain muulla tavalla ja kysyä, onko hän lähettänyt kyseisen viestin.

74

Mieti, mitä jaat

Facebook on suunniteltu kokemusten ja vaikutelmien jakamiseen ystävien ja perheen kanssa, mutta mieti kuitenkin hetki sitä, mitä todella jaat muille.

Jos profiiliasi ei ole määritetty yksityiseksi, kuka tahansa voi periaatteessa nähdä jakamasi tiedot ja käyttää niitä sinua vastaan. Tämä ei koske vain tilapäistietojasi, vaan myös kaikkia profiilissasi olevia tietoja. Harkitse näiden yksityisten tietojen piilottamista. Lue tästä lisää verkkosivustoltamme: kotimikro.fi/2513.

75

Ota hälytykset käyttöön

Facebookin asetuksissa voi ottaa käyttöön ominaisuuden, joka ilmoittaa sinulle, jos joku käyttää tiliäsi epätavanomaisessa sijainnissa. Silloin voit reagoida nopeasti ja kirjautua ulos palvelusta. Tämän jälkeen sinun kannattaa vaihtaa salasanasasi välittömästi.

Hallinnoi hälytyksiä

Kerro, miten haluat saada ilmoituksen, jos joku kirjautuu sisään tilillesi tuntemattomassa sijainnissa. Ilmoitamme, mitä laitetta käytettiin ja missä sitä käytettiin.

Facebook

Lähetämme sinulle Facebook-ilmoituksen.



Sähköposti

Lähetämme ilmoituksen seuraaviin osoitteisiin: renix@adslhome.dk



Toiminto löytyy yksityisyysasetuksista kohdasta **Asetukset ja yksityisyys**. Valitse kohta **Sisäänkirjautumisilmoitukset**.

76

Hyväksy kavereiksi vain ihmisiä, jotka tunnet

Jos saat kaveripyynnön henkilöltä, jota et tunne tai ole tavannut, sinun ei kannata hyväksyä pyyntöä, etenkin jos sinulla ei ole yhteisiä ystäviä kyseisen henkilön kanssa. Tällaisissa tapauksissa kyseessä voi olla huijari. Lue täältä, miten tunnistat väärennetyn profiilin: kotimikro.fi/2513.

Salasana ja turvallisuus

Sisäänkirjautuminen ja palautus

Hallinnoi salasanojasi, sisäänkirjautumisasetuksiasi ja palautustapojasi.

Vaihda salasana

Kaksivaiheinen todennus

Tallennetut kirjautumistiedot

Tilisi suojauksen asetuksista voit vaihtaa tarvittaessa salasanasasi ja ottaa käyttöön kaksivaiheisen todennuksen.

77

Käytä kaksivaiheista todennusta

Facebookin kaksivaiheisessa todennuksessa sinun on annettava salasanasasi lisäksi puhelimeesi lähetettävä koodi, kun kirjautut sisään. Tämä vaikeuttaa hakkereiden pääsyä tilillesi. Voit ottaa kaksivaiheisen todennuksen käyttöön asetuksista.



78

Poista vakoilevat evästeet

Evästeet voivat tallentaa tietojasi usein vierailemillesi verkkosivustoille, jolloin sivut latautuvat nopeammin, mutta evästeitä käytetään myös seuraamaan sinua eri verkkosivustojen välillä. Erityisesti kolmannen osapuolen evästeisiin on kiinnitettävä huomiota, sillä näiden evästeiden takana on joku muu kuin verkkosivusto, jolla olet käynyt.

Kolmansien osapuolten evästeet ovat yleensä peräisin mainostoimistoilta, jotka seuraavat verkkokäyttäytymistäsi voidakseen näyttää sinulle mainoksia, jotka on kohdistettu sinulle aiemman verkkotoimintasi perusteella. Tämä tarkoittaa, että verkkosivustoilla näkyvät mainokset liittyvät aiempaan verkkokäyttäytymiseesi, mikä voi olla yksityisyyttäsi loukkaavaa.

Valitse tietotyyppiä, joiden avulla sivustot voivat seurata sinua selaamisen aikana.

☐ Salli kolmannen osapuolen evästeet

☐ Estä kolmannen osapuolen evästeet incognito-tilassa

☒ Estä kolmannen osapuolen evästeet

☐ Sivustot voivat käyttää evästeitä selaukskokemuksesi parantamiseen, esimerkiksi kirjautuneena tai muistaa ostoskorisi sisällön

☐ Sivustot eivät näe selaustoimintaasi eri sivustoilla evästeiden kautta esim. mainoksia. Joidenkin sivustojen ominaisuudet eivät välttämättä toimi

Google Chromessa ja useimmissa muissa selaimissa voi estää kolmansien osapuolten seurantaevästeet. Chromessa tämä tehdään **Yksityisyys ja turvallisuus** -asetuksissa.

Luvat



Sijainti

Sivustot voivat pyytää sijaintiasi



Kamera

Sivustot saavat pyytää kameran käyttö lupaa



Mikrofoni

Sivustot saavat pyytää mikrofonin käyttö lupaa

Chromessa voi tarkistaa sivustoille annetut luvat avaamalla yksityisyyden ja turvallisuuden asetukset. Valitse **Sivustoasetukset**. Voit käydä luvat läpi ja katsoa, mitä lupia sivustoille on annettu.

79

Tarkista luvat

Monet verkkosivustot pyytävät tietokoneesi kameran, mikrofonin ja sijainnin käyttöoikeuksia, kun taas toiset verkkosivustot haluavat luvan saada lähettää sinulle ilmoituksia selaimeen. Näitä valtuutuksia kannattaa säännöllisesti tarkistaa ja muokata, jotta et anna verkkosivustoille tarpeettomia käyttöoikeuksia.

80

Sulje selain säännöllisesti

Selaimen pitäminen päällä päiviä kausia voi rasittaa tietokonetta ja aiheuttaa turvallisuusriskejä. Kun suljet selaimen, tietyt väliaikaiset tiedostot ja istuntoevästeet poistetaan. Hakkerit voivat muuten käyttää niitä seuraamiseesi. Tee verkkoselaimen säännöllisestä sulkeamisesta päivittäinen tapa.

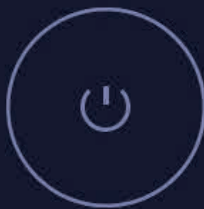
81

Poista kirjautumistiedot

Saattaa tuntua kätevältä antaa selaimen muistaa kirjautumistietosi, mutta se on turvallisuusriski. Jos tietokoneesi tai Google-tilisi – jos käytät Chrome-selainta – vaarantuu, ulkopuoliset voivat helposti päästä käsiksi kirjautumistietoihisi. Verkkosivuillamme näytämme, kuinka voit poistaa tallennetut kirjautumistiedot sekä Chrome- että Edge-selaimesta: kotimikro.fi/2513.

CyberGhost VPN

Start a Connection



Connect to:



United States

82

Käytä VPN-yhteyttä

VPN salaa internetyhteytesi ja piilottaa IP-osoitteesi. Tämä vaikeuttaa hakkereiden toimintaa ja verkkosivustojen seurantaa. Useimmat VPN-yhteydet ovat maksullisia, mutta CyberGhost VPN Free Proxy -laajenuksen voit asentaa ilmaiseksi. Lue täältä, kuinka sitä käytetään: kotimikro.fi/2513.

Ilmaisella CyberGhost VPN Free Proxy -selainlaajennuksella saat Chromeen ja Firefoxin erinomaisen VPN-yhteyden, joka piilottaa IP-osoitteesi.

83

Älä napsauta mainoksia

Mainokset verkkosivustoilla voivat olla muitakin kuin ärsyttäviä. Jotkin mainokset on suunniteltu johdattamaan sinut haitallisille verkkosivustoille tai asentamaan tietokoneellesi haittaohjelmia. Nämä mainokset yrittävät houkutella napsauttamaan niitä väärillä varoituksilla tai tarjouksilla tuotteista tai tietokoneohjelmista.

Jopa näennäisesti oikeat mainokset voivat olla huijausta, joten älä napsauta mainoksia, joiden alku-kerästä et ole varma.

84

Varo mitä lataat

Monet ongelmat alkavat varomat-
tomista latauksista. Vältä siis la-
taamista tiedostoja tuntematto-
mista tai epäluotettavista lähteistä.
Mikäli olet epävarma, tarkista aina
lataamasi tiedostot virustorjunta-
ohjelmalla.

Ole erityisen varovainen verk-
kosivustoilla, jotka houkuttelevat
ilmaisilla versioilla kalliista tietoko-
neohjelmista. Muista, että jos jokin
vaikuttaa liian hyvältä ollakseen
totta, se todennäköisesti onkin.

Tietoja Chromesta



Google Chrome



Chrome on ajan tasalla

Versio 136.0.7103.114 (Virallinen koontiversio)

Ohjeita Chromen käyttöön

Ilmoita ongelmasta

Tietosuojaikäytäntö

Chromessa voi katsoa, onko selain ajan
tasalla. Tieto löytyy asetusten kohdasta
Tietoja Chromesta.

86

Pidä selain päivitettyinä

Vanhoissa selainversioissa – ku-
ten monissa muissakin ohjelmissa
– on usein tietoturva-aukkoja, joita
hakkerit voivat hyödyntää.

Tietoturva-aukot korjataan, kun
selain päivitetään. Useimmat se-
laimet, kuten Google Chrome ja
Microsoft Edge, päivittyvät toki au-
tomaattisesti. Sinun on kuitenkin
käynnistettävä selain itse uudel-
leen sulkemalla se ja avaamalla se
uudelleen.

WPS PDF

Read and Comment PDF files

WPS PDF - Read, Edit, Fill,...

4,6 ★ (135) @

Easy-to-use PDF tools to view,
edit, convert, fill, e-sign PDF files...



Shazam: Find song names...

4,7 ★ (25,3 t.) @

Identify music, search lyrics &
more



Lue arvosteluja laajennuksista ennen kuin lataat
niitä esimerkiksi Chrome Webstoresta.

85

Tarkista laajennukset

Selainlaajennukset voivat ol-
la hyödyllisiä, mutta ne voi-
vat myös olla haitallisia. Tar-
kista siksi, mitä laajennuk-
sia olet asentanut, ja poista
tarpeettomat. Tutki myös
arvosteluja ja julkaisijan luo-
tettavuutta. Lue täältä, mi-
ten laajennukset poistetaan:
kotimikro.fi/2513.

87

Käytä turvallista selainta

Jotkut selaimet, kuten Firefox ja
Brave, keskittyvät yksityisyyteen
ja turvallisuuteen. Niissä voi hallita
paremmin siitä, mitä tietoja jae-
taan kolmansille osapuolille. Brave
estää seurantaevästeet ja mainok-
set automaattisesti, kun taas Fire-
foxissa on edistyneet yksityisyyden
hallinta-asetukset. Selaimet voi ladata
täältä: kotimikro.fi/2513.



Brave ja Firefox
ovat hyviä, jos haluat
suojata paremmin yksityi-
syyttäsi verkossa.

88

Varo väärä verkkotunnuksia

Tietojenkalastelu tapahtuu usein
tunnettuja sivustoja muistuttavilla
verkkotunnuksilla, kuten "face-
book.com" osoitteen "facebook.
com" sijaan. Tarkista aina verkko-
tunnus huolellisesti ennen kirjau-
tumista tai lataamista. Yksikin
vierailu väärällä sivustolla voi antaa
hakkerille pääsyn tietoihisi.



89

Tarkista Avainlippu-tunnus

Avainlippu-merkki osoittaa, että kyseisen verkkokaupan ylläpitäjä on suomalainen yritys, joka työllistää Suomessa. Avainlipun voivat saada verkkokaupalleen suomalaiset yritykset, jotka myyvät omia tuotteita ja brändejä tai jotka jälleenmyyvät muiden tuotteita verkkokaupoissaan. Suosi siis verkkokauppoja, joilla on tämä kotimaisuuden osoittava tunnus.



Avainlippu verkkokaupan sivustolla osoittaa, että kyseisen verkkokaupan ylläpitäjä on suomalainen.

90

Älä käytä julkisia tietokoneita

Julkiset tietokoneet, kuten kirjastojen ja hotellien tietokoneet, eivät ole turvallisia. Verkkokauppoissa annat usein arkaluonteisia tietoja, kuten maksutietoja ja osoitteita. Käytä aina omaa tietokonettasi verkkokaupoissa ja varmista, että se on päivitetty ja että siihen on asennettu virustorjuntaohjelma.

91

Lue ehdot huolellisesti

Monet hyväksyvät helposti kaupan ehdot lukematta niitä, mutta ne sisältävät tärkeitä tietoja, kuten palautusehdot, toimitusajat ja maksut. Etenkin ulkomailta ostettaessa ostohinnan lisäksi saattaa tulla muita kustannuksia tai kulutajansuoja voi olla heikompi. Käytä siis aikaa ehtojen lukemiseen, jotta tiedät, millaisin ehdoin olet suostunut kauppaan.

92

Tarkista myymälän osoite

Luotettava verkkokauppa ilmoittaa aina fyysisen osoitteensa. Jos osoite puuttuu tai näyttää salaperäiseltä, kannattaa olla varovainen. Tarkista Google Mapsin avulla, onko osoite olemassa ja vastaako se yrityksen profiilia. Monet huijarikaupat käyttävät keksittyjä osoitteita tai viittaavat palvelutoimistoihin, mikä voi olla vaaran merkki.

93

Maksa MobilePayllä

MobilePay on nopea ja turvallinen maksutapa, kun teet ostoksia verkossa. Käyttämällä Mobile Payta korttitietojasi ei anneta verkkokaupalle, ja koska valtuutat maksun puhelimellasi, voit hallita maksuja paremmin. Lisäksi maksutapahetuma tallentuu selkeästi sovellukseen ja pankkiin, joten sinulla on dokumentit ongelmien varalta. Käytä siis verkkokaupoissa maksamiseen MobilePayta aina, kun se on mahdollista.

94

Etsi yrityksen VAT-numero

Voit tarkistaa nopeasti ja varmasti, oletko tekemisissä oikean yrityksen kanssa: etsi vain yrityksen VAT-numero (ALV-tunnus), joka löytyy myymälän verkkosivustolta. VAT-numeron voi tarkistaa osoitteesta https://ec.europa.eu/taxation_customs/vies/#/vat-validation. Suomessa yrityksillä on Y-tunnus, joka vastaa VAT-numeroa. Jos sitä ei löydy, kyse on usein huijauksesta.

Tervetuloa ostoksille!

Verkkokauppa.com Oyj
Tyynenmerenkatu 11
00220 Helsinki
Y-tunnus 1456344-5

Verkkokaupan VAT-numero on yleensä sivuston alussa tai lopussa.



MobilePayllä maksettaessa kauppa ei saa maksukorttisi numeroa, joten voit tehdä kaupat rauhallisin mielin.

95

Osta vain sivustoilta, joiden osoitteessa on https

Osoitepalkissa näkyvä lyhenne "https" ja riippulukko tarkoittaa, että yhteys sinun ja verkkokaupan välillä on salattu. Tämä suojaa tietojasi siltä, etteivät kolmannet osapuolet pääse sieppaamaan niitä. Jos sivuston verkko-osoite alkaa vain lyhenteellä "http", kannattaa välttää henkilökohtaisten tietojen ja etenkin maksukorttitietojen syöttämistä. Nykyään useimmat selaimet merkitsevät näkyvästi sivustot, joilla ei käytetä suojattua yhteyttä.



https://www

97

Varo yksityisiä kauppiaita

Yksityishenkilöiden kanssa esimerkiksi Huuto.netissä kauppaa käydessä ei ole turvana samanlaisia kuluttajansuojaa kuin verkko-kaupasta ostaessasi. Älä koskaan siirrä rahaa etukäteen, ellet luota täysin myyjään. Tapaa vastapuoli henkilökohtaisesti ja maksa vasta, kun olet saanut tavarat. Jos tavara on tarkoitus lähettää, kannattaa käyttää turvallisia maksutapoja.

98

Tarkista pankkitilisi oston jälkeen

Verkkokaupoissa on hyvä tarkistaa pankkitapahtumat. Varmista, että hyväksymäsi summa vastaa veloitettua summaa. Luvattomat tai kaksinkertaiset veloitukset voivat olla merkki virheestä tai väärinkäytöstä. Mikäli huomaat jotain epäilyttävää, ota heti yhteyttä pankkiisi. Mitä nopeammin reagoit, sitä parempi sinulle itsellesi.

99

Tallenna tilausvahvistus

Säilytä aina tilausvahvistus, kun olet tehnyt ostoksia. Se lähetetään usein sähköpostina tai pdf-tiedostona ja on todiste siitä, mitä olet ostanut, milloin ja mihin hintaan. Se on hyödyllinen palautusten ja reklamaatioiden yhteydessä tai jos tuote ei saavu perille. Säilytä tilausvahvistus turvallisessa paikassa, jotta löydät sen tarvittaessa.

Order confirmation

Hi martinlorentsen77 user,

Thank you for shopping with us. Your order 3035585457205239 is confirmed. We'll let you know when your order ships.

[View your order](#)

Order details

Placed on May 23, 2024, 04:58

Shop1102066081 Store

Tilausvahvistuksella voit tarvittaessa helposti tarvittaessa osoittaa, mitä olet ostanut ja mihin hintaan.

96

Katso aina arvostelut

Trustpilotin käyttäjäarvostelut voivat antaa käsityksen siitä, miten yritys kohtelee asiakkaitaan. Katso sekä arvostelut että itse kommentit. Huomioi etenkin huonot arvostelut. Jos muut ovat kohdanneet ongelmia toimituksissa, asiakaspalvelussa tai palautusoikeudessa, kannattaa olla erityisen varovainen.

Etsi luotettava yritys

Aitoja arvosteluja oikeilta ihmisiltä.

Hae yritystä tai kategorias

Etsi kauppa Trustpilotista ja lue arvostelut tarkasti.

100

Tarkista lähetyspaikka

Aina ei ole selvää, mistä paikasta verkosta ostamasi tuote lähetetään. Monilla verkkokaupoilla on suomalainen nimi ja verkkotunnus, mutta tuotteet lähetetään Kiinasta tai muista EU:n ulkopuolisista maista. Toimitusajat voivat olla pitkiä, toimituskulut suuria ja lisäksi voi tulla tulli ja arvonlisävero. Tarkista toimitustiedot ennen tilaamista. Pienellä prantätyt ehdot voivat nostaa merkittävästi kustannuksia.



Lisäkuluja voi seurata, jos verkosta ostamasi tuote lähetetään kaukaa.