

[Meta](#) julkisti tällä viikolla [Instagramille](#) kolme uutta ominaisuutta, jotka lupaavat ”auttaa käyttäjiä muodostamaan yhteyden”. Kaksi ovat melko vaarattomia: kyky jakaa julkisia keloja ja uusi "Friends" -välilehti, jossa voit nähdä sisältöä, josta ystäväsi ovat pitäneet ja kommentoineet.

Kolmas on kuitenkin huolestuttavampi.

Instagramilla on nyt oma Instagram-ystäväkartta, jonka avulla voit jakaa sijaintisi vastuullisesti Instagram-kartan avulla valitsemiesi ystävien kanssa. Voit jakaa sijaintisi ystävien kanssa ja päinvastoin.

On todennäköistä, että tämä ominaisuus on otettu käyttöön kilpailemaan [SnapChatin](#) suosittu "Snap Map" -ominaisuuden kanssa, joka tarjoaa samanlaisen ystäväkarttatoiminnon, joka on ollut aktiivinen vuodesta 2017. Tällä hetkellä Instagram-sijainnin jakaminen on saatavilla vain Yhdysvalloissa, mutta se otetaan käyttöön maailmanlaajuisesti. Ominaisuuden tarkoitusta Instagram kuvailee keinoksi ”pysyä ajan tasalla ystävien kanssa”.

Mutta Metan aiemmat kiistat ja taloudelliset kannustimet herättävät kysymyksiä sijaintitietojen jakamisen turvallisuudesta ja havainnollistavat sijainnin seurannan käynnistämisen tietosuojariskejä.

Miten Instagram-sijainnin jakaminen toimii?

[Sijainnin seuranta\(uusi ikkuna\)](#) sosiaalisen median työkalujen kautta on melko yksinkertainen. Sosiaaliset kartoitustyökalut käyttävät älypuhelimesi Global Positioning System (GPS) -tekniikkaa löytääksenne sinut. Tämä geopaikannusjärjestelmä toimii satelliiteilla, jotka kiertävät maata, eikä se vaadi Internet-yhteyttä tai puhelimen vastaanottoa.

Päälle [iOS-versio\(uusi ikkuna\)](#) ja [Android-käyttöjärjestelmä\(uusi ikkuna\)](#), voit hallita, jos ja kun jaat GPS-sijaintisi. Voit sanella, mitkä sovellukset voivat käyttää sitä ja milloin ne voivat tehdä niin. Instagram käyttää GPS-sijaintia, Bluetoothia ja WiFi-yhteyksiä [määrittää sijaintisi\(uusi ikkuna\)](#) kun kytket sijaintipalvelut päälle. Se arvioi myös sijaintisi, kun:

- Syötä sijaintisi profiiliisi
- Merkitse sijaintisi viesteihin, reeleihin tai tarinoihin
- Ilmoittaudu sisään tapahtumassa Facebookissa
- Anna osoitteesi Marketplacessa

Uuden Friend Map -ominaisuuden lanseerauksen myötä Instagram luo nyt käyttäjille kartan, joka näyttää niiden ystävien nykyisen sijainnin, jotka ovat päättäneet jakaa sijaintinsa. Metan mukaan mikä tahansa sisältö, jolla on merkitty sijainti, voi näkyä kartalla, mukaan lukien:

- Reels, viestit ja tarinat ihmisiltä, joita seuraat, ovat käytettävissä 24 tuntia niiden julkaisemisen jälkeen
- Muistiinpanoja ihmisiltä, joita seuraat vastavuoroisesti, saatavilla 24 tuntia sen jälkeen, kun ne on lähetetty

Sijaintisi on oletusarvoisesti pois päältä, kun käytät ensimmäistä kertaa Instagram-karttaa, mutta on epäselvää, kytkeekö sovellus sijaintisi päälle, jos vieraillet toisen kerran. Sijaintipalvelut on otettava käyttöön laitteessasi, jotta ominaisuus voidaan kytkeä päälle, mikä saattaa olla, jos olet koskaan merkinnyt sijaintisi Instagram-tarinassa tai syötteesi julkaisussa. Jos päätät jakaa sijaintisi, voit nähdä sen käyttämällä postilaatikon yläosassa olevaa karttaa.

Onko sijainnin jakaminen Instagramissa turvallista?

Sijaintisi jakaminen rakkaasi kanssa sosiaalisessa mediassa saattaa tuntua turvalliselta: Voit löytää jonkun helposti, jos joku teistä on kadonnut, tai voit varmistaa, että lapsesi on turvallisessa paikassa. Noin vuodesta 2017 lähtien sijainnin jakaminen sosiaalisiin tarkoituksiin on ollut melko kaikkialla. Sitä markkinoidaan keinona sekoittaa "oikea" ja online-elämä ja olla yhteydessä ystäviisi ja perheeseesi.

Sosiaalisen median alustat normalisoivat tätä tekniikkaa, koska heillä on kannustin tehdä niin - eikä se ole sinun turvallisuutesi. Se, mitä se todella tekee, on tarjota [Big Tech](#) -alustoille, [kuten](#) Googlelle ja Metalle, mahdollisuus loukata yksityisyyttäsi ja myydä tietojasi.

Sijaintisi vapaaksi antaminen Instagramin tai minkä tahansa muun alustan kautta ei ehkä tunnu invasiiviselta, mutta sillä on kauaskantoisia seurauksia. Sijaintisi on arvokas datapiste sekä hallituksille että mainostajille. Mainostajat voivat nähdä, minne menet, ymmärtää tapojasi ja rutiinejasi ja markkinoida sinulle vastaavasti. Tietojasi, mukaan lukien sijaintisi, käytetään luomaan sinusta yksityiskohtainen digitaalinen profiili, joka voidaan myydä [tietojen välittäjille](#) ja kolmansille osapuolille.

Hallitukset voivat myös käyttää tietojasi valvontatarkoituksiin. He eivät tarvitse etsintälupaa, kun jaat sijaintisi sosiaalisen median kautta. Lainvalvonta luottaa yhä enemmän [Sosiaalisen median tiedot\(uusi ikkuna\)](#) rakentaa tapauksia ja asettaa syytteeseen ihmisiä. Sijaintisi antaa sinusta henkilökohtaisia tietoja, joita voidaan käyttää syytteeseen, jos elät hallinnon alaisuudessa, joka kriminalisoi asioita, kuten abortti, viisumirikkomukset tai homoseksuaalisuus.

Sen lisäksi, että Big Tech loukkaa yksityisyyttäsi, sijainnin jakaminen luo myös mahdollisuuksia kyberstalkkaukseen. Perheväkivallan hyväntekeväisyysjärjestö [Turvapaikka\(uusi ikkuna\)](#) kirjoittaa, että ”moderni teknologia antaa väärinkäyttäjille jatkuvasti kasvavia tapoja väijyä, eristää ja hallita naisia jokapäiväisen elämän työkalujen avulla.” Tässä yhteydessä elävän syötteen luominen ihmisen toiminnasta on uskomattoman vaarallista. Live-syötteen luominen [Lapsen toiminta](#) Se on vielä vaarallisempaa.

Riskit, jotka liittyvät sijaintisi säännölliseen jakamiseen sosiaalisen median kautta, ovat paljon suuremmat kuin hyödyt. Jos olet valmis vähentämään sijaintisi jakamisen normalisointia verkossa, on helppo hallita näitä tietoja.

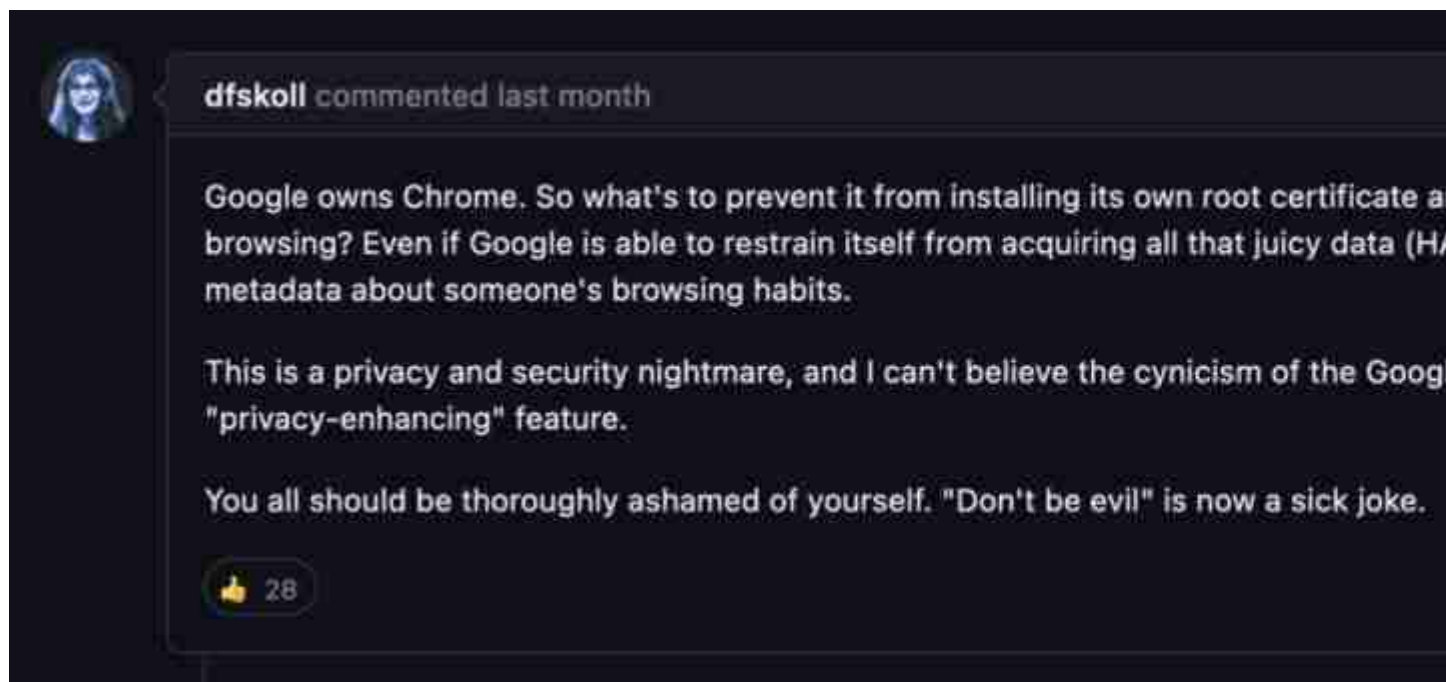
Viime kuussa Google julkaisi Chromelle uuden ominaisuuden nimeltä IP Protection, joka helpottaa yrityksen vakoilua sinua. Ei ihme, sillä tämä on Googlen liiketoimintamalli. Mutta huolestuttavaa on, että Google markkinoi tätä tietosuojaoimaisuutena.

Yhä enemmän Google käyttää yksityisyyden pesua, väärän mainonnan muotoa, joka on suunniteltu huijaamaan ihmisiä ajattelemaan, että heidän tuotteensa ovat yksityisiä.

Ennen IP-suojauksia oli ”[parannettu mainosten yksityisyys\(uusi ikkuna\)](#)”, toinen Chrome-ominaisuus, joka on suunniteltu vangitsemaan sinut Googlen valvontaverkostoon muiden yritysten ulkopuolelle.

IP-suojauksen taustalla oleva ajatus on pitkälti sama. Se suojaa tietokoneesi IP-osoitteen muilta verkkosivustoilta ja siirtää samalla kaiken verkkoliikenteesi Googlen omistaman palvelimen kautta. Tämä antaa Googlelle Jumalan silmänäkymän jokaisesta verkkosivustosta, jolla vieraillet koko ajan Chromen käytön aikana, riippumatta siitä, oletko kirjautunut Google-tilillesi vai et. **IP-suojaukseen ei ole mitään tietosuojatua nykyisessä muodossaan, ja suosittelemme, että ihmiset eivät ota sitä käyttöön.**

Myös muut yksityisyyden puolustajat herättävät hälytyksen. Kehittäjät, jotka tarkistavat koodipohjaa, ovat [voimakkaasti kritisoitu Google\(uusi ikkuna\)](#).



"Tällä ei ole *mitään* tekemistä turvallisuuden kanssa", yksi kehittäjä kirjoitti. "Tässä on kyse kontrollista, tietojen keräämisestä ja Googlen aseman varmistamisesta internetin mainosjohtajana."

Miksi Google tekee näin?

Googlen kilpailuetu on sen erittäin kohdennettu mainonta, ja sen 80 prosenttia on [\\$224 miljardia liikevaihtoa\(uusi ikkuna\)](#) tulossa mainoksista. Nämä mainokset ovat arvokkaita vain niin kauan kuin Google tietää kaiken kiinnostuksen kohteistasi hakujesi ja selaustoimintasi perusteella.

Maailman suosituimpana verkkoselaimena Chrome on Googlen ikkuna miljardeille ihmisille, erityisesti yhdistettynä muihin tietolähteisiin, kuten Google Searchiin tai Google Mapsiin. Jos olet

kirjautunut Google-tilillesi, esimerkiksi päästäksesi Gmailiin, yritys voi sitten liittää kaikki hakusi tiliisi. Yhtiöllä on tapoja seurata sinua [Vaikka käyttäisit Incognito-tilaa\(uusi ikkuna\)](#).

Siksi IP-suojaus on huijausta. Alkuvaiheessa Google Chrome käyttää omaa välityspalvelintaan luodakseen väliaikaisen IP-osoitteen piilottaakseen todellisen IP-osoitteesi Googlen omistamien tiettyjen verkkosivustojen luettelosta. Jotta IP-suojaus voidaan ottaa käyttöön tässä vaiheessa, sinun on otettava yhteyttä.

Tulevissa vaiheissa Google sanoo, että se voi lisätä toisen välityspalvelimen, jota ylläpitää toinen yritys. "Toinen hyppy", kuten he kutsuvat sitä, näkisi vain väliaikaisen IP-osoitteen ensimmäisestä palvelimesta ja verkkosivustosta, jolla aiot vierailla. Tämä toinen yritys on oletettavasti riippumaton, mutta Google todennäköisesti valitsisi palveluntarjoajan ja määritteli sen käytännöt.

Kaksihop-järjestelmä voi näyttää tietosuojaedulta - paitsi että Googllella on jo lukuisia muita tapoja seurata sinua. Google näkee hakuhistoriasi, Google Analyticsin, Chrome-historiasi, evästeesi mainosverkostossaan, mobiilisijainnissa, postilaatikossa, kalenterissa ja edelleen. Mitä järkeä on toisessa tietosuojakerroksessa, kun Google voi seurata toimintaasi niin monella muulla tavalla?

IP-suojauksessa on kyse kahdesta asiasta: yksityisyyden pesusta ja vallihaudan rakentamisesta.

Google haluaa vakuuttaa sinulle, että sen palvelu on yksityinen, samalla kun se kerää intiimiä dataasi ja estää kilpailijoita tekemästä samoin. IP-suojausseinät poistavat tietosi muusta internetistä ja tiivistävät samalla Googlen valvontalaitteen seinän puolelle.

Mitä IP-suojauksen sijaan voi tehdä?

Yksityisyysseinän rakentaminen on helppo aloittaa Googlen kanssa ulkopuolella

Voit suojata selaustoimintasi ja suorittaa IP-suojauksen vaatimukset yksinkertaisesti yksityisyyttä suojaavalla selaimella ja VPN: llä. Yksi Googlen IP-suojauksen tavoitteista saattaa itse asiassa olla estää käyttäjiä käyttämästä itsenäisiä VPN-palveluita, varsinkin kun paremmissa VPN-palveluissa on sisäänrakennetut mainos- ja seurantaestotekniikat (kuten NetShield Proton VPN:ssä).

Käytä yksityistä selainta

Google Chrome on huono yksityisyyden kannalta. Mutta niitä on [vaihtoehtoja, jotka kunnioittavat yksityisyyttäsi\(uusi ikkuna\)](#). Vaikka Chrome kerää tietoja siitä, mitä teet verkossa, Firefoxin kaltaiset selaimet eivät. Jos olet joku, joka välittää yksityisyyden parantamisesta Googlessa, sinun pitäisi vain [Lopeta Googlen käyttö\(uusi ikkuna\)](#).

Parhaat selaimet yksityisyydellesi vuonna 2025

Tämä artikkeli päivitettiin syyskuussa 2025 vastaamaan viimeisimpiä muutoksia ja päivityksiä käsiteltyihin selaimiin. Olemme myös lisänneet luetteloon Zen Browserin ja Ladybirdin.

Verkkoselaimesi on ikkunasi verkkomaailmaan. Pöytätietokoneissa ja kannettavissa tietokoneissa se on ensisijainen keino käyttää maailmanlaajuista verkkoa ja muita Internet-palveluja.

Sovellusten suosion ansiosta selain on vähemmän tärkeä mobiilialustoilla, mutta se on edelleen tärkein tapa käyttää useimpia verkkosisältöjä. Ja jos välität yksityisyydestä, päästä palveluun sen avulla [Verkkosivusto paljastaa paljon vähemmän tietojasi\(uusi ikkuna\)](#) kuin käyttää sen sovellusta.

Selaimellasi on suora pääsy henkilökohtaisimpien ja intiimimpien tietojesi aarteisiin. Teoriassa selaimesi voi lähettää tietueen kaikesta, mitä teet verkossa, takaisin sen kehittäjille - jopa mitä kirjoitat kenttiin yksittäisillä verkkosivuilla.

Tästä syystä me Protonilla katsomme, että on tärkeää selittää ihmisille, mitä selaimia he voivat käyttää, jos he haluavat pitää online-toimintansa yksityisenä. Siellä on satoja selaimia, joten emme voineet tutkia niitä kaikkia. Kokosimme kuitenkin luettelon kahdeksasta avoimen lähdekoodin selaimesta, jotka kunnioittavat yksityisyyttäsi vaihtelevassa määrin.

- [Mozilla Firefox-Säh](#)
- [Kromi](#)
- [Rohkea](#)
- [Tor-selain](#)
- [Firefox Focus -toiminto](#)
- [LibreWolf-Susi](#)
- [Zen-selain](#)
- [Leppäkerttu](#)

Omat selaimet

Saatat huomata, että monet suosituimmista selaimista, nimittäin Google Chrome, mutta myös Apple Safari ja Opera, eivät sisälly yllä olevaan luetteloomme. Tämä johtuu siitä, että he, kuten useimmat suositut selaimet, käyttävät omaa suljettua koodia, joten emme voi tietää, miten he käsittelevät tietojasi. Suljettua koodia käyttävät selaimet ovat:

- Google Chrome
- Microsoft Edge -käyttöjärjestelmä
- Apple Safari
- Ooppera
- Vivaldi
- Samsung Internet-yhteys
- UC-selain
- DuckDuckGo-tietosuojaselain

Nämä selaimet ovat epäilemättä turvallisia, koska niillä on lukuisia erittäin tehokkaita suojausmekanismeja hakkeriteitä vastaan. Mutta pitäisikö meidän luottaa siihen, että he kunnioittavat yksityisyyttämme?

Googlen koko liiketoimintamalli on loukata yksityisyyttämme, jotta se voi paremmin kohdistaa meille erittäin personoituja mainoksia. Microsoft tekee myös rahaa kohdennetusta mainonnasta ja sillä on [pitkät tiedot käyttäjien yksityisyyden loukkaamisesta\(uusi ikkuna\)](#).

Apple markkinoi itseään käyttäjiensä yksityisyyden puolustajana, mutta se teki täysimääräistä yhteistyötä [NSA:n PRISM-vakoiluohjelman\(uusi ikkuna\)](#) että Edward Snowden paljasti vuonna 2013. Sen suhtautuminen kilpaileviin selaimiin iOS-alustallaan (keskustellaan alla) tekee myös selväksi, että sen käyttäjien etu ei ole yrityksen ensisijainen tavoite.

Tärkeintä on, että emme yksinkertaisesti tiedä, kuinka invasiivisia nämä selaimet ovat yksityisyytellemme, koska ne ovat suljettuja (vaikka Chromen on osoitettu käyttävän seurantalaitteita "[järjettömät mittasuhteet\(uusi ikkuna\)](#)").

Kyse on siitä, kuinka paljon luotat kehittäjiin näillä selaimilla. Vaikka *doluottaisitkin* heihin, hyvä turvallisuus ei toimi näin.

Avoimen lähdekoodin selaimet

Avoin lähdekoodi ei ole ihmelääke, kun on kyse ohjelmistojen yksityisyyden ja turvallisuuden varmistamisesta. Pelkkä selaimen luomiseen liittyvän koodin määrä tarkoittaa, että ammattimaiset ohjelmistotarkastajat voivat jättää asioita paitsi.

Kuitenkin se, että kuka tahansa voi tutkia koodia (ja suosittujen selainten tapauksessa, monet ovat), tarjoaa kuitenkin parhaan mahdollisen varmuuden siitä, että sen koodi on virheetön eikä sisällä piilotettuja yllätyksiä.

Siksi harkitsemme tässä artikkelissa vain täysin avoimen lähdekoodin selaimia.

Selaimet iOS:ssä ja iPadOS:ssä

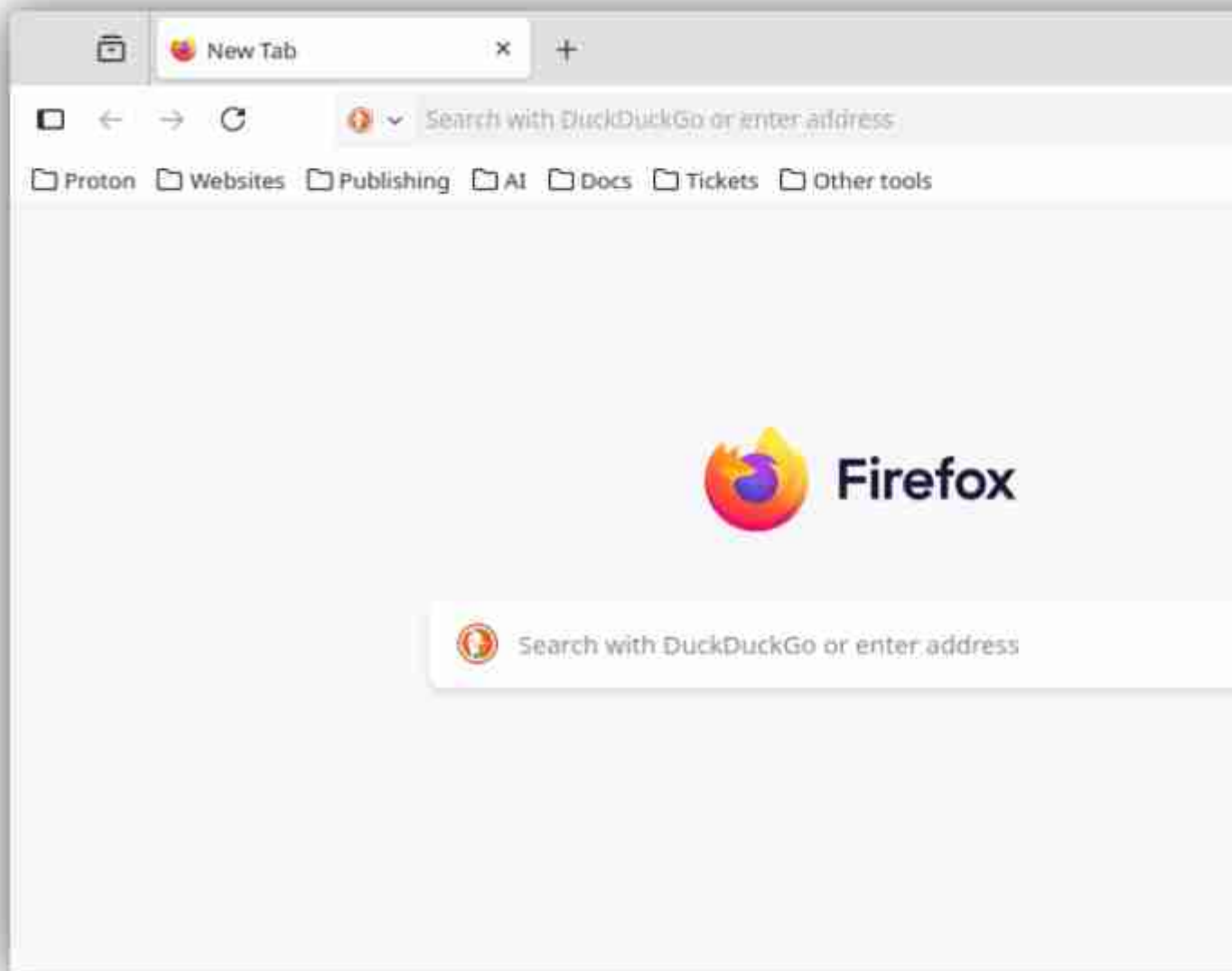
Omena [pakottaa kaikki selaimet\(uusi ikkuna\)](#) iOS- ja iPadOS-alustoillaan omien käyttö [WebKit-selainmoottori\(uusi ikkuna\)](#). (A) [selainmoottori\(uusi ikkuna\)](#) muuntaa HTML-tiedoston visuaaliseksi verkkosivuksi, jonka kanssa voit olla vuorovaikutuksessa.) Tämä tarkoittaa, että kaikki iOS:n kolmannen osapuolen selaimet ovat periaatteessa vain Safarin uudelleenbrändättyjä versioita (paitsi että Safari iOS:lle tarjoaa edistyneitä ominaisuuksia, joita Apple estää kilpailijoiltaan).

Siksi kaikki tässä artikkelissa käsitellyt selaimet koskevat kommentit **nimenomaisesti sulkevat pois niiden iOS-versiot**. Nämä selaimet voivat silti olla hyödyllisiä iOS: ssä (esimerkiksi kirjanmerkkien synkronointiin, avoimiin välilehtiin ja selaushistoriaan kaikissa laitteissasi), mutta ne eivät sisälly alla käsiteltyihin sovelluksiin.

Vaikka se ei ole suoraan merkityksellinen tämän artikkelin kannalta, on huomattava, että iOS: n sovelluksen sisäiset selaimet, kuten iOS: n käyttämät [TikTokissa\(uusi ikkuna\)](#), [Instagram ja Facebook\(uusi ikkuna\)](#) sovellukset, voivat olla hyvin epävarmoja ja niitä tulisi välttää hinnalla millä hyvänsä.

Parhaat turvalliset ja yksityisyys-ensimmäiset verkkoselaimet

Mozilla Firefox-Säh



Plussat

- Paljon yksityisyyttä parantavia ominaisuuksia, joissa on aina enemmän kehitystä
- Suuri selainlisäosien ekosysteemi
- Turvallinen laitteiden ja alustojen välinen synkronointi
- Ainoa avoimen lähdekoodin kilpailu Googlen selainmoottorille
- Saatavilla kaikilla tärkeimmillä alustoilla

Miinukset

- Haavoittuva selaimen sormenjäljille
- Liikaa telemetriaa
- Liian riippuvainen Googlesta rahoitukseen

Firefox on avoimen lähdekoodin selain voittoa tavoittelemattomasta Mozilla-organisaatiosta. Se keskittyy yksityisyytesi suojaamiseen sisäänrakennetulla [parannettu seurantasuojaus\(uusi ikkuna\)](#), joka sisältää [sormenjälkien ottaminen resistenssi\(uusi ikkuna\)](#). Kuitenkin, suoritetuissa testeissämme, Firefoxin puhtaassa asennuksessa oli edelleen [ainutlaatuinen selaimen sormenjälki\(uusi ikkuna\)](#).

Firefoxin oletusasetukset korostavat yksityisyyttä, mutta voit mukauttaa niitä tarjoamaan entistä paremman yksityisyyden. Voit esimerkiksi hienosäätää evästeitä ja jäljittämiä, jotka estät.

Mahdollisuus muokata Firefoxia parantaa entisestään sen tuki valtavalle valikoimalle [Kolmannen osapuolen lisäosat\(uusi ikkuna\)](#), joista monet tarjoavat erinomaisia tietosuojatietoja. Hyviä esimerkkejä ovat [Yksityisyysmäyrä\(uusi ikkuna\)](#), [Cookie AutoPoista\(uusi ikkuna\)](#), [uBlock Alkuperä\(uusi ikkuna\)](#), [Decentraleyes-tuotteet\(uusi ikkuna\)](#), ja enemmänkin. Ja toisin kuin Chromium-pohjaiset selaimet, Mozillalla on [Ei suunnitelmia \(uusi ikkuna\)](#) alentaa vanhempia (Manifest V2) laajennuksia.

Tässä on se, että jokainen käyttämäsi lisäosa lisää Firefoxin esiintymän ainutlaatuisuutta, mikä tekee sinusta alttiimman sormenjälkien sormenjäljille.

Yksityisyysnäkökohtien ulkopuolella Firefox on kevyt, nopea ja täysin varusteltu moderni selain, joka voi synkronoida välilehdet, kirjanmerkit ja selaushistorian useilla alustoilla päästä päähän - salauksen avulla. Valitettavasti Mozilla on äskettäin tehnyt useita harha-askeleita, jotka vieraannuttivat monia Firefox-käyttäjiä. Näitä ovat:

- **Käyttöehdot** - Uusi kieli näytti myöntävän Mozillalle laajan, rojaltivapaan lisenssin käyttäjä mitä tahansa Firefoxin syöttämäsi sisältöä, jonka monet pelkäsivät viittaavan heidän tietojensa omistamiseen. Myös nimenomaisen ”älä koskaan myy käyttäjätietoja” -lupauksen poistaminen aiheutti hälytyksen. Vastaiskun jälkeen Mozilla [selkeytetty\(uusi ikkuna\)](#) että tämä lisenssi oli tarkoitettu yksinomaan Firefoxin käyttämiseen ja teki *ei* merkitsee käyttäjien tietojen omistajuutta.
- **Taskuintegraatio** – Suljetun lähdekoodin Pocket-lukulistapalvelu oli aluksi pakollinen asentajassa, sitten valinnainen, mitä monet avoimen lähdekoodin puristit pitivät "täysin avoimen lähdekoodin" lupauksen rikkomisena. Pocket poistettiin heinäkuussa 2025
- **Riippuvuus Googlen tuloista** — Sopimus Googlen kanssa, jotta Google voi tehdä hakuista oletushakukonetilinsä [85 % Mozillan liikevaihdosta\(uusi ikkuna\)](#). Monet pitivät tätä luottamusta juuri siihen, mitä Firefoxin pitäisi olla vaihtoehto, jota ei voida hyväksyä.
- **Telemetria** — Firefox lähettää myös [enemmän metatietoja\(uusi ikkuna\)](#) takaisin Mozillan oletusarvoisesti kuin useimpien ihmisten pitäisi olla tyytyväisiä (vaikka voit poistaa tämän käytöstä käytöstä).

On kuitenkin huomattava, että Firefox tekee myös monia asioita oikein: Esimerkiksi:

- **Parannettu sertifikaattien hallinta** — Käyttää [CRLite-ohjelma\(uusi ikkuna\)](#) teknologiaa tarkistaa nopeasti ja saumattomasti ja välittömästi epäluotettava [TLS-todistukset](#).
- **Täydellinen evästesuojaus(uusi ikkuna)** — Tämä on nyt oletusarvoisesti käytössä Standard-tilassa, mikä varmistaa, että kolmannen osapuolen evästeet estetään, ellei se ole ehdottoman välttämätöntä.
- **Tehostettu seurantasuojaus(uusi ikkuna)** Strict-tilassa — Sisältää **Pomppuseurantasuojaus** että estää uudelleenohjausseurantalaitteiden (poistoseurantalaitteiden) keräämisen, kun siirryt verkkosivustojen välillä.

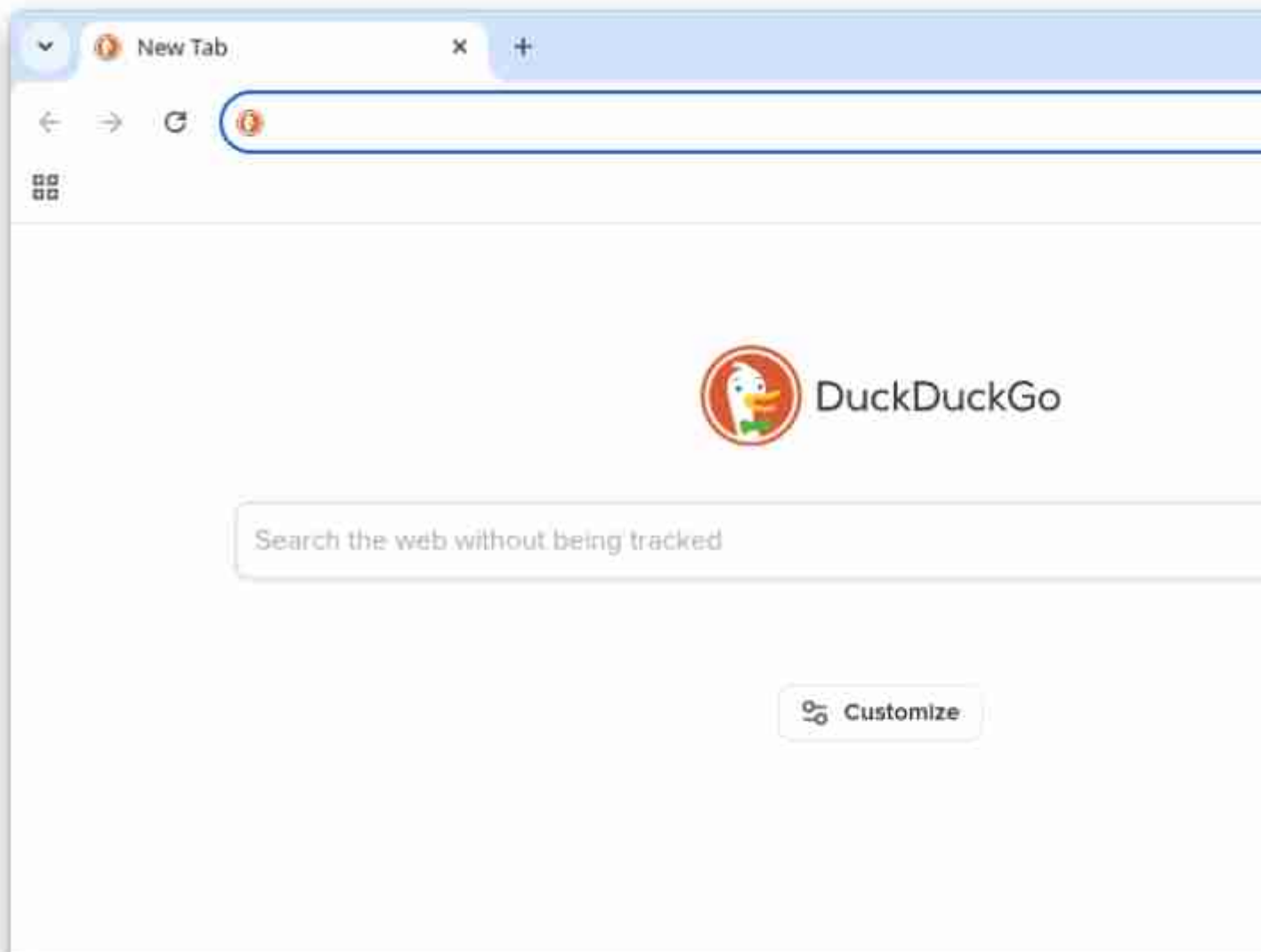
- **Unified Consent** Dialog – Parantaa, miten tietojen suostumus toimii selaimen laajennuksissa.

Ja mitä tahansa näkemyksesi tekoälystä, sen uusista [shake-to-summare\(uusi ikkuna\)](#) ominaisuus iOS on epäilemättä innovatiivinen.

Loppujen lopuksi, kaikista Mozillan vioista huolimatta, Firefox on loistava selain. Se on myös Chromen *Ainoastaan* todellinen ilmainen ja avoimen lähdekoodin kilpailija. Sen jyrkkä [markkinaosuuden lasku\(uusi ikkuna\)](#) Siksi heidän pitäisi olla syvästi huolissaan kaikille, jotka arvostavat yksityisyyttään.

Kyllä, voit käyttää Firefox-haarukkaa sen sijaan (kuten LibreWolf tai Zen Browser, jota käsitellään alla), mutta vain Mozillalla on resursseja (ongelmallinen kuin nämä voivat olla) tarjota kriittisiä rutiininomaisia tietoturvapäivityksiä ja kehittää uusia ominaisuuksia, jotka tarjoavat sille ainakin jonkin verran kilpailukykyä kaupallisia kilpailijoitaan vastaan.

Kromi



Plussat

- Se on Chrome, jossa kaikki oma koodi on poistettu

- Tukee Chrome-selaimen laajennuksia

Miinukset

- Ei sisäänrakennettua synkronointiratkaisua
- Ei automaattista päivitystä (oletuksena)
- Haavoittuva selaimen sormenjäljille
- Se on edelleen Google-tuote

Jotta näet koodin avoimen lähdekoodin arvon, sinun ei tarvitse etsiä kauempaa kuin Chromium. Google tekee Chrome-selaimensa ydinkoodin (helposti [suosituin selain maailmassa\(uusi ikkuna\)](#)) avoin lähdekoodi, jotta turvallisuusyhteisö voi tarkistaa ja tarkastaa sen.

Chromium on (lähinnä) avoimen lähdekoodin versio Chrome-selaimesta, jossa kaikki Googlen oma koodi on poistettu. Tai ainakin näin sen pitäisi toimia. Kuitenkin äskettäinen sisällyttäminen [Google Safe Browsing -toiminto\(uusi ikkuna\)](#) binary tarjota rakennettu-in [tietojenkalastelu\(uusi ikkuna\)](#) ja [haittaohjelma\(uusi ikkuna\)](#) suojaus tarkoittaa, että kromia ei voida enää pitää täysin avoimena lähdekoodina. Toinen huolenaihe on, että sen koodikannan koon ja monimutkaisuuden vuoksi jokin ei-toivottu Google-koodi saattaa jäädä huomaamatta.

Chromium on saatavana valmiiksi rakennettuina latauksina Windowsille, macOS:lle, Linuxille ja Androidille (esimerkiksi [Bromiitti\(uusi ikkuna\)](#)).

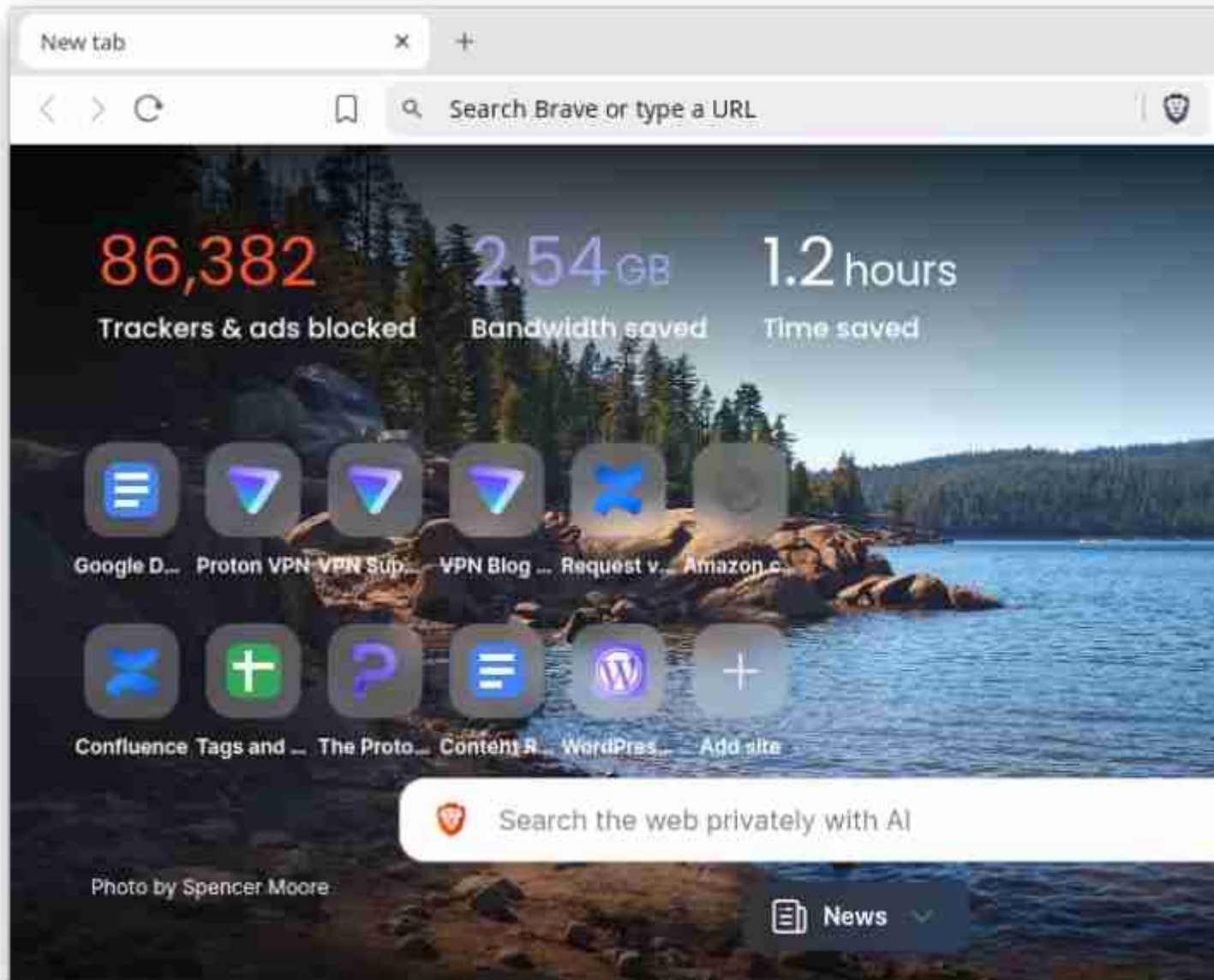
Lukuun ottamatta joitakin pieniä brändäystietoja, Chromium tarjoaa lähes identtisen selauskokemuksen Chromelle. Valitettavasti vuonna 2021 Google veti [tuki välilehtien, historian ja kirjanmerkkien synkronointiin\(uusi ikkuna\)](#) Google-tilin käyttäminen. Kolmannen osapuolen synkronointivaihtoehdot ovat olemassa, mutta useimmat näistä eivät ole avointa lähdekoodia.

Synkronoimalla ongelmat sikseen, Chromium tarjoaa saumattoman tavan siirtyä pois Chromesta (kunhan et välitä edelleen käyttää Googlen luomaa koodia), ja se sisältää nyt rajoitettuja yksityisyyttä parantavia ominaisuuksia, kuten [paikan eristäminen\(uusi ikkuna\)](#) ja [hiekkalaatikko\(uusi ikkuna\)](#).

Chrome-selainlaajennusten täysi tuki tarkoittaa, että voit asentaa kolmannen osapuolen tietosuojaratkaisuja, vaikka mikä tahansa selainlaajennus lisää selaimen sormenjäljen ainutlaatuisuutta. Kun testasimme Chromiumin uutta puhdasta installaatiota, [Peitä Jäljit\(uusi ikkuna\)](#) ilmoitti, että sillä oli ainutlaatuinen sormenjälki.

Toinen ongelma on, että Chromium ei oletusarvoisesti päivitä automaattisesti, mitä suosittelemme kaikille tekemään, koska päivitykset sisältävät uusimmat tietoturvakorjaukset. Tämä ei ole suuri ongelma Linuxissa, koska useimmat pakettien hallinnat päivittävät sovelluksen. On myös useita kolmannen osapuolen työkaluja, jotka on suunniteltu auttamaan tässä Windowsissa ja macOS: ssä.

Rohkea



Plussat

- Sormenjälkiä kestävä
- Paljon out-of-the-box yksityisyyttä parantavia ominaisuuksia
- Yhteensopiva Chrome-selainlaajennusten kanssa
- Turvallinen laitteiden ja alustojen välinen synkronointi
- Saatavilla kaikilla tärkeimmillä alustoilla
- Ei oletusarvoisesti telemetriaa (opt-in anonymit käyttäjämittarit käytettävissä)

Miinukset

- Valinnaiset kryptovaluutta- ja mainostuetut ominaisuudet eivät välttämättä miellytä puristeja
- Automaattisesti uudelleenohjatut kryptovaluuttahaut affiliate-linkkeihin
- Perustuu Google-koodiin

Ensimmäisen kerran vuonna 2016 julkaistun vuoden 2016 Braven kehitti entinen Mozillan toimitusjohtaja ja JavaScriptin keksijä Brenden Eich. Chromiumille rakennettu Brave on suunniteltu

vahvalla yksityisyyspainotteisella. Kuten Chromiumissa, Brave sisältää nyt suljetun lähdekoodin Google Safe Browsing -binääriin.

Yksi tämän selaimen merkittävimmistä asioista on Brave Search, a [nyt täysin riippumaton\(uusi ikkuna\)](#) hakukone, joka ratkaisee kaikki kyselyt paikan päällä välittämättä niitä kolmannelle osapuolelle. Tätä tuetaan ensisijaisesti "yksityisyyttä säilyttävillä" mainoksilla, vaikka voit valita nämä maksullisella tilauksella.

Itse selaimessa on sisäänrakennettu seurantasuojaus, sisäänrakennettu mainos- ja kommentosarjaesto, sisäänrakennettu [HTTPS-Kaikkialla\(uusi ikkuna\)](#) toiminnallisuus, ja yhden napsautuksen anti-sormenpainatus. Testeissämme Brave oli ainoa selain, joka oli täysin tehokas selaimen sormenjälkien ottamista vastaan työpöydällä ja Android-sovelluksessaan (vaikkakaan ei ole yllättävää, ei iOS: ssä / iPadOS: ssä).

Sisään [vuoden 2020 tutkimus\(uusi ikkuna\)](#), se oli myös helposti kaikkein yksityinen selain telemetrian suhteen, joka lähetettiin takaisin kehittäjilleen.

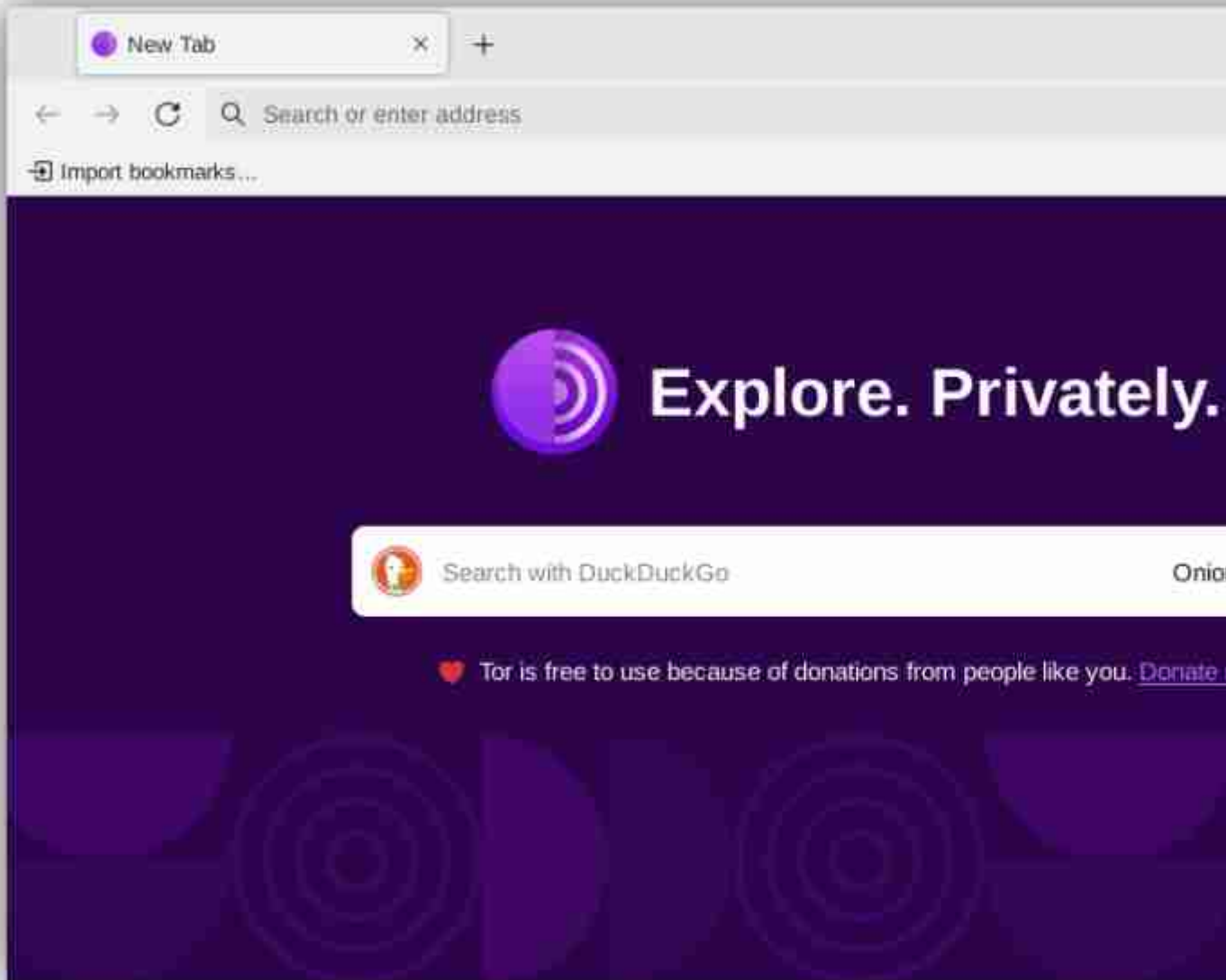
Brave estää oletusarvoisesti kolmannen osapuolen evästeet ja voi jopa estää evästeiden suostumusilmoitukset (nyt tekoälyn käyttäminen suorituskyvyn parantamiseksi). Koska Brave perustuu Chromiumiin, voit käyttää tavallisia Chrome-selainlaajennuksia (ladattu joko omasta Brave Web Storesta tai Chrome Web Storesta). Brave tarjoaa myös turvallisen välilehden, historian ja kirjanmerkkien synkronoinnin laitteiden ja alustojen välillä.

Brave tarjoaa kuitenkin myös kiistanalaisempia ominaisuuksia. [Rohkeat palkinnot\(uusi ikkuna\)](#) voit ansaita BAT (Basic Attention Tokens, Braven oma kryptovaluutta, jonka voit muuntaa rahaksi) valitsemalla nähdä mainoksia kaupallisilta kumppaneilta. Vielä pahempaa, yli \$100: n voitot vaativat nyt henkilöllisyytesi vahvistamista.

Muita ominaisuuksia ovat Brave News ja [Rohkea lompakko\(uusi ikkuna\)](#), kryptovaluutta- ja NFT-lompakko, joka on sisäänrakennettu selaimen. [Rohkeat uutiset\(uusi ikkuna\)](#) on henkilökohtainen, mainosten tukema uutissyöte (ja personointi suoritetaan laitteella yksityisyytesi suojaamiseksi). Jos käytät uutta [Leo AI -avustus\(uusi ikkuna\)](#)nt, se lähettää joitakin metatietoja, kyselykonteksti, jne., sen backend.

On huomattava, että kaikki nämä "ominaisuudet" ovat tiukasti opt-in. Vuonna 2020 Brave joutui kuitenkin pyytämään anteeksi automaattisesti [Kryptovaluuttahakujen uudelleenohjaaminen maksettuihin affiliate-linkkeihin\(uusi ikkuna\)](#) että se on maksettu. Se teki tämän kysymättä käyttäjiensä lupaa.

Tor-selain



Plussat

- Paras tapa käyttää Tor-anonymiteettiverkkoa
- Vahva yksityisyyden suoja
- Tarjoaa osittaisen suojan sormenjälkiä vastaan
- Saatavilla useimmilla alustoilla (ei iOS)

Miinukset

- Voi olla jäljessä Firefoxista ominaisuuksien suhteen
- Ei synkronointitoimintoa
- Erittäin hidas käytettäessä Tor-verkkoa

Tor Browser on Firefox ESR:n haarukoitu versio, joka reitittää kaikki yhteydet [Tor-anonymiteettiverkosto\(uusi ikkuna\)](#). Se on myös "karkaistu" parantamaan yksityisyyttä ja tarjoaa

valmiita ominaisuuksia, kuten sisäänrakennettuja [HTTPS kaikkialla\(uusi ikkuna\)](#) tuki, komentosarja-esto, ja se käyttää aina [yksityinen selaustila\(uusi ikkuna\)](#).

Koska kaikki muokkaamattomat Tor-selaimet näyttävät täsmälleen samalta, asiantuntijat suosittelevat sitä usein parhaana tapana estää selaimen sormenjälkien ottaminen. Omissa testeissämme se tarjosi kuitenkin vain osittaisen suojan ja oli Braven parempi.

Tor Browser on rakennettu Firefox ESR: lle (laajennettu tukiversio yrityskäyttöön), joka yleensä seuraa tavallisen version takana ominaisuuksien suhteen. Lisäksi Tor testaa ja muokkaa laajasti uusia versioita parantaakseen yksityisyyttä ennen niiden julkaisemista. Nettotulos on, että Tor Browser voi olla jäljessä Firefoxin uusimmista ominaisuuksista (nämä uudet ominaisuudet ovat usein pois päältä tietosuojasyistä joka tapauksessa).

Tor Browser voi käyttää tavallisia Firefox-selaimen lisäosia, mutta tätä ei suositella, koska ne lisäävät selaimeen ainutlaatuisuutta. Synkronointitoimintoa ei ole.

Kun Tor-verkkoa käytetään, Tor Browser tarjoaa korkeimman mahdollisen todellisen nimettömyyden Internetissä (mutta edes tätä ei pitäisi koskaan pitää 100% nimettömyytenä). Tämän hinta on valtava lasku selausnopeuksissa (tyypillisesti noin 90% tai enemmän), mikä tekee Tor-verkosta epäkäytännöllisen useimmissa päivittäisissä Internet-tehtävissä.

Voit käyttää Tor-selainta muodostamatta yhteyttä Tor-verkkoon. Tässä käyttötapauksessa se on hyvä yksityisyyteen keskittyvä selain, mutta tarjoaa melko paljon luin kokemuksen päivittäiseen selaamiseen.

Firefox Focus -toiminto

Plussat

- Vahva suoja seurantaan vastaan
- Ei oletuksena telemetriaa

Miinukset

- Ainutlaatuinen sormenjälki
- Liian vähän päivittäiseen käyttöön
- Käyttötilastot ja tutkimukset ovat opt-out-mahdollisuuksia

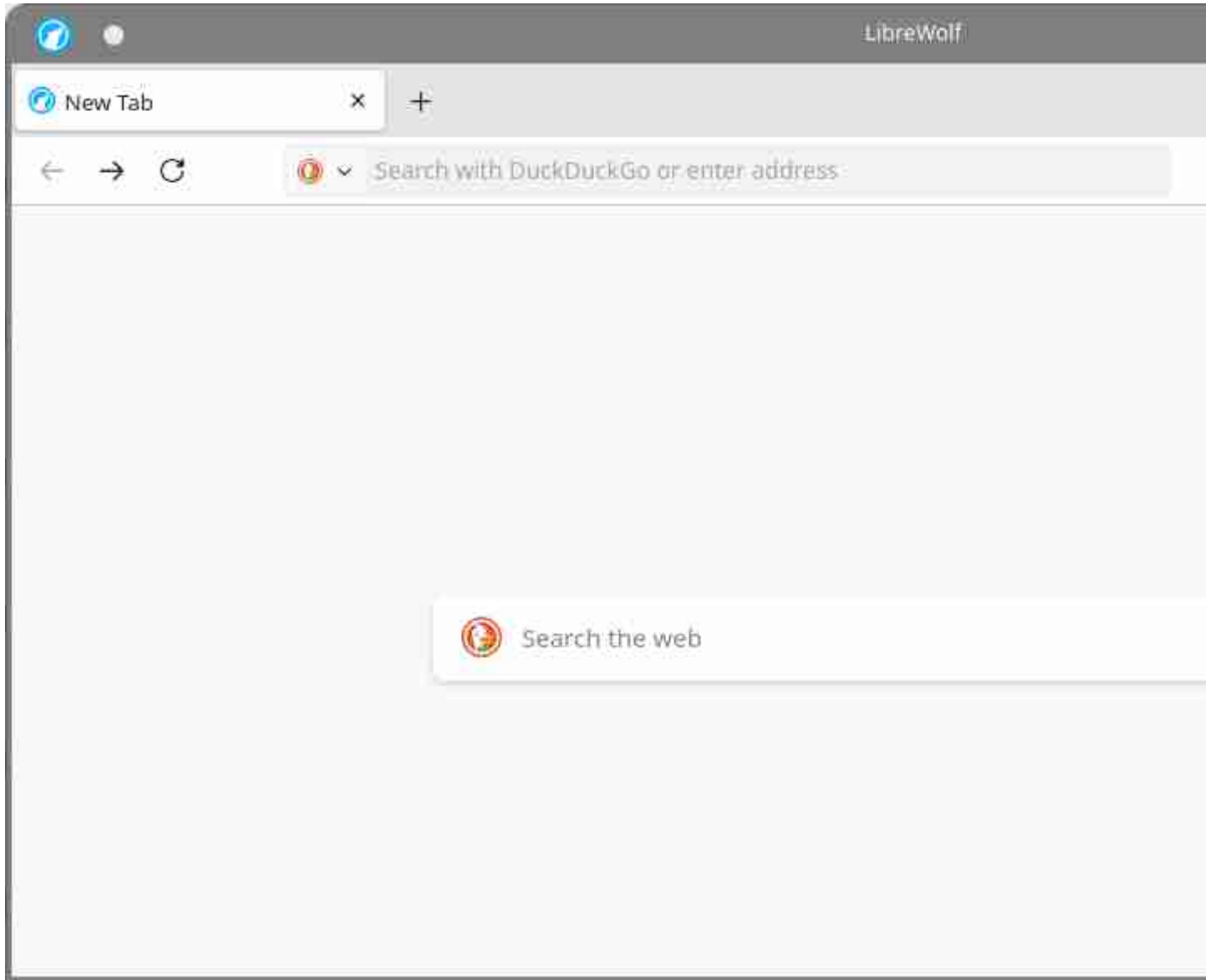
Tämä Mozillan mobiiliselain aloitti elämän seuranta-estosovelluksena iOS: ssä. Voit silti käyttää sitä iPhoneen ja iPadin seurantalaitteena, vaikka et käyttäisi itse selainta.

Firefox Focus perustuu tietysti Firefoxiin, mutta sillä on minimaalinen estetiikka. Ei ole tukea synkronoinnille, selaimen lisäosille tai edes uusien välilehtien avaamiselle (välilehtien selaaminen on mahdollista vain avaamalla linkki uuteen välilehteen).

Ei ole yllättävää, että Firefox Focusilla on tehokas seurantasuojaus ja mainosten estäminen (ei toisin kuin Proton VPN:n oma [Netshield Ad-blocker -editori\(uusi ikkuna\)](#) ominaisuus). Tervetulleessa muutoksessa käyttötilastot ovat opt-in, ja se toteuttaa nyt välilehteä kohti evästeiden eristämisen. Se on kuitenkin altis selaimen sormenjäljille.

Riisutun ominaisuuden ansiosta Firefox Focus on liian rajoitettu suosittelemaan päivittäiseen selaamiseen, mutta se on edelleen hyvä vaihtoehto, jos tarvitset korkeaa yksityisyyden tasoa (erityisesti iOS: ssä).

LibreWolf-Susi



Plussat

- Se on Firefox, mutta entistä paremmalla yksityisyyden suojalla
- Todella yhteisöllinen, avoimen lähdekoodin projekti
- Tukee Firefoxin synkronointia ja lisäosia

Miinukset

- Lähes ainutlaatuinen sormenjälki

LibreWolf on mukautettu Firefox-versio, joka on suunniteltu lisäämään suojaa seuranta- ja sormenjälkitekniikoilta ja sisältäen samalla monia muita tietoturvaparannuksia. Se on saatavilla Windowsille, macOS:lle ja Linuxille.

LibreWolf ei kerää telemetriaa, käyttää yksityisyysystävällisiä hakukoneita (DuckDuckGo, Searx, Qwant jne.), on uBlock Origin -selainlaajennus asennettuna oletusarvoisesti ja toteuttaa erilaisia [muut kovettumisominaisuudet\(uusi ikkuna\)](#) (erityisesti sisäänrakennettu DNS-yli-HTTPS (DoH)).

Sormenjälkitesteissämme LibreWolf sai paremman pistemäärän kuin vanilja Firefox ”lähes ainutlaatuisella” sormenjäljellä, mutta tämä on vielä kaukana ihanteellisesta.

LibreWolf perustuu aina Firefoxin uusimpaan versioon ja pyrkii julkaisemaan päivitykset kolmen päivän kuluessa uusimmasta Firefox-julkaisusta. Vaikka Firefox Sync ei ole oletusarvoisesti käytössä, voit helposti ottaa Firefoxin käyttöön LibreWolfin asetuksissa ja synkronoida kirjanmerkit, välilehdet ja selaushistorian eri alustojen ja laitteiden välillä. Se tukee myös tavallisia Firefox-lisäosia, kuten [Proton VPN:n\(uusi ikkuna\)](#) ja [Protonissi](#) selainlaajennukset.

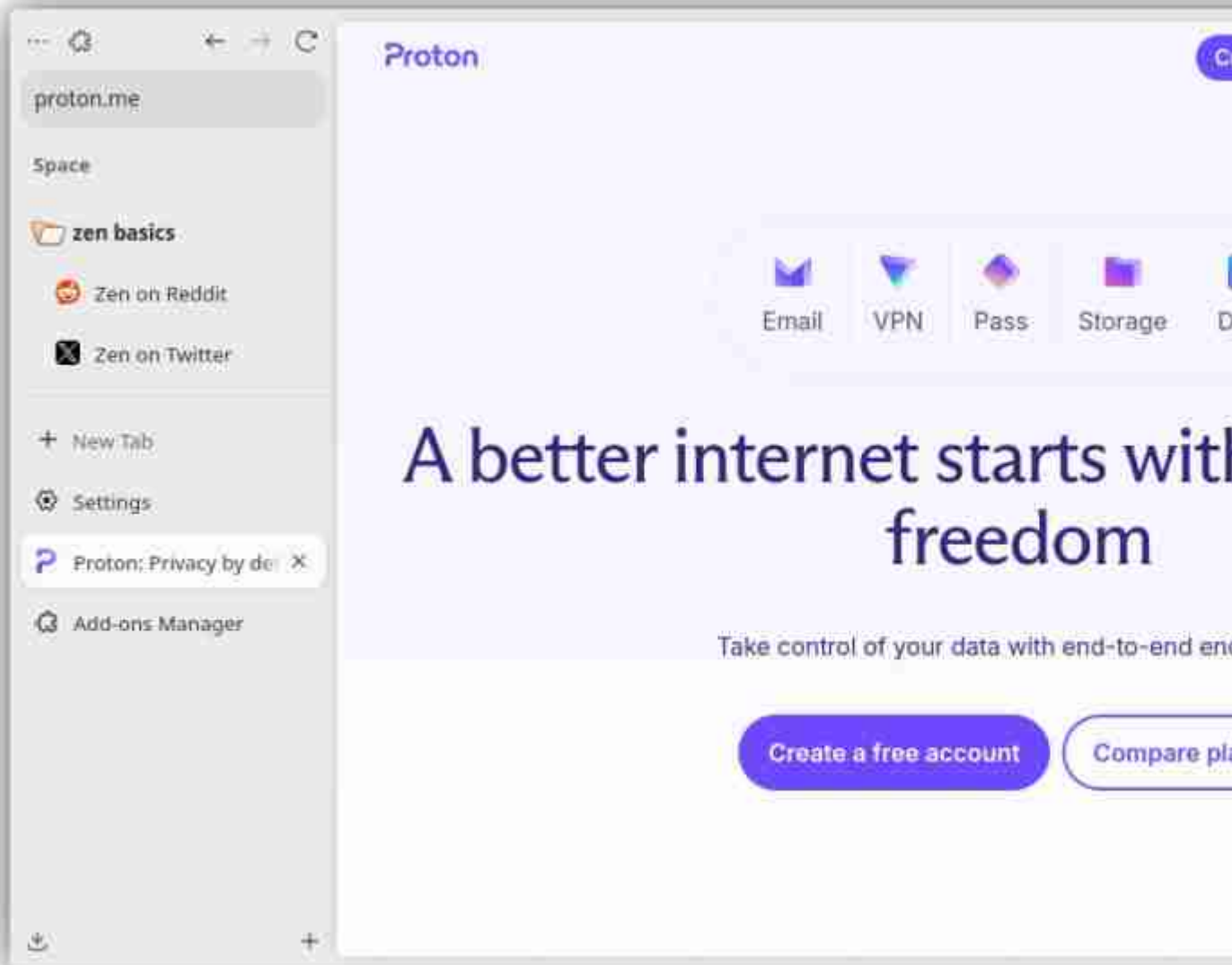
Zen-selain

Plussat

- Se on Firefox, mutta parempi käyttöliittymä (subjektiivinen)
- Ei koske Mozillan typerämpiä harha-askeleita (esimerkiksi ei telemetriaa)
- Tukee Firefoxin synkronointia ja lisäosia

Miinukset

- En ole kaikkien makuun
- Yhä beta-vaiheessa kirjoitushetkellä



Uusi (2024) Firefox-pohjainen lapsi lohkossa, Zen Browser toivoo ravistelevansa selainmaisemaa keskittyen yksityisyyteen ja tarjoamalla erittäin muokattavissa olevan minimaalisen käyttöliittymän.

Se vetää Firefox-päivitykset 72 tunnin kuluessa niiden julkaisemisesta, kerää telemetriaa, estää kolmannen osapuolen seurantalaitteet oletusarvoisesti, tarkistaa vaaralliset SSL-varmenteet, pakottaa automaattisesti HTTPS-vain jne. (periaatteessa, kuten Firefox tekee). Toisin kuin LibreWolf (joka räikkää ne oletusarvoisesti), Zen-selain on oletusarvoisesti Firefoxin hieman löysemmät "Standard" -yksityisyysasetukset, vaikka niitä voidaan tietysti muuttaa.

On luultavasti reilua ajatella Zen Browseria Firefoxina, jossa on esteettisesti parannettu muotoilu (jos pidät sellaisesta). Hyödyllisesti se tukee Firefox-lisäosia ja Firefox Sync -sovelluksia, joiden avulla Zenin ja muiden Firefox-pohjaisten selainten välillä on helppo hypätä saumattomasti (mukaan lukien mobiiliselaimet, mikä on kätevää, koska Zen Browser on tällä hetkellä vain työpöytä).

Leppäkerttu

Kukaan, joka välittää yksityisyydestä, ei halua maailmaa, jossa jokainen selain on Google Chromen (tai Applen Safarin) versio, jos käytät jotain sen omistamista ja kalliista lukituista laitteista.

Firefox on todella fantastinen avoimen lähdekoodin vaihtoehto näille, mutta huono hallinta ja joukko huonoja markkinointipäätöksiä ovat vieraannuttaneet jopa monia tietosuoja-fanaatikkoja, vahingoittaneet suuresti sen asemaa suuren yleisön kanssa ja jättäneet Mozillan voimakkaasti (ja hyvin ironista kyllä) riippuvaiseksi Googlen rahoituksesta (jota se toimittaa kilpailuoikeudellisista syistä) sen jatkuvasta olemassaolosta.

Enter-kirjautuminen [Leppäkerttu\(uusi ikkuna\)](#), avoimen lähdekoodin ja täysin uuden selaimen, jota ei vielä ole olemassa. Ensimmäinen julkinen alfa-julkaisu on suunnattu kesälle 2026 (Linux & macOS), ja se sisältää beta-julkaisun vuodelle 2027 ja täydellisen vakaan julkaisun vuodelle 2028. Työstäminen on kuitenkin alkanut käyttämällä tuoretta sisäänrakennettua kaavauskoodia, joka ei perustu Chromiumiin, Firefoxiin (Gecko) tai Safariin (WebKit).

Tämä on mahdollisesti uskomattoman jännittävä projekti, mutta tällä hetkellä on aivan liian aikaista tietää, näkeekö se edes päivänvaloa, puhumattakaan todellisen haasteen nykyiselle status quolle. Loppujen lopuksi Firefox on olemassa nyt, on erittäin hyvä ja kypsä ja hyvin tuettu selain. Mutta se on aina kohdannut ylämäkeä kilpailemaan pelkän vaurauden, monopolistisen markkinointivoiman ja globaalin valta-aseman kanssa Googlen ja Applen selainten takana. On mParhaat selaimet yksityisyydellesi vuonna 2025



Lopulliset ajatukset

Kaikki yllä luetellut selaimet ovat hyväksi yksityisyydelle. Heillä on jokaisella erilaisia etuja ja haittoja, jotka vetoavat eri ihmisten prioriteetteihin selaimen valinnassa, joten emme ole listanneet niitä missään tiettyssä järjestyksessä. Kehotamme sinua kokeilemaan niitä kaikkia nähdäksesi, mikä niistä sopii sinulle parhaiten.

On myös avoimen lähdekoodin luonne, että on olemassa lukuisia vähemmän tunnettuja selaimia (lähes kaikki haarukoitu joko Firefoxista tai Chromiumista). Näitä ovat muun muassa [GNU Icecat \(englanniksi\)\(uusi ikkuna\)](#), [SeaMonkey-ohjelma\(uusi ikkuna\)](#), [Iridiumia\(uusi ikkuna\)](#), [Kalpea Kuu\(uusi ikkuna\)](#), [Waterfox-yhtiö\(uusi ikkuna\)](#), ja muut, joilla on pieniä mutta (epäilemättä ansaitusti) uskollisia fanijoukkoja.

Vaikka niitä kaikkia ei ole voitu tutkia yksityiskohtaisesti täällä, kannustamme kaikkia, jotka ovat kiinnostuneita tästä aiheesta, tutkimaan kaikkia käytettävissä olevia vaihtoehtoja.

Se, miten käytämme internetiä, on suurelta osin [kourallisen yhdysvaltalaisen](#) teknologiajättien - Google, Apple, Microsoft, Amazon ja Meta, erityisesti muokkaama. Vaikka ne saattavat tehdä elämästä helpompaa, tällä mukavuudella on hintansa: yksityisyytesi. Heidän sovelluksensa keräävät valtavia määriä henkilötietoja, käyttämällä niitä algoritmien tarkentamiseen, mainosten kohdentamiseen ja tarvittaessa jopa [näiden tietojen jakamiseen hallitusten ja lainvalvontaviranomaisten kanssa](#).

[Ulkomaantiedustelun valvontalain \(FISA\) 702 §: n](#) kaltaiset lait antavat Yhdysvaltain hallitukselle mahdollisuuden vaatia pääsyä yksityisiin tietoihisi tietämättäsi ja ilman lupaa - riippumatta siitä, asutko Yhdysvalloissa vai et. Jokainen viesti, haku ja tallennettu tiedosto yhdysvaltalaisella alustalla on [järjestelmässä, joka on suunniteltu tarkkailemaan, luokittelemaan ja joskus luovuttamaan tietosi](#) helposti viranomaisille. Ja koska massavalvonta ei ole keskustelun aiheena, kysymys ei ole enää siitä, kerätäänkö tietojasi, vaan kuka niitä valvoo.

On kuitenkin olemassa työkaluja, joiden avulla voit ottaa takaisin tämän hallinnan. Jos haluat käyttää internetiä luopumatta arkaluonteisimmista, arvokkaimmista tiedoistasi, monet eurooppalaiset palvelut tarjoavat tietosuojavaihtoehdon.

Aloitetaan joistakin omistamme. Perustimme Protonin Sveitsissä vuonna 2014 vastustaaksemme erityisesti yhdysvaltalaisen teknologiayritysten suorittamaa massavalvontaa ja henkilötietojen väärinkäyttöä. Ratkaisumme oli sijoittaa [päästä päähän -salaus](#) kaiken toimintamme ytimeen – salaamalla tietosi avulla ohjaamillasi avaimilla, muilla kuin sinulla ja ihmisillä, joiden kanssa kommunikoit, ei koskaan ole pääsyä yksityisiin tietoihisi.

- [Proton Mail](#) (Gmail vaihtoehto)
- [Proton Drive](#) (Google Drive vaihtoehto)
- [Proton Docs](#) (Google Docs -vaihtoehto)
- [Proton Pass](#) (Google Password Manager vaihtoehto)
- [Protonikalenteri](#) (Google-kalenterin vaihtoehto)
- [Proton VPN:n\(uusi ikkuna\)](#) (VPN-vaihtoehto yhdysvaltalaisille palveluille)

Big Techin ulottuvuus ulottuu kuitenkin kaikkiin elämän osa-alueisiin verkossa. Jos haluat täysin paeta Yhdysvaltojen valvontaverkkoa, tässä on joitain tietosuojaystävällisiä eurooppalaisia vaihtoehtoja eri kategorioissa.

Yksityisyyteen keskittyvät eurooppalaiset vaihtoehdot

Hakukoneet

Google seuraa hakujasi ja luo sinulle laajan profiilin. Kokeile sen sijaan näitä eurooppalaisia palveluita:

- [Qwantissa\(uusi ikkuna\)](#) (Ranska): Tietosuoja edellä hakukone, joka ei seuraa käyttäjiä; perustuu tällä hetkellä Bing, [Qwant ja Ecosia\(uusi ikkuna\)](#) ovat lyöttäytyneet yhteen eurooppalaisen hakuindeksin rakentamiseksi
- [Ekosia\(uusi ikkuna\)](#) (Saksa): Yksityisyyteen keskittyvä hakukone, joka rahoittaa puiden istutusta mainostuloilla
- [Mojeek-elokuva\(uusi ikkuna\)](#) (Yhdistynyt kuningaskunta): Riippumaton hakuindeksi, jossa on tiukat tietosuojakäytännöt

Verkkoselaimet

Chrome on tunnettu [selauskäyttäytymisen seuranta\(uusi ikkuna\)](#). Vaihda näihin vaihtoehtoihin:

- [Vivaldi\(uusi ikkuna\)](#) (Norja): Mukautettava selain, jossa on vahvat tietosuojaominaisuudet
- [LibreWolf-Susi\(uusi ikkuna\)](#) (EU): Firefox-pohjainen selain, joka keskittyy turvallisuuteen ja yksityisyyteen
- [Waterfox-yhtiö\(uusi ikkuna\)](#) (Iso-Britannia): Poistaa Firefoxin telemetrian ja seurannan

Viestisovellukset

WhatsApp (Metan omistama) kerää metatietoja jokaisesta lähettämästäsi viestistä. Harkitse:

- [Kolmivuotias\(uusi ikkuna\)](#) (Sveitsi): Päästä päähän salattu, metatietoja minimoiva chat
- [Ovidin\(uusi ikkuna\)](#) (Ranska): Puhelinnumeroa ei tarvita, erittäin turvallinen
- [Istunto\(uusi ikkuna\)](#) (EU): Hajautettu, anonymi keskustelu
- [Delta\(uusi ikkuna\)](#) [Chat-keskustelu\(uusi ikkuna\)](#) (EU): Käyttää tavallista sähköpostia salattuun viestiin
- [Elementti \(Matrix\)\(uusi ikkuna\)](#) (EU): Avoimen lähdekoodin, liittoutunut viestintä
- [Lanka\(uusi ikkuna\)](#) (Sveitsi): Turvallinen, päästä päähän salattu viesti henkilökohtaiseen ja yrityskäyttöön

Navigointi ja kartat

Google Maps kerää valtavia määriä sijaintitietoja. Voit kokeilla sen sijaan:

- [Osm Ja\(uusi ikkuna\)](#) (EU): Avoimen lähdekoodin kartat, joissa on offline-navigointi
- [Orgaaniset kartat\(uusi ikkuna\)](#) (EU): Ei seuranta, akun käyttö on vähäistä
- [Taika Maa\(uusi ikkuna\)](#) (Alankomaat): Tekoälyllä toimivat kartat ilman tiedonkeruuta
- [TÄÄLLÄ WeGo\(uusi ikkuna\)](#) (Saksa): Google Mapsin suuri kilpailija

Webhotelli

Siirrä verkkosivustosi tai palvelimesi tietosuojaystävälliseen isäntään:

- [OVHcloud-yhdiste\(uusi ikkuna\)](#) (Ranska): Suuri EU-isäntä, jolla on useita pilvi- ja palvelinvaihtoehtoja
- [Infomaniak-sivusto\(uusi ikkuna\)](#) (Sveitsi): Sveitsiläinen isännöinti, jolla on vahva yksityisyyden suoja
- [Hetzneriä\(uusi ikkuna\)](#) (Saksa): Edullinen, suorituskykyinen isännöinti EU:ssa

Lisää eurooppalaisia vaihtoehtoja yhdysvaltalaisille teknologiajäteille

Niille, jotka haluavat vähentää täysin riippuvuutta amerikkalaisesta teknologiasta, tässä on muita eurooppalaisia vaihtoehtoja eri kategorioissa:

Suoratoisto ja media

- [Deezeriä\(uusi ikkuna\)](#) (Ranska): Vaihtoehto Apple Musicille
- [Luokka: Qobuz\(uusi ikkuna\)](#) (Ranska): Korkean resoluution musiikin suoratoisto
- [SoundCloud-Pelti\(uusi ikkuna\)](#) (Saksa): Itsenäinen taiteilija-alusta
- [Spotifyssa\(uusi ikkuna\)](#) (Ruotsi): Suosittu musiikin suoratoistoalusta, jolla on massiivinen maailmanlaajuinen luettelo
- [PeerTube-Puot\(uusi ikkuna\)](#) (EU): Hajautettu YouTube-vaihtoehto
- [DailyMotion-ohjelma\(uusi ikkuna\)](#) (Ranska): YouTube-kilpailija, jolla on yksityisyyspainotteinen

Muistiinpanon tekeminen

- [Vakiomuistiinpanot\(uusi ikkuna\)](#) (Sveitsi): Salattu muistiinpanovaihtoehto Google Docsille
- [Kryptotyynty\(uusi ikkuna\)](#) (Ranska): Turvallinen, yhteistyöhön perustuva Google Docs -vaihtoehto

Sosiaalinen media

- [Mastodon\(uusi ikkuna\)](#) (Saksa): Hajautettu vaihtoehto Twitter/X:lle
- [Lemmy\(uusi ikkuna\)](#) (EU): Federated Reddit-tyylinen alusta
- [Ystävällinen\(uusi ikkuna\)](#) (EU): Vaihtoehto Facebookille

Käännöspalvelut

- [DeepL:n\(uusi ikkuna\)](#) (Saksa): Korkealaatuinen käännösvaihtoehto Google Translatelle
- [Reverso-\(uusi ikkuna\)](#) (Ranska): tekoälyllä toimiva käännöstyökalu
- [ModerniMT\(uusi ikkuna\)](#) (Italia): Yritystason käännöspalvelu

Videopuhelut ja neuvottelut

- [Jitsiä\(uusi ikkuna\)](#) (EU): Avoimen lähdekoodin Google Meet -vaihtoehto
- [- Miksi\(uusi ikkuna\)](#) (Norja): Yksityisyyteen keskittyvät videoneuvottelut

Käyttöjärjestelmät

- [/e/ OS\(uusi ikkuna\)](#) (Ranska): DeGoogled Android -vaihtoehto

- [SailfishOS:n\(uusi ikkuna\)](#) (Suomi): Turvallinen mobiilikäyttöjärjestelmä
- [Ubuntu\(uusi ikkuna\)](#) (Iso-Britannia): Suosittu Linux-pohjainen työpöytäkäyttöjärjestelmä
- [Linux-rahapaja\(uusi ikkuna\)](#) (EU): Windows/Mac-vaihtoehto

Kehittäjätyökalut

- [Codebergiä\(uusi ikkuna\)](#) (EU): Vaihtoehto GitHubille
- [JetBrains-tuotteet\(uusi ikkuna\)](#) (Tšekki): IDE-kilpailija Visual Studiolla
- [SonarQube-yhtiö\(uusi ikkuna\)](#) (Sveitsi): Koodin analysointityökalut

Suunnittelutyökalut

- [Tehosekoitin\(uusi ikkuna\)](#) (Alankomaat): Ilmainen, avoimen lähdekoodin 3D-animaatiotyökalu, jota käytetään luomaan [Flow, latvialainen elokuva, joka voitti Disneyn Oscar-gaalassa](#)
- [Affiniteetti\(uusi ikkuna\)](#) (Iso-Britannia): Vaihtoehto Adobe-työkaluille
- [Luonnos\(uusi ikkuna\)](#) (Alankomaat): Vaihtoehto Figmalle

Ota takaisin hallinta

Kun hallitukset laajentavat ulottuvuuttaan, usein Big Techin avulla, elämämme hallinta verkossa on vaarassa luisua pois. Mutta et ole voimaton. Voit silti valita palveluita, jotka asettavat yksityisyyden etusijalle – missä viestejä, tiedostoja ja henkilötietoja ei kerätä, tallenneta tai jaeta.

Proton [sijaitsee Sveitsissä](#), jossa vahvat tietosuojalait pitävät tietosi massavalvonnan ulottumattomissa. Pysyt aina hallinnassa. Ja koska palvelumme käyttävät [päästä päähän -salausta](#), edes me emme pääse käsiksi sähköposteihisi, tiedostoihisi, salasanoihisi tai kalenteriisi – vain sinä voit.

Mutta yksityisyyden suojaaminen ylittää sähköpostin ja tallennuksen. Hakukoneista viestisovelluksiin, selaimista pilvitallennukseen, muut eurooppalaiset vaihtoehdot voivat antaa sinulle työkalut hallinnan takaisin.

Yksityisyytesi palauttaminen ei tarkoita yhteyden katkaisemista tai piiloutumista. Se tarkoittaa [teknologian käyttöä yoursinun](#) ja pelkästään sinun [your](#)ehdoillasi. Se tarkoittaa sitä, että valitset sinua kunnioittavia palveluita. Ja se alkaa astumalla järjestelmän ulkopuolelle, joka hyötyy katsomalla sinua ja sellaiseen, joka [on rakennettu kanssasi tärkeimpänä prioriteettina](#).