

EFF tippek a magánszféra védelme és az online biztonság érdekében

PCLinuxOS Magazine 2025. november

Az EFF (Electronic Frontier Foundation) a számítógép-használók jogainak védelmével foglalkozó szervezet a honlapján októberben közzé tett egy a hónap végéig [naponta bővített listát](#) olyan ajánlásokkal, amik erősíthetik az online biztonságodat és önvédelmedet. Az írás méretei és összetettsége miatt rövidítve és kissé átdolgozva tesszük közzé. *(Megjegyzés: az ajánlások október 17-ig megjelent részét a PCLinuxOS Magazine is leközölte)*

Az eredeti, folyamatosan bővített írás [itt tekinthető](#) meg. Szerzői: [Thorin Klosowski](#), [Lena Cohen](#), [Christian Romero](#), [Hayley Tsukayama](#), [Bill Budington](#), [Rindala Alajaji](#), Yael Grauer, és [Paige Collings](#)

1. tipp: teremts jó digitális higiéniát:

- [használd jelszókezelőt](#);
- minden fiókhoz [eltérő jelszót \(és azonosítót\)](#) legyen;
- [kétfaktoros azonosítást](#) használj.

(Ajánlott forrás: [Surveillance Self-Defense](#) útmutató jelszókezelő és kétfaktoros azonosítás bekapcsolására.)

2. tipp: ismerd meg, hogy az Adatbrókerek mit tudnak rólad

Bizonyos államokban törvény kötelezi az adatbrókereket, hogy a rólad gyűjtött adatokat adják ki neked. Kérd ki és tanulmányozd.

(Megjegyzés: hazánkban kötelező érvényű szabályozás nincs, csak ajánlás.)

3. tipp: iPhone-on és Androidon kapcsold ki a hirdetéskövetést

Telefon- és operációs rendszerfüggő, hogy hol találsz, de tiltsd le a követést (tracking), a hirdetések személyre szabását (personalized ads) és a hirdetési azonosítót (advertising ID).

Pl. Androidon nézd meg a Google fiókodban (account), milyen információkat osztanak meg a Google-alkalmazások másokkal. *Kulcsszavak: Web & App Activity settings; personalized ads; YouTube share.*

Határozd meg, hogy milyen adatokat mentsen (back up) a rendszer automatikusan.

Kapcsold be a fokozott védelmet (Advanced Protection). Stb.

Alaposan nézd át a lehetőségeket a telefonodon!

(Források: [iPhone](#); és [Android](#) telefonra, illetve az EFF-féle [Surveillance Self-Defense](#) útmutató.)

4. tipp: selejtezd az alkalmazásaidat

(Ajánlott oldalak: [iPhone-ra](#); [Androidra](#).)

5. tipp: az Amazonon kapcsold ki az ajánló hirdetéseket

Az Amazon jelentős mennyiségű adatot gyűjt és tárol a vásárlási szokásaidról. Ha itt kell, vagy szoktál vásárolni legalább csökkentsd az adatgyűjtés mértékét. Jelentkezz be az Amazon-fiókodba és

- Keresd az Advertising Preferences-t és nézd át.

EFF tippek a magánszféra védelme és az online biztonság érdekében

- Ha van Amazon-féle Alexa eszközöd, kapcsold ki a hangfelvételt és az adathasználat-követés (data usage tracking) egyes elemeit.
- Ha van Ring (csengőbe épített) kamerád, fontold meg a végpontok közötti titkosítás bekapcsolását.

6. tipp: telepítsd a Privacy Badger-t az online-követés blokkolására

A [Privacy Badger](#), az EFF (Electronic Frontier Foundation) ingyenes böngésző kiterjesztése, ami blokkolja a követést és folyamatosan fejlesztve küzd a változó követési eljárások ellen. Ha Privacy Badger egyes oldalak megjelenítését lehetetlenné teszi, akkor [kapcsold ki](#) ideiglenesen,

7. tipp: vizsgáld felül a tartózkodási hely követése beállításokat

Az olyan alkalmazások, amiknél a helymeghatározás bekapcsolt, a helyadataidat folyamatosan továbbíthatják adatkereskedőknek, vagy ha hirdetési felületet adtak el, a felületre licitáló összes részvevőnek. Javasolt – a telefon beállításainál – átnézni az egyes alkalmazások hozzáférési engedélyeit és kikapcsolni a helyadatok elérését. Emellett, a 3. tippben javasolt hirdetési azonosító (ad ID) kikapcsolása is célszerű. Továbbá, a telefon repülőgép üzemmódba helyezése is kikapcsolja a nyomkövetést.

(Ajánlott oldalak: [iPhone-ra](#); [Androidra](#).)

8. tipp: korlátozd a játékkonzolod adatgyűjtését

A játékkonzolok figyelik a játékkal kapcsolatos szokásaid. Amit érdemes megtenni, hogy először is ellenőrizd a kétfaktoros azonosítás (2FA) bekapcsolt voltát. Ezután ellenőrizd az adatvédelmi beállításokat. (A cikk [Playstation 5](#), [Xbox XJS](#) és [Nintendo Switch](#) konzolokra leírja a teendőket.)

9. tipp: a Strava útvonaladon a kiinduló- és végpontot rejtse el

A kültéri szabadidős sportokat űzők egyik közkedvelt útvonalmegosztó és nyomkövető alkalmazása a [Strava](#), amit online le lehet olvasni. A helyadatok érzékeny információk. A kiinduló- és végpontból a lakóhely beazonosítható. (2018-ban a szabadidejünkben sportoló katonák adatai alapján titkos katonai bázisok elhelyezkedésére derült fény.)

A végpontok elrejtésének módja

- weblapon: a profilképedre állva → **Settings** → **Privacy Contorls** (adatvédelem) → **Map Visibility** (térkép láthatósága)
- mobil alkalmazásban: **Settings** → **Privacy Contorls** → **Map Visibility**.
- Egyenként is szerkeszthetőek az útvonalak: a „...” menü megnyitása → **Edit Map Visibilty**. Itt részleteiben is, de egészében is letiltható a láthatóság **„Hide the Entire Map”**.

10. tipp: keresd meg és töröld a már nem használt fiókokat

Töröld a már nem használt fiókjaidat. A korábban megosztott személyes adataiddal is visszaélhetnek, csökkentsd a kockázatot! A jelszókezelőből töröld! A böngészőben keress rá a „password”, „welcome to”, vagy „confirm your email” a mentett bejegyzésekre!

A [„HaveBeenPwned”](#) weblapon rákereshetsz azokra az oldalakra, ahol a személyes adataid kiszivárogtak és nézd meg, van-e olyan, amit már nem használsz. További információk a Security Planner [„Delete Unused Accounts tip”](#) részben olvashatóak.

EFF tippek a magánszféra védelme és az online biztonság érdekében

11. tipp: keress rá magadra (nevedre)

Ellenőrizd a neten rólad elérhető információkat úgy, hogy beírod a nevedet a keresőbe. Ha valamelyik oldal olyan adatokat oszt meg rólad, amit nem szántál a nyilvánosságnak, intézkedj. ([Töröld a fiókodat](#), kérd meg az oldal üzemeltetőit az adataid eltávolítására stb.)

12. tipp: töröldesd a személykereső oldalakkal az információkat rólad

Személykereső oldalakon töröldesd az adataidat. Van egy [összesítő lista](#) azokról helyekről, ahol a személyes adataidat tárolhatják, kiegészítve a törléssel kapcsolatos információkkal. Három céget emel ki az [Intelius-t](#), ([törlési űrlap](#)) [Spokeo](#) ([törlési űrlap](#)) és [BeenVerified](#). Utóbbinál [ingatlanra](#) is lehet keresni. Az egyes szolgáltatóknak saját eljárása van a keresőből törlésre, van ahol csak fizetség fejében teszik.

13. tipp: töröldesd a lakcímedet a keresőmotorokból

Gyakran előfordul, hogy a lakcímedet pár kattintással elő lehet hívni. A törlést kezddheted a Google keresőjével. Van egy [külön oldal](#) erre, ami leírja a teendőket (angolul). Lényege, hogy a „[results-about-you](#)”-ra kattintva végigvezet a tennivalókon (**ez már magyarul van**).

14. tipp: próbáld ki a Signal-t

A [Signal](#) végpontok közötti titkosított üzenetváltást tesz lehetővé. Emellett WiFi segítségével lehetővé teszi az ingyen üzenetküldést és fogadást, illetve telefonálást. A Signal kipróbálásának menete, hogy letöltöd a telefonra az applikációt. Ellenőrzöd a telefonszámodat és beállítasz egy biztonsági PIN-kódot és már használhatod is. [Leírás itt](#) olvasható.

15. tipp: válts a magánszférát védő böngészőre

A böngészők rengeteg személyes információt tárolnak, amiket a cégek a hirdetések személyre szabására használhatnak. A böngészőválasztás meghatározza, hogy mennyire lehet a követést kizárni. A Google Chrome és Safari böngészője jelentősen korlátozzák az adatvédelmet. Pl. a [Chrome Incognito](#) módban csak elrejt az előzményeket, de a követést nem kapcsolja ki. A Safari a törölt [előzményeket is megőrzi](#), illetve a [privát](#) böngészésben is gyűjti az adatokat.

A [Firefox](#) a privát módban automatikusan blokkolja a követést és hirdetéseket, illetve figyelmeztet, ha személyes adataidat próbálnák letölteni. Van még pár személyes adatok védelmére fókuszáló böngésző, mint a [DuckDuckGo](#), a [Brave](#) és a [Tor](#).

16. tipp: készíts alternatív online személyiségeket

Az online megjelenés különböző területeinek elkülönítése megakadályozhatja, hogy személyedről az adathalászok teljes képet alkothassanak. Pl. a hivatali és a magánélet, a gyerekek iskolai dolgai és a hagyományos, személytel terhelt levelezés szétválasztható eltérő e-mail-címek, telefonszámok, vagy fiókok használatával.

17. tipp: ellenőrizd le a virtuális kártya szolgáltatókat

Próbáld ki a virtuális kártya-szolgáltatásokat. A bankkártya internetes használata veszélyes lehet nemcsak a hamis kereskedelmi oldalak miatt, hanem az elavult, feltörhető egyen e-kereskedelmi szoftvert használó cégek miatt is. A bankkártyaadatok elrejtethetők virtuális kártya mögé, amik esetén nemcsak a tranzakciók száma (eseti, vagy

EFF tippek a magánszféra védelme és az online biztonság érdekében

rendszeres használat), hanem a típusa (pl. ruhavásárlás) és az összeghatár is meghatározható. Természetesen a szolgáltatás nem ingyenes, ezért érdemes alaposan megvizsgálni a lehetőségeket figyelve az esetleges plusz költségeket. Ilyen szolgáltatók pl. a [Privacy.com](#), illetve a [IronVest](#). A használatnak lehetnek regionális, országokra vonatkozó korlátai az eltérő pénzügyi rendelkezések, törvények miatt.

(Megjegyzés: [összefoglaló](#) a Magyarországon elérhető virtuális kártyáról, illetve tanácsok használatukhoz.)

A PCLinuxOS Magazine – lapzártá miatt – csak a 17. tippig hozta le a cikket, de az EFF a hónap végéig további javaslatokkal egészítette ki az ajánlásait.

18. tipp: digitális fizetési alkalmazások kockázatcsökkentése

A digitális fizetési alkalmazások, mint a Cash App, Venmo és Zeller védelme gyengébb, mint a hagyományos bankkártyáké. Ha lehet inkább a normál bankkártyát használd. Ha mégsem, akkor

- kapcsold be a tranzakció figyelmeztetést;
- Azonnal jelezd a szolgáltatónak, ha ismeretlen tranzakció történt, bármennyire is kis összegre. Egyrészt, az lehet egy teszt a nagyobb levonás előtt, másrészt a szolgáltatók garanciája időkorlátos. A PayPal és Venmo 60 napon belül jelzett visszaélésre nyújt fedezetet, de a Cash App csak 48 órányira.

És persze kapcsold be a [többfaktoros azonosítást](#). [Javaslatok](#) a mobil használatához érintésmentes fizetésre.

19. tipp: kapcsold ki a hirdetések személyre szabását

A [technológiai óriások](#) tonnaszámra [gyűjtik](#) az online és azon kívüli tevékenységünk adatait és árulják bárkinek, aki fizet érte, bármire is használja fel azokat. Kapcsold ki a hirdetések személyre szabását, hogy elkerüld ezt.

[Meta](#) (Facebook és Instagram): **Profilkép → Beállítások és adatvédelem → Adatvédelmi központ → Adatvédelmi beállítások ellenőrzése.** Ez új oldalra visz, itt a **személyes hirdetési beállításaid** ...

[Google](#): menj el [erre a weblapra](#), lépj be a fiókodba → és jobbra fent a **Személyre szabott hirdetések** opciót váltsd **Ki** állásra.

[X](#) (korábban Twitter): látogass el [erre az oldalra](#) és a **Data sharing and personalization** alatt mindent kapcsolj ki.

Továbbiakat [itt olvashatsz](#).

20. tipp: szigoríts a fiókjaid biztonsági beállításain

Néhány nagyobb cég esetén a teendőkről a hivatkozásoknál:

[Apple](#), [Discord](#), [Facebook](#), [Google](#), [Instagram](#), [LinkedIn](#), [Microsoft](#), [Snapchat](#), [TikTok](#), [Twitch](#), [Venmo](#), [WhatsApp](#), [X](#), [YouTube](#)

21. tipp: adatvédelem online randizás során

A randi alkalmazások, mint a Grindr és a Tinder jelentős mennyiségű intim információt gyűjtenek. Rossz kezekbe kerülésük beláthatatlan következményekkel járhat. Tippek az önvédelemhez:

EFF tippek a magánszféra védelme és az online biztonság érdekében

1. ellenőrizd a bejelentkezési információidat – legyen erős, egyedi jelszavad és kapcsold be a kétfaktoros azonosítást;
2. kapcsold ki személyre szabott hirdetést;
3. ellenőrizd a lakhelyedhez és a kameramozgathoz hozzáférés elérhetőségét;
4. gondosan válaszd meg a megosztott fényképeidet;
5. kapcsold ki a külső applikációk integrálását (pl. Spotify);
6. válogasd meg miről társalogsz (különösen az első kapcsolatfelvételnél). Például **ne ossz meg pénzügyi információkat és higgy a megérzésednek**.

22. tipp: a TV-n kapcsold ki az ACR-t (Automatic Content Recognition)

Az Internetre kötött TV-k egyik opciója az ACR – automatikus tartalomfelismerés, ami képernyőképeket készít és azokat egy adatbázissal összevetve elemzi, hogy miket nézel a TV-n. Felmérések [szerint egyes TV-k](#) óránként akár 7200 képet is csinálnak. Természetesen eladásra, célzott hirdetések készítése céljából. Ez aggályos lehet különösen, amikor külső adathordozón tárol anyagokat (képek, Blue-Ray, DVD stb.) böngészünk.

Nem biztos, hogy könnyű az ACR kikapcsolása, de [Consumer Reports útmutatója](#) segíthet nagyobb gyártók esetében.