Az Ősvaló honlappal és tanácsadási tevékenységemmel kapcsolatos adatvédelmi tájékoztatás mellett fontosnak tartom, hogy a személyes adataid (születési adatok, életesemények, ingatlanok részletei) biztonságosan juthassanak el hozzám, és az elkészített kiértékelések írásos anyagát is biztonságosan juttathassam el hozzád. Éppen ezért bevezettem néhány alapvető biztonsági irányelvet az adatcserét illetően:

1. **Facebook Messenger**en a lehető legkevesebb kommunikációt folytatok. Tanácsolom, hogy te is kerüld ezt a csatornát minden olyan esetben, amikor az üzeneted személyes jellegű, és nem a nyilvánosságnak szánod. Ez a csatorna ugyanis alapértelmezetten nem titkosított, így bárki belenézhet, ha ért hozzá. Biztonságos és felhasználóbarát csevegőalkalmazás: Signal (telefonálni is lehet vele)
2. **Nem biztonságos**nak tartott csatornákon – Facebook, a legtöbb email-rendszer – csak olyan üzeneteket váltok, amiknél nem baj, ha nyilvánosságra kerülnek (nem feltétlenül lesz így, de benne van a kockázat).
3. **Titkosításra** van lehetőség számos levelezőrendszerben (pl. Gmail, Yahoo, Hotmail stb.; sőt, akár biztonsági kulcs, lejárati idő is alkalmazható, mely eltávolítja a továbbküldési és letöltési gombokat, letiltja a másolhatóságot – vagyis csak olvasni engedi az üzenetet, jelszavak küldésére remek út).

   Ám ettől még illetéktelenek hozzáférhetnek érzékeny személyes adataidhoz (pl. a Gmail csak akkor titkosít, ha a másik fél is használ titkosítást, nem pedig végponttól végpontig; minden Gmailes biztonsági kulcsot a Google állít elő, nem te; illetve a Google köztudottan nyomon követi minden egyes tevékenységed, levelezéseid, hangparancsaid, helyzeted, keresési és böngészési történeted, vásárlási szokásaidat, használt készüléked adatait, YouTube használatodat stb.).
4. **Biztonsági okokból** létrehoztam hát az osvalo@protonmail.com fiókot, ahova védett módon küldheted személyes adataidat. Javaslom neked is az ingyenes a fiókot. Kényelmesebb is, bemutatom miért:

Előnyök

- ingyenes és könnyen használható, akárcsak más online postafiók
- szokványos levélküldésen túl titkosítva is lehet küldeni az adatokat (levelek, csatolmányok), így sokkal kisebb az esélye annak, hogy bárki illetéktelen tudomására jut azok tartalma
  - legbiztonságosabb és legkényelmesebb, ha *mindkét félnek protonmail fiókja van*
  - biztonságos *nem protonmailes fiókba* küldött üzenet is: jelszó és PGP gondoskodik a titkosításról, digitális aláírás szavatolja a küldő hitelességét. Ez jelentősebb odafigyelést, hozzáértést, több kattintást és lépést kíván mindkét fél részéről, mint két ProtonMail fiók közötti üzenetváltás (ahol maga a fiók intézi helyettünk az összetett eljárást), de megbízható.
- minden levelezést (akármilyen forrásból is érkezett) titkosítottan tárol, amit csak te, a levelezőfiók felhasználója tudsz feloldani, amikor belépsz a fiókodba – ezzel szemben a Gmail
- titkosított a névjegyzéke is, így levelezőtársaid adatait is védetten kezeli
- az adatok *még a ProtonMail csapata számára sem hozzáférhetők*, hiszen a feloldáshoz szükséges kulcsot csak a felhasználó birtokolja – ennek megfelelően azt a vállalat hatósági felszólításra sem tudja kiadni az adatokat harmadik feleknek, csak a visszafejthetetlenül titkosított adatokat.
- lehetőség van kétfaktoros autentikáció (2FA) érvénybe léptetésére, vagyis arra, hogy a jelszón kívül egy hatjegyű kód is szükséges legyen a belépéshez (amit a kevésbé biztonságos SMS helyett egy mobiltelefonos alkalmazás állít elő számodra minden egyes bejelentkezési alkalommal) – tehát ha az egyiket el is lopnák, a másik nélkül nem mennek sokra vele
- nem követi nyomon szokásaidat, nem küld reklámokat vagy biztonsági értesítőnek álcázott adatgyűjtő kéréseket, ha a megszokottól eltérő készülékről jelentkeztél be – cserébe a saját védett fiókodban tartja nyilván a bejelentkezéseidet (akár IP-címmel együtt is)

Hátrányok

- ha elveszíted a jelszavad, a tárolt információkhoz sem jutsz többé hozzá
- jelszó visszaállításnál az összes korábbi levelezés olvashatatlanná válik (mivel változik a titkosítás) – bár ha később eszedbe jutna, ezeket is feloldhatod
- az ingyenes változat egyelőre 500 MB tárhelyet biztosít és napi 150 levél küldését teszi lehetővé

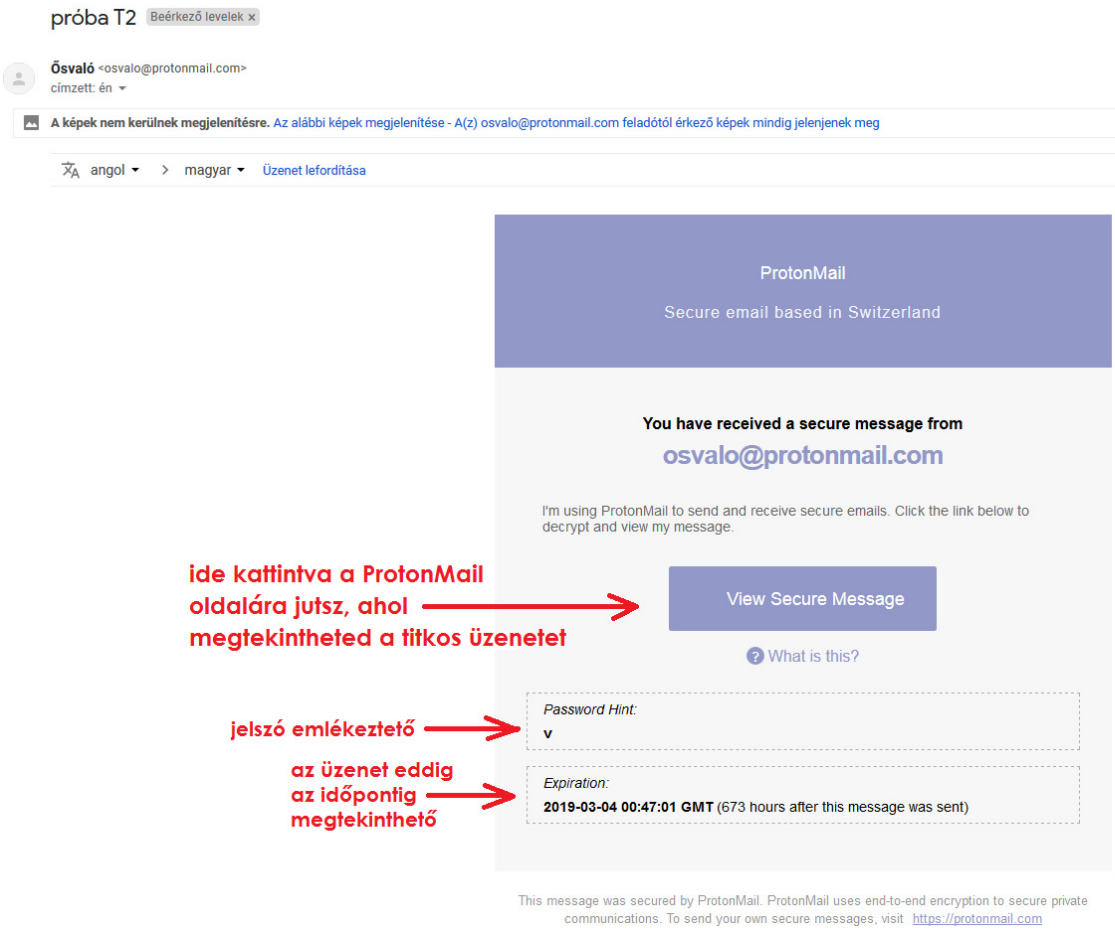
Ajánlott ismertetők magyar nyelven:

- https://index.hu/tech/2016/03/31/biztonsagos_email_protonmail/
- https://index.hu/szolgalati-kozlemeny/2018/08/02/index_titkositott_uzenetek_informator_signal_protonmail/
- https://www.hwsw.hu/hirek/58113/protonmail-titkositott-email-biztonsag.html
- https://maganelet.hu/
- Glenn Greenwald: Miért fontos a magánélet? (TED-előadás)

Milyen az, amikor Te fogadsz védett tartalmú üzenetet tőlem

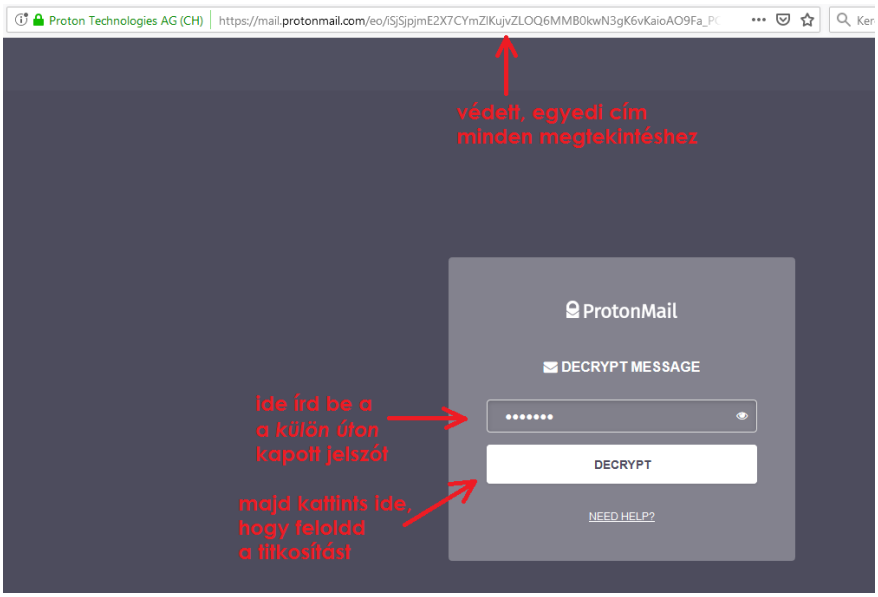
a) nem ProtonMail fiókba

Valami ilyesmi tartalmú emailt kapsz (a bemutatóhoz egy GMail-es fiókot használtam):

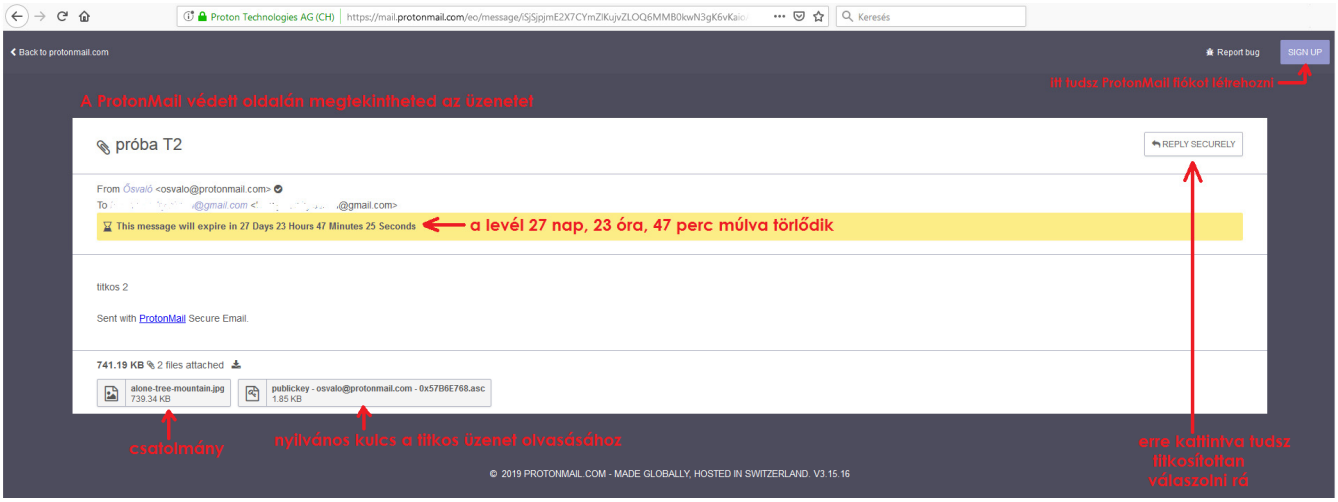


Hogy megtekinthesd a védett tartalmat, egy védett oldalra irányít a levélben szereplő gomb. A következő oldalakon bemutatom, hogyan teheted olvashatóvá a titkosított üzeneteket, csatolmányokat.

1. lépés: a titkosítás feloldása jelszóval, melyet biztonsági okokból egy *másik csatornán* keresztül juttatok el neked, így ha levelezési fiókodhoz illetéktelenek férnének is hozzá, a jelszóval nem tudják összekapcsolni.



2. lépés: a levél elolvasása, csatolmányok letöltése (erre megadott idő, kb. *1 hónap* áll rendelkezésre),



3. lépés:

titkosított válasz küldése, melléklet csatolása

(kép esetén két lehetőség is van: *As an attachment* = csatolmányként; *Inline* = beillesztett képként)

Egyszerű és biztonságos.

b) ProtonMail fiókba

A rendszer magától gondoskodik róla, hogy az üzenet végponttól végpontig, azaz teljes úton védettséget élvezzen (end-to-end encryption), a feladótól a címzettig titkosítva van.

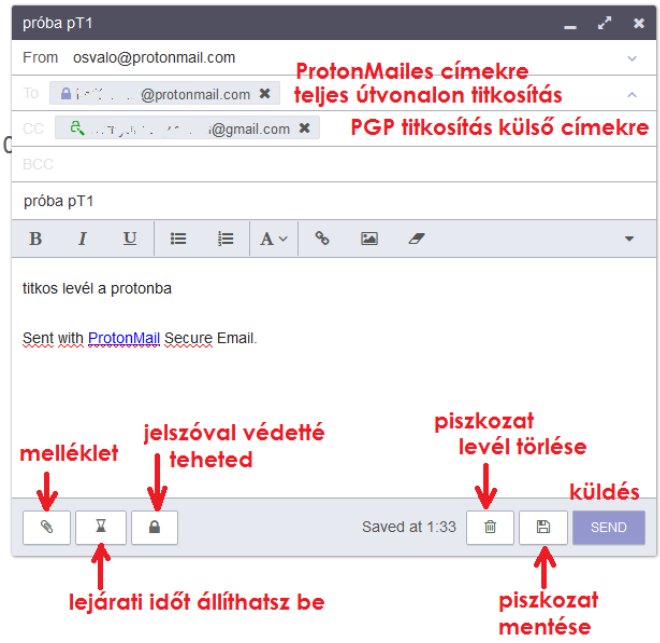
Milyen az, amikor Te küldesz védett tartalmú üzenetet nekem

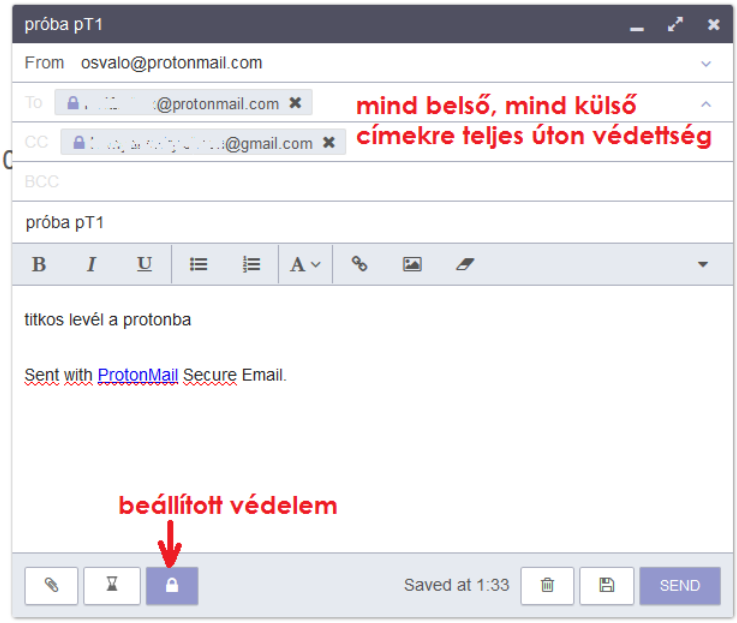
a) nem ProtonMail fiókból

Ehhez saját megoldás szükséges, nincs általános irányelv, ajánlott biztonságtechnikai szakértelem is hozzá. A lényeg, hogy az üzenet *megfelelően* titkosítva legyen és én el tudjam olvasni.

b) ProtonMail fiókból

Akár Protonmail címre, akár más, „külső" címre szánod az üzenetet, lehetőséged van védetté tenni. Az előbbi esetről gondoskodik maga a ProtonMail rendszer, az utóbbi ráadás – de egyszerű – beállítást igényel.





Továbbá hangsúlyozom: nem tárolok a levelezőrendszerben személyes adatokat tartalmazó leveleket, csatolmányokat – tehát a protonmail fiókomból is törlöm az első adandó alkalommal, eleget téve az európai uniós GDPR és a magyar Infotv. hatályos adatkezelési rendelkezéseinek.

Ez a szemlélet természetesen nem azt jelenti, hogy kerülendő a Facebook Messenger és minden nem Protonmail levelezőrendszer használata – csak meggondolandó, milyen adatokat közölsz rajtuk keresztül, a saját érdeked és *mindenki más érintett* érdekében.

Bízom benne, hogy ez a bemutató – az alapvető biztonsági irányelvek tudatosítása mellett – elősegíti a tudatos életvezetésedet, hiszen éberségre és figyelmességre nevel saját személyes adataidat, szokásaidat, választásaidat illetően.

Írta: Hornyánszky Simon, 2019. február 4. a Föld-Disznó napév hajnalán :)