CTI Jelentés

# Tanácsok a biztonságosabb Facebook és közösségimédia-használathoz

1996
Fortes fortuna adiuvat
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

KiberPajzs
Védelem a pénzügyekben

# Tartalomjegyzék


Bevezetés 4

Online fiókok elleni támadások 5

- Hogyan jelenthetem, hogy ellopták a fiókomat? 6
- „Miért pont én lennék célpontban?!" 8
- Hogyan szerezhet egy hacker hozzáférést a Facebook fiókokhoz? 10

Első lépés: A legalapvetőbb fiókvédelemi beállítások 11

- Mitől lesz „erős" egy jelszó? 11
- Mi az a kétfaktoros hitelesítés? 12
  - Így aktiválhatjuk a kétfaktoros hitelesítést a Facebookon 14
  - Értesítések kérése az ismeretlen bejelentkezésekről 21

Második lépés: Csökkentsük a támadási felületet! 23

- Hogyan találhatnak meg mások, és hogyan léphetnek velünk kapcsolatba a Facebookon? 23
- Ki láthatja a tevékenységeinket? 24
- Alkalmazások és engedélyek 25
- Hirdetéskezelési beállítások a Facebookon 25

Harmadik lépés: Használjuk biztonságtudatosan! 28

- A leggyakoribb csalástípusok ma a Facebookon 29
  - Nyereményjátékok, ajándékok 29
  - Hamis termékek 30


- Romantikus átverések 30
- Befektetési csalások 32
- Hitelcsalások: 32
- Álláshirdetéses csalások: 33
- Hozzáférésikód-lopások: 34
- Csalások a Facebook Marketplace-en 34
- Az aktuális „forró téma” 35

Általános biztonsági tanácsok: 36

Online zaklatás 38

- Tiltások kezelése 38
- Tájékozódás és álhírek a közösségi médiában 39
- Moderálás a Facebookon 42

# Bevezetés

A közösségi oldalakon záporozó posztok, kommentek, felvillanó hirdetések a másodperc töredéke alatt annyiféle ingert és érzelmet képesek kiváltani – izgalom, kíváncsiság, meglepetés, öröm, izgalom, empátia, harag –, hogy hajlamosak vagyunk teljesen belefeledkezni a virtuális létbe. Ez az önfeledtség azonban magában hordozhatja az óvatlanságot, amivel a rosszindulatú felhasználók és a csalók könnyen visszaélhetnek és kárt okozhatnak nekünk.

A számtalan közösségi platform közül — Instagram, TikTok, Snapchat, Twitter, LinkedIn, YouTube, hogy csupán a legnagyobb neveket említsük — azért a Facebookot helyeztük e tájékoztató középpontjába, mert ma a felhasználók számát és a felhasználás sokszínűségét – szabadidős szórakozás, kapcsolattartás, hírfogyasztás, és kereskedés – tekintve ez a legnépszerűbb közösségi platform a magyar lakosság körében.

A lakosság biztonságtudatos közösségimédia-használatának támogatása érdekében bemutatjuk a Facebookon elérhető fontosabb adatvédelmi és fiókbiztonsági beállításokat — fókuszban a kétfaktoros hitelesítéssel és a hitelesítőalkalmazásokkal — és tanácsokat adunk a közösségi oldalon előforduló leggyakoribb csalási formák és más valós veszélyek felismeréséhez és elkerüléséhez.

Az összefoglaló 2023 februárjában készült.

# Online fiókok elleni támadások

Az Identity Theft Resource Center 2022-es felmérése megdöbbentő képet fest a közösségi fiókok elleni támadásokról: 2021-hez képest 1000%-kal nőtt globálisan a fiókfeltöréses esetek száma. A megkérdezettek Instagram fiókjának 85%-át, Facebook fiókjának 25%-át törték fel, ráadásul az áldozatok 70%-a többé sosem fért hozzá a profiljához. A támadók az esetek többségében hónapokon át használták az áldozat profilját, miközben annak ismerőseit is megpróbálták átveri.

Az Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézethez is gyakran érkezik olyan lakossági bejelentés, amiben a felhasználók kétségbeesve kérnek segítséget, mert valaki kizárta őket a Facebook fiókjukból.

A tapasztalatok szerint egy ilyen támadás az áldozatokat mindig komoly érzelmi sokként éri, azonban kollégáinknak — legjobb szándékuk ellenére — nincs érdemi lehetősége segíteni. Az érintett egyetlen esélye, hogy jelenti a Facebook Help Center felületén, hogy a fiókját illetéktelenek használják. Azzal azonban érdemes számolni, hogy hetek vagy akár hónapok is eltelhetnek, mire választ kapunk a kérésünkre, és arra sincs garancia, hogy végül visszakapjuk a fiókunkat.

*Az amerikai The Wall Street Journal napilap is foglalkozott azzal, hogy miért ennyire nehéz felvenni a kapcsolatot a Facebookkal. A lap arra jutott, hogy a Facebook tulajdonos Meta — dacára annak, hogy a felhasználók száma globálisan a 3 milliárdot közelíti — eddig nem rendelkezett hagyományos értelemben vett, például telefonon is elérhető, valódi ügyfélszolgálattal. A felhasználók igényét azonban a Meta is felismerhette, mert a nemrég bejelentett havidíjas szolgáltatás részeként már az ügyfélszolgálathoz való direkt kapcsolatot is ígér a cég.*

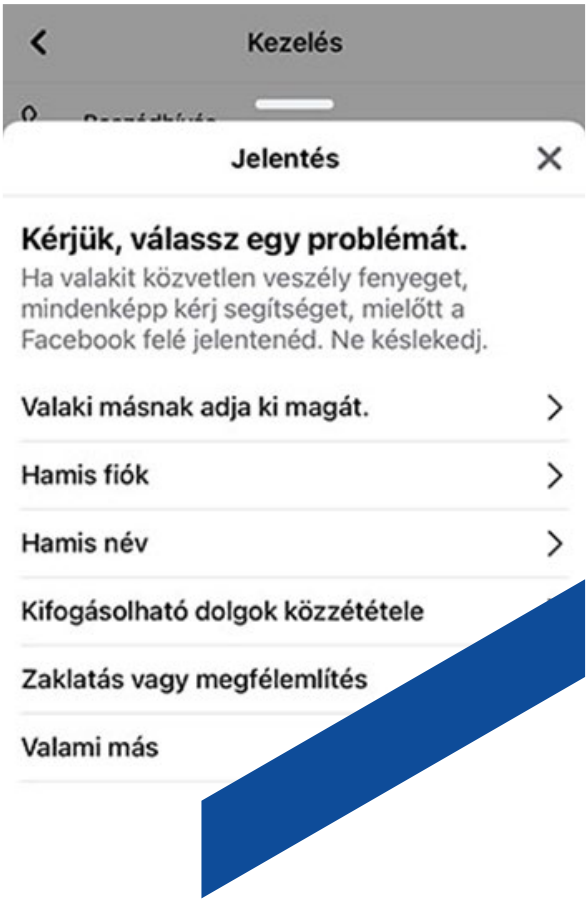
# Hogyan jelenthetem, hogy ellopták a fiókomat?

Ha valakit kizártak a Facebook fiókjából, azt jelezheti a platform moderátorainak például ezen az űrlapon vagy a Facebook súgóközpontján keresztül.

Ilyenkor be kell bizonyítanunk, hogy mi vagyunk a fiók valódi tulajdonosa, ezért javasolt, hogy ugyanarról az eszközről és arról az Internet hálózatról – például otthonról – jelezzük a fiókfeltörést, mint amiről egyébként is Facebookozni szoktunk. A Meta ugyanis a különböző rögzített technikai azonosítók (például IP cím) alapján így könnyebben tudja megállapítani, hogy ez valóban a mi fiókunk.

Ilyen helyzetben érdemes az ismerősöknek is jelezni, hogy a fiókot feltörték, illetve segítséget is kérhetünk, hogy az alábbiak szerint jelentsék a fiókot:

- Nyissák meg a feltört fiók profilját!
- Kattintsanak a borítóképen szereplő ikonra, és válasszák ki a „Jelentem" lehetőséget, majd kövessék a képernyőn megjelenő utasításokat!




Segítség kérése feltört fiók setén

Gyakran az ismerősök már akkor jelzik, hogy valami nincs rendben a fiókkal, amikor mi még észre sem vettük, hogy baj történt. Például olyan posztokra vagy üzenetekre hívják fel a figyelmünket, amelyeket valaki a profilunkhoz hozzáférve, a tudtunkon kívül küldött. Előfordulhat az is, hogy kapunk egy zsaroló e-mailt, amiben azt állítja a feladó, hogy hozzáfért a fiókunkhoz. Ez legtöbbször csak blöff és a csaló egy korábban kiszivárgott jelszavunkat küldte el e-mailben. Az ilyen megkeresésekre nem javasolt válaszolni, azonban cseréljünk jelszót minden olyan szolgáltatásnál, ahol az érintett jelszót valaha is használtuk!

# “Miért pont én lennék a célpont?!”

A legtöbben azt gondolják, hogy egy hacker számára nem jelentenek vonzó célpontot. Fontos tudni, hogy egy online fiók elleni támadás a legtöbb esetben nem személyes indíttatású. Ez szigorúan üzlet.

A hackerek számára a különböző online fiókok különböző értékkel bírnak, például egy PayPal fiók az online feketepiacokon legtöbbször drágább, mint egy meghackelt közösségi account, azonban általánosságban azt mondhatjuk, hogy mindegyikre van kereslet. Előbbivel direkt anyagi kárt okozhatnak, egy feltört Facebook fiók pedig tökéletesen alkalmas vírusos tartalmú üzenetek terjesztésére, illetve adathalászatra.

A kiberbűnözők a legtöbbször arra is felhasználják a feltört fiókokat, hogy általuk a csaló hirdetések elérését növeljék lájkolással, megosztással.

Fokozott veszélynek vannak kitéve a nagy követői bázissal rendelkező közszereplők, influenszerek, cégvezetők Facebook — és Instagram — fiókjai. Az ilyen, sokszor hosszú évek munkájával felépített közösségi profilok és oldalak csábító célpontot jelentenek a támadóknak, a feltört fiókjaik ugyanis jó zsarolási alapot jelentenek, vagy álhírek terjesztésre is felhasználhatóak.

*Az influenszerek fiókjai elleni támadásra jó példa, hogy 2022-ben Magyarország legismertebb, videójátékok streamelésével népszerűvé váló TheVR csapatának két YouTube csatornáját is feltörték. A hírek szerint a támadó privátra állította a csatornákon megosztott videókat, megváltoztatta a csatornák neveit, és egy hamis Patreon hivatkozást tett közzé.*


A TheVR egyik tagjának vonatkozó Twitter bejegyzése

Érdemes külön megemlíteni azokat a csalókat is, akik kifejezetten az üzleti fiókokat veszik célba, azért, hogy az áldozat számlájára — a fiókokban beállított fizetési adatokkal — hirdetéseket adjanak fel. Egy ilyen kiberbűnözői kör ellen a Facebook például 2021 decemberében már jogi lépéseket is tett, az általuk okozott pénzügyi kár a 16 millió dollárt is meghaladta.

# Hogyan szerezhet egy hacker hozzáférést a Facebook fiókokhoz?

Számos módon, ám leggyakrabban:

- Adathalász üzenetekkel. Valójában a támadóknak a legegyszerűbb „elkérni" a jelszót az áldozattól. Persze ezt nem nyíltan teszik, hanem például a Facebook nevében küldött adathalász e-mailekkel.
- Kiszivárgott hitelesítőadatokkal. Manapság – egy kis túlzással – szinte minden napra jut egy hír arról, hogy hackerek feltörték valamely szolgáltatót, majd az ellopott adatokat kiszivárogtatták, legtöbbször egy internetes feketepiacon. A veszélyt itt az jelenti, hogy sokan ugyanazzal az e-mail címmel regisztrálnak több online szolgáltatásba, és ugyanazt a jelszót több helyen is használják.
- Ha túl gyenge jelszóval védett a fiókunk. A gyenge jelszavak kitalálhatóak. A hackerek tisztában vannak a tipikus jelszavakkal. Szomorú, de Magyarországon 2022-ben a legnépszerűbb jelszó az „123456" volt.
- Szoftveres sérülékenységeket kihasználva. Természetesen a kifejezetten a Facebookot érintő lehetséges szoftveres sérülékenységeket, biztonsági incidenseket is meg kell említenünk.

# Első lépés: A legalapvetőbb fiókvédelemi beállítások

A közösségi fiók elleni támadások kivédéséhez kettő dolgot egyszerűen nem kerülhetünk meg, és ez bármely számunkra fontos online fiókra, például az e-mailekre is érvényes:

1. Egy erős, egyedi jelszó beállítását,
2. A kétfaktoros hitelesítés aktiválását.

## Mitől lesz "erős" egy jelszó?


Az erős jelszó nehezen kitalálható. Ez alatt egy kicsit bővebben azt értjük, hogy

- legalább 10-12 karakter hosszú;
- szerepel benne szám és speciális karakter is (pld.: $&@) is – ami lehetőleg ne a jelszó végére kerüljön;
- nem tartalmaz egyszerű sorozatokat vagy ismétlődéseket, mint például: 123456789, 111222333
- nem tartalmaz személyünkhöz köthető információkat, amelyek esetleg könnyen hozzáférhetők lehetnek mások számára – tehát például születési évszámot, becenevet, sem a háziállatunk nevét, amiről vélhetően gyakran posztolunk;
- egyedi, azaz lehetőleg egyetlen fióknál van beállítva – így, ha nyilvánosságra kerülne, akkor sem sodorja veszélybe a további szolgáltatások biztonságát.


- *Érdemes figyelni az NBSZ NKI kiberbiztonsági elemzéseit, mert a jelszavak témájában önálló tájékoztatóval is készülünk.*
- *Az egyedi jelszavak esetében inkább a mennyiséggel van probléma. Erre egy jelszókezelő program használatát javasoljuk. A megfelelő program kiválasztásához egy korábbi segédletünk nyújthat segítséget.*

# Mi az a kétfaktoros hitelesítés?


A kétfaktoros hitelesítés (2 factor authentication – 2FA) az online fiókoknál azt jelenti, hogy a jelszó beírása után **még egy hitelesítési lépés következik**, meg kell adnunk egy egyszer használatos kódot is.

Extra védelmet ez azért jelent, mert ha valaki a nevünkben szeretne bejelentkezni a fiókba, nem elég kitalálnia vagy megszereznie a jelszavunkat, hanem erre a 2FA kódra is szüksége lesz. Ennek a megszerzése általában olyan sok erőforrást igényelne a támadótól – pl. a telefonunk és a hitelesítő alkalmazás feltörése –, hogy az egyszerűen **„nem éri meg a fáradságot" a támadó számára**.

Aki manapság netbankol vagy bankkártyával vásárol online, valójában már ismeri a kétfaktoros hitelesítés lényegét, hiszen ugyanarról van szó, mint a 2019-ben bevezetett erős ügyfélhitelesítés, ami a netbankos belépéseknél és a bankkártyás fizetéseknél már a hétköznapjaink részévé vált.

A bankszámla védelmének fontosságát senki sem vitatja, azonban sajnos kevesen érzik úgy, hogy a többlépcsős hitelesítésre más online szolgáltatásoknál is szükség van.

A problémát a tech ipar is felismerte, és az olyan óriáscégek, mint például a Google és a Microsoft, azon dolgoznak, hogy a biztonságos hitelesítés minél egyszerűbb és kényelmesebb legyen. A megoldást valószínűleg a **jelszavak teljes kiváltása** fogja eredményezni az olyan technológiák segítségével, mint belépőkulcsok (passkeys). A belépőkulcsok lényege, hogy amikor fiókot hozunk létre egy weboldalon, jelszó beállítása helyett egy mobileszközt fogunk regisztrálni, ekkor a készülék eltárol egy egyedi technikai azonosítót.

Amikor ezt követően be szeretnénk jelentkezni az adott fiókba, a készülék ezt az azonosítót el fogja küldeni weboldalnak, ám előtte még ujjlenyomat vagy arcfelismerés útján ellenőrizni fogja, hogy valóban a készülék tulajdonosa próbál bejelentkezni.

Habár ez már a közeli jövőben elérhetővé válhat, addig továbbra is kétfaktoros hitelesítés alkalmazását javasoljuk minden olyan online szolgáltatásnál, ami erre lehetőséget biztosít.

## Így aktiválhatjuk a kétfaktoros hitelesítést a Facebookon


A Facebook háromféle 2FA üzemmódot támogat:

- Biztonsági kulcs – Egy különálló fizikai eszköz segítségével jelentkezünk be a fiókba.
- Hitelesítő alkalmazás – A telefonra letölthető applikációk, amelyek biztonsági kódokat generálnak, amit a Facebookos bejelentkezésnél a jelszó beírása után kell megadni.
- SMS – Itt is kódot adunk meg, azonban ez SMS-ben érkezik a profilban beállított telefonszámra.

Először ejtsünk néhány szót a legbiztonságosabbnak tekintett megoldásról, a hardveres biztonsági kulcsokról. Ennek használatát elsősorban közszereplők, influenszerek, és mindazok számára ajánljuk, akik kiemelten veszélyeztetve érzik online fiókjaik biztonságát, részükre egy FIDOU2F vagy az újabb FIDO2 tanúsítvánnyal rendelkező hardverkulcs termék választását javasoljuk. Ezek a termékek nem ingyenesek, azonban NFC-kompatibilis (Near-field communication) eszközökkel használhatóak. Számos ilyen termék érhető el, a legismertebb gyártó a Yubico.

Hardverkulcs termékek Forrás: The Verge

Ebben az útmutatóban a hitelesítőalkalmazások beállítását mutatjuk be. Az SMS-ben kapott kódoknál ez ugyanis biztonságosabb megoldás, ami mindenki számára elérhető. Az SMS hitelesítő kódok egyik nagy hátránya, hogy például SIM kártya csalással egy támadó eltérítheti az SMS-ben kapott kódokat. Ezt elkerülhetjük, ha olyan alkalmazást választunk, amihez nem kell telefonszámot regisztrálni.

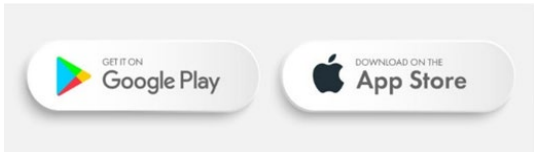
Fontos tisztázni, hogy 100 százalékos biztonság nem létezik, még hitelesítő alkalmazásokat használva sem. Nemrég például a népszerű Authy alkalmazás esetében történt biztonsági incidens. Hackerek megszerezték a cég egy alkalmazottjának belépési adatait, azzal pedig hozzáfértek az Authy anyacégének (Twilio) informatikai rendszereihez. Az Authy tájékoztatásából tudjuk, hogy a bűnözők forráskódok mellett összesen 93 Authy ügyfél adatait is megszerezték, ezután pedig saját eszközeiket beregisztrálták az áldozatok online Authy fiókjába, így elméletileg hozzáférhettek a kétfaktoros belépőkódokhoz is. A cég gyorsan reagált, tájékoztatta ügyfeleit a teendőkről és arra a beállításra is felhívta a figyelmet, amivel egy ilyen támadás kivédhető.

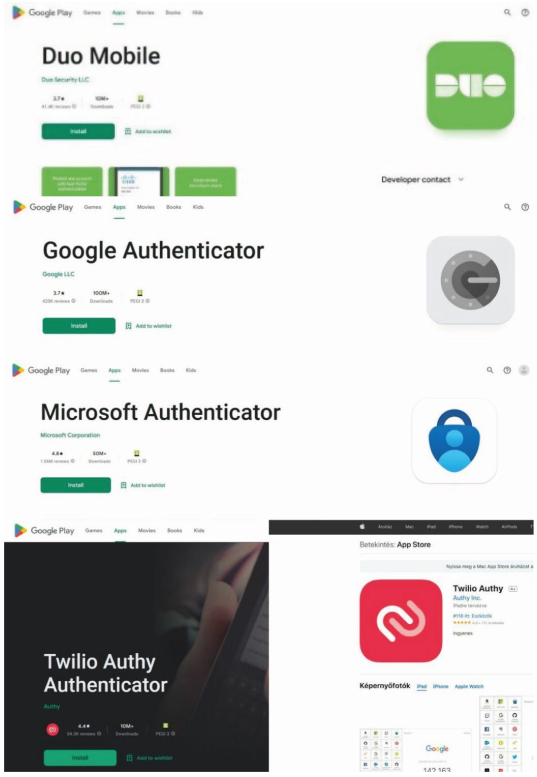
## Hitelesítő alkalmazás letöltése

A Facebook több terméket is támogat, így például használhatjuk a legismertebb, erre a célra szolgáló ingyenes appokat:

- a Microsoft Authenticatort,
- a Google Authenticatort,
- a Twilio Authy-t,
- vagy a Duo Mobile-t.

A kiválasztott appot kizárólag hivatalos alkalmazásboltból (Google Play Store, App Store) töltsük le!




A választáshoz tisztában kell lennünk azzal, hogy az elérhető funkciók között léteznek különbségek, ilyen például az online biztonsági mentés (backup) kérdése. Érdemes az alábbi kérdésekre választ keresni:

- **Lehetséges-e az alkalmazással biztonsági mentést készíteni a belépőkódokról, és az hol kerül tárolásra?**

A funkció fontossága abban mutatkozik meg, hogy segítségével a telefon elvesztése esetén könnyen át tudunk állni egy másik készülékre. Elméletileg, ha a telefonról van biztonsági mentésünk – számítógépen vagy felhőtárhelyen – az átálláskor a 2FA alkalmazás is működni fog, azonban, ha szeretnénk biztosra menni, ez egy szempont lehet a választás során. (Az Authy, a Duo Mobile, a Microsoft Authenticator például nyújt ilyen funkciót, a Google Authenticator azonban nem.)

- **Hány eszközön szeretnénk elérni az alkalmazást?**

A legtöbben egyetlen eszközt, a telefonjukat használják erre a célra, de létezik olyan alkalmazás (pl. az Authy), amivel több eszköz (pl. laptop, tablet, stb.) között is megoszthatjuk a kódokat.

- **Hány online accounthoz szeretnénk használni a Facebookon kívül?**

Ha idővel több fiókhoz is használnánk – e-mail cím(ek), közösségi oldalak, stb –, érdemes lehet olyan szolgáltatást választani, ami többféle szolgáltatással is kompatibilis.

- **Kell-e telefonszámot megadni regisztrációkor?**

Ezt, ha lehet, kerüljük, mert egyrészt nyitva hagyja a lehetőséget a fentebb már említett SIM kártya csalások előtt, másrészt egyébként is tanácsos a telefonszámot a lehető legkevesebb szolgáltatásnál megadni. A fenti listából egyedül az Authy kér telefonszámot, ám ennek megadása megkerülhető.

Bármelyik applikáció mellett is tesszük le a voksunkat arra mindig figyeljünk oda, hogy az alkalmazás mindig megkapja a legújabb frissítést, vagyis az

## automatikus alkalmazás-frissítés legyen bekapcsolva!

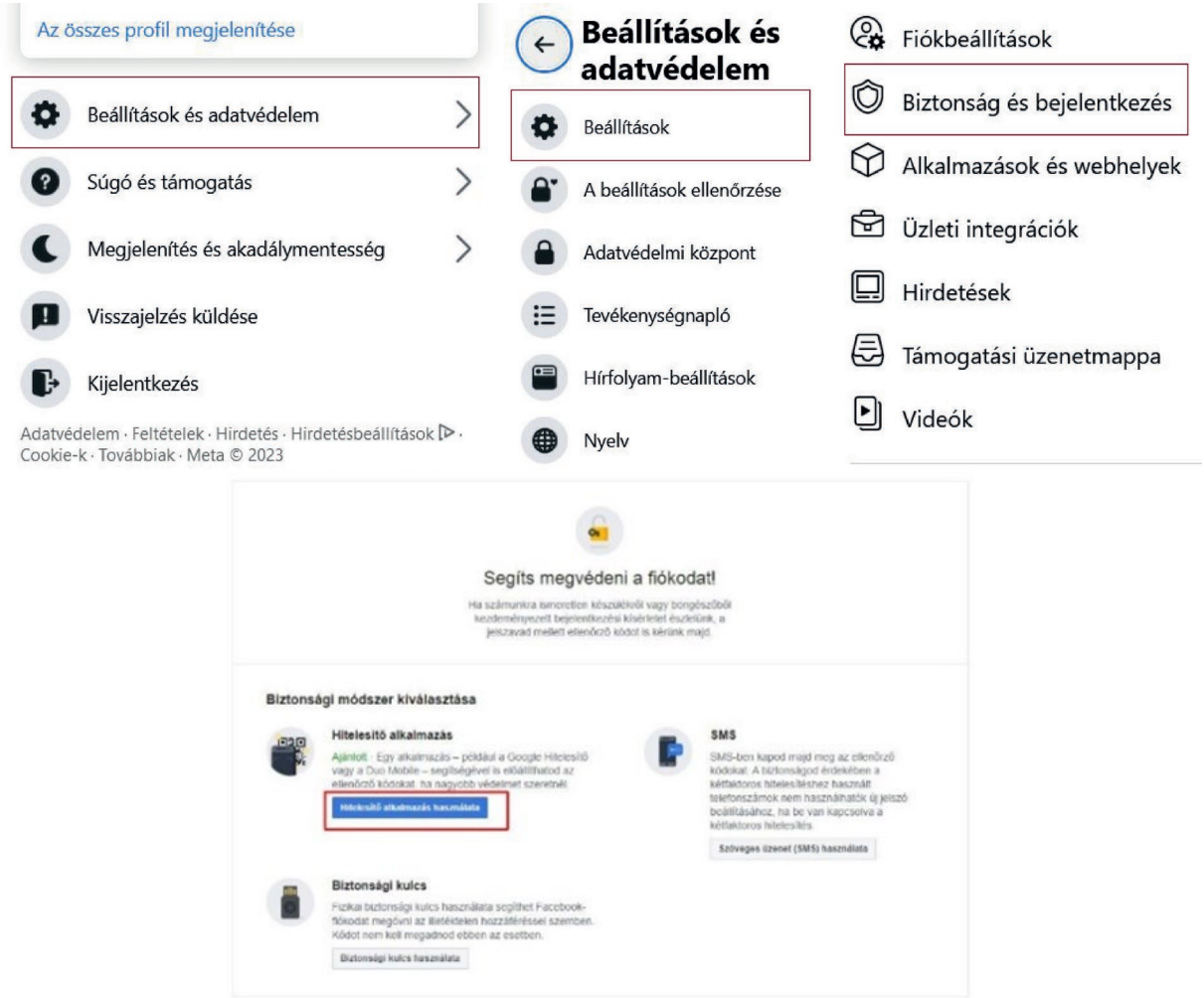
Miért fontos ez? A szoftverekben gyakorta fordulnak elő szoftveres hibák.

Az összefoglaló elkészítése idején került publikálásra a hír, miszerint egy biztonsági kutató olyan biztonsági hibát talált, ami az Instagrammal összekötött Facebook fiókok esetében lehetővé tehette a kétfaktoros hitelesítés kikapcsolását. A Meta azóta javította a hibát, azonban a felhasználóknak frissíteniük kellett a hitelesítőalkalmazásaikat.

## A kétfaktoros hitelesítés bekapcsolása a Facebook profilban

A következő lépés, hogy a 2FA beállítást aktiváljuk a Facebook profilban, amit asztali alkalmazásban itt érhetünk el:

Kattintsunk a profilképünkre > Beállítások és adatvédelem > Beállítások > Biztonság és bejelentkezés > Kétfaktoros hitelesítés használata. > Kattintsunk / koppintsunk a „módosításra"

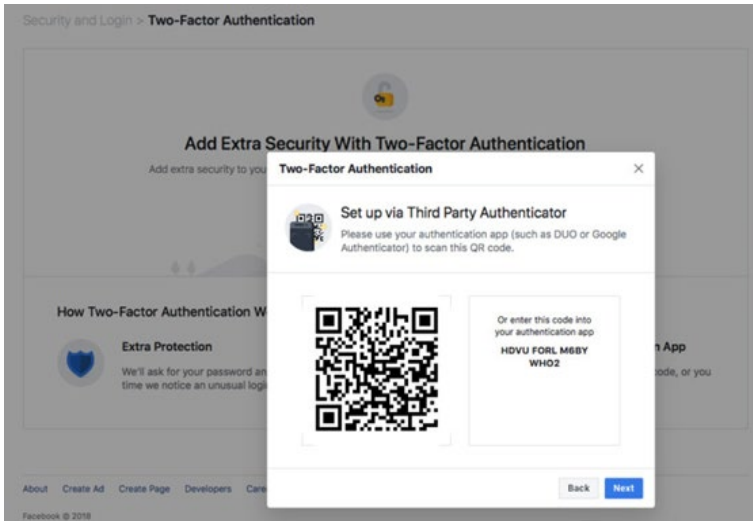



Kétfaktoros hitelesítés bekapcsolása lépésről-lépésre

## A Facebook profil és a hitelesítőalkalmazás összekapcsolása

Ebben a lépésben „kötjük össze" az alkalmazást és a Facebook szerverét. Az eljárás során egy algoritmus 30-60 másodpercenként generál egy (általában) hatjegyű, ideiglenes jelszót, amely az egyediség miatt olyan egyéb tényezőket is figyelembe vehet, mint például az aktuális napszak.

- Amennyiben számítógép előtt ülve állítjuk be a kétfaktoros hitelesítést, nyissuk meg a már letöltött hitelesítőalkalmazást a telefonunkon, és olvassuk be a Facebook felületen megjelenő QR kódot, majd adjuk meg az alkalmazás által generált kódot!
- Ha a Facebook mobil alkalmazásban állítjuk be, nem jelenik meg QR kód, helyette a hitelesítő alkalmazásból kell kimásolnunk a kódot, amit ezután be tudunk illeszteni a Facebook felületén.




Az alkalmazás innentől kezdve folyamatosan új belépőkódokat (tokeneket) generál majd, amikkel be tudunk jelentkezni a profilunkba. Ezeket a kódokat szerencsére általában csak akkor kell kézzel megadni, ha egy másik eszközön jelentkezünk be a Facebookba (pl. laptopon), a telefonos alkalmazásnál ezek a háttérben szinkronizálódnak.

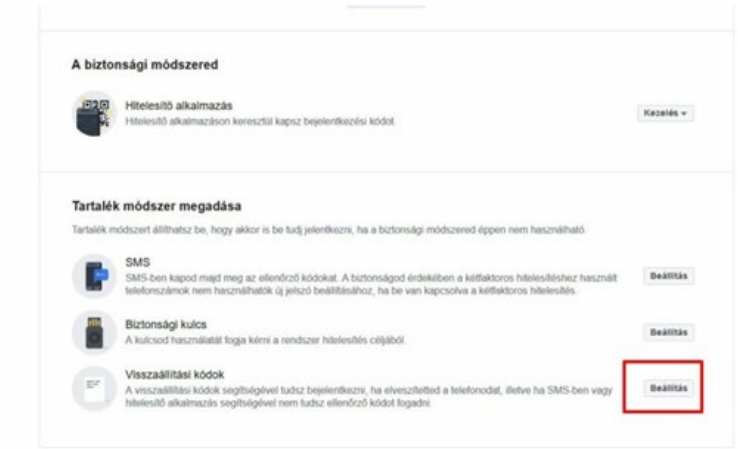
## Tartalék módszer beállítása a hitelesítőalkalmazáshoz

Miután aktiváltuk a kétfaktoros hitelesítést, csak akkor tudunk bejelentkezni a fiókba, ha a telefonunk kéznél van. Mi történik azonban akkor, ha elveszítjük a készüléket, vagy ha az megrongálódik? Erre helyzetre találták ki az ún. visszaállítási kódokat (recovery code), amelyek birtokában akkor is hozzá tudunk férni a fiókunkhoz, ha a telefonunk tönkre menne.

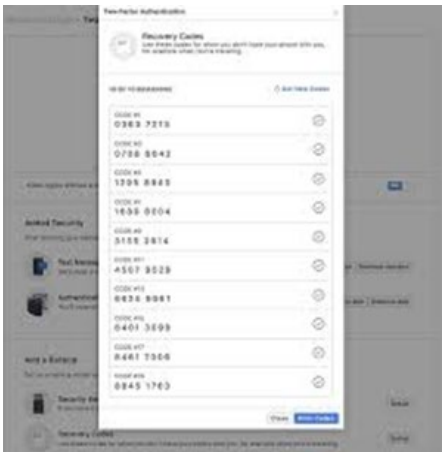
Minden alkalommal, amikor a 2FA-t aktiváljuk egy online fiókban, érdemes egyből lementeni ezeket a helyreállító kódokat, például a jelszókezelőbe vagy egy külső merevlemezre! Akár ki is nyomtathatjuk ezeket a kódokat, ám ebben az esetben tartsuk gondosan elzárva! Fontos megemlíteni, hogy minden ilyen kód egyszer használatos, de bármikor generálhatunk új helyreállítási kódokat.

A visszaállítási kódokat a Facebook profilunkban itt találjuk:

Beállítások és adatvédelem > Beállítások > Biztonság és bejelentkezés > Kétfaktoros hitelesítés használata > Visszaállítási kódok




Vissazállítási menüpont



Vissazállítási kódok

## Készítsünk biztonsági mentést a telefonról!

A biztonsági mentésekből az adataink mellett helyreállíthatjuk a hitelesítő alkalmazást is, ezért célszerű mentést végezni, például az otthoni számítógépünkre, vagy egy megbízhatónak tartott felhőtárhelyre. Így, ha elveszítenénk a telefonunkat – vagy például készüléket cserélnénk – a mentésből helyreállíthatjuk a számunkra fontos információkat egy másik készüléken.

Amennyiben olyan alkalmazást választottunk, ami rendelkezik online backup funkcióval, aktiváljuk azt is, ha ehhez jelszót, PIN kódot kell megadni, azt tároljuk biztonságos helyen!


- *A biztonsági mentésekről bővebben a SANS OUCH! hírlevélben írtunk korábban.*

## Értesítések kérése az ismeretlen bejelentkezésekről

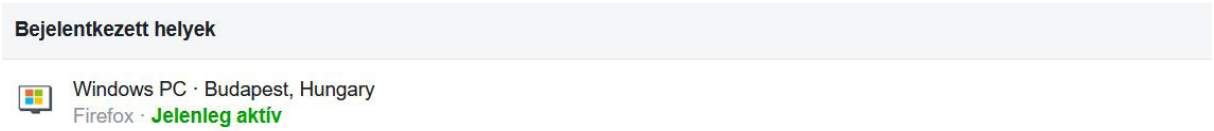

Nagyon hasznos biztonsági funkció, hogy beállíthatjuk, hogy a Facebook automatikusan értesítést küldjön, amennyiben egy új bejelentkezés történik a fiókunkban egy másik készülékről, így egyből értesülhetünk arról, ha valaki bejelentkezne a profilunkba. Ez az értesítés érkezhet e-mailben, Messenger üzenetben, vagy a Facebook applikációban.

Itt aktiválhatjuk:

Kattintsunk / koppintsunk a profilképünkre > Beállítások és adatvédelem > Beállítások > Biztonság és bejelentkezés > Kiegészítő biztonsági funkciók beállítása


Értesítések kérése az ismeretlen bejelentkezésekről menüpont

Amennyiben a Bejelentkezett helyek alatt olyan eszközt (illetve várost vagy országot) találunk, ami ismeretlen, a jobb oldali három pöttyre kattintva a lenyíló menüben kijelentkeztethetjük az adott eszközt, így, ha arról valaki be volt jelentkezve, annak azonnal megszűnik a hozzáférése. Ha ilyet tapasztalnánk, mindenképp javasolt jelszót is cserélni!




Példa egy bejelentkezett eszközre

# Második lépés: Csökkentsük a támadási felületet!

A közösségi oldalak biztonságáról szólva mindig átgondolandó kérdés, hogy mennyire engedjük meg idegeneknek, hogy kapcsolatba tudjanak lépni velünk, hiszen ezzel – bizonyos mértékig – képesek vagyunk csökkenteni annak esélyét is, hogy egy potenciális zaklató ránk találjon.

Ez is egy fontos lépés ahhoz, hogy a csalások ellen védekezzünk, ezért mindenképp érdemes megismerkedni az adatvédelmi beállításokkal, és döntést hozni a finomhangolásukról. Ezeket a profilunk alatt itt találjuk:

Kattintsunk / koppintsunk a profilképünkre > Beállítások és adatvédelem > Beállítások > Adatvédelem

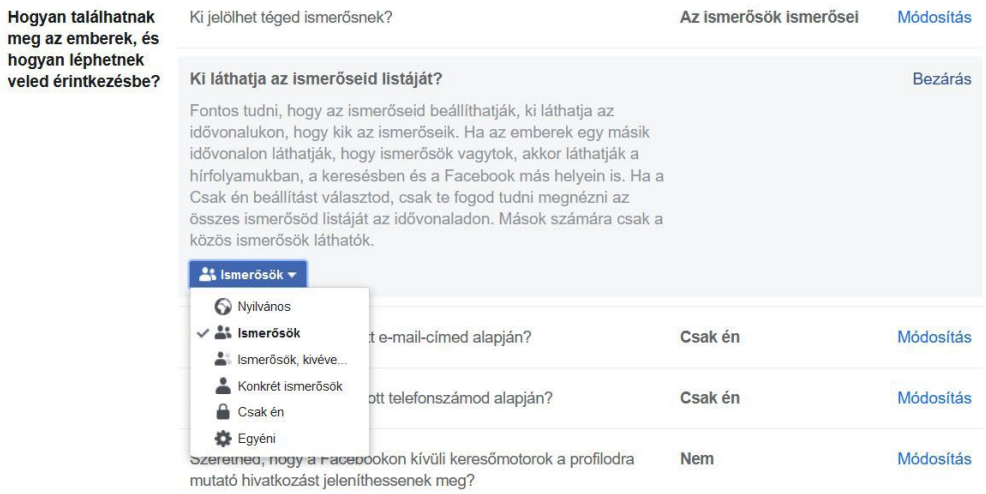
## 1. Hogyan találhatnak meg mások, és hogyan léphetnek velünk kapcsolatba a Facebookon?

Általánosságban elmondható, hogy érdemes az alábbi beállításokat bizonyos mértékig korlátozni:

- Ki jelölhet ismerősnek?
- Ki találhat meg a megadott e-mail cím alapján?
- Ki kereshet meg a megadott telefonszám alapján?
- Szeretnéd, hogy a Facebookon kívüli keresőmotorok a profilodra mutató hivatkozást jelenítsenek meg?

A beállítási szintek általában a Nyilvános (bárki számára láthatótól) – Ismerősök – Ismerősök, kivéve (kizárt ismerősök) – Konkrét ismerősök (csak a kijelölt ismerősök számára érhető el) – Csak én (teljesen privát) szintig terjednek.

Egy magánhasználatú fiók esetében érdemes lehet kikapcsolni az e-mail cím és telefonszám-alapú, valamint a Facebookon kívüli keresőmotorok (például a Google keresője) számára engedélyezett keresést, így, ha valaki ezekre az azonosítóinkra keres rá az Interneten, nem találja meg annyira könnyen a profilunkat.




Hogyan találhatnak meg az emberek és hogyan léphetnek veled érintkezésbe? menüpont

## 2. Ki láthatja a tevékenységeinket?

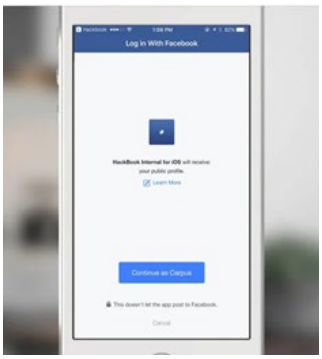
A **Saját tevékenységek** szekcióban azt tudjuk beállítani, hogy kik láthatják a bejegyzéseinket és az általunk megosztott tartalmakat.

Ez esetben is gondoljuk át, hogy meg akarunk-e osztani mindent a nagyvilággal, vagy elég, ha az ismerőseinknek van arról információja, hogy például merre voltunk nyaralni.

Ugyanitt korlátozhatjuk a **múltbeli** bejegyzések láthatóságát, illetve a tevékenységnapló segítségével átnézhetjük az összes bejegyzésünket és mások bejegyzéseit is, amelyekben minket megjelöltek. Amennyiben ezt még nem tettük volna meg, érdemes erre egy kis időt szánni, és megvizsgálni, hogy ki milyen bejegyzésben jelölt meg bennünket.


Saját tevékenységed menüpont

## 3. Alkalmazások és engedélyek




Ha egy olyan alkalmazást töltünk le, ami online regisztrációt igényel, ma már általában két lehetőség közül választhatunk, készítünk hozzá egy önálló fiókot, vagy a egy másik, például Facebook fiókkal bejelentkezve is használjuk.

A Facebookos bejelentkezés praktikus, kényelmes megoldásnak tűnik, azonban érdemes tudni, hogy amikor így jelentkezünk be egy harmadik fél által fejlesztett applikációba, az sok mindenhez hozzáférhet a Facebook profilunkban, például:

- név, felhasználónév és a felhasználói azonosító (a fiók száma);
- profilkép;
- hálózatok, amelyekhez csatlakoztunk;
- a Facebook profilban szereplő minden nyilvános információ.

Nem egy esetről tudunk, amikor egy külső alkalmazás visszaélt a begyűjtött felhasználói adatokkal, a legemlékezetesebb ilyen incidens minden bizonnyal a Cambridge Analytica 2018-ban kirobbant botránya volt. Az eset röviden: a cég egy közösségi médiában megosztott kvízzel 87 millió Facebook felhasználóról gyűjtött érzékeny profiladatokat az érintettek engedélye nélkül. Ezek az adatok azután a 2016-os amerikai elnökválasztási kampány során pszichológiai profilozásra és személyre szabott kampányhirdetések készítésére kerültek felhasználásra.

Habár a botrány hatására a Meta szigorított azon, hogy a külső alkalmazások milyen adatokhoz és milyen célból férhetnek hozzá, egy 2020-as tanulmány szerint ezt nem kényszeríti ki megfelelően. A tanulmány egy másik fontos aspektusra is rámutat, miszerint sem a végfelhasználók, sem a platformok nem képesek felmérni a különböző alkalmazások által gyűjtött adatok későbbi felhasználását, sőt ennek a kutatása sem egyszerű feladat.

A Facebookon itt ellenőrizhetjük, hogy az alkalmazások mihez férhetnek hozzá: Kattintsunk / koppintsunk a profilképünkre > Beállítások és adatvédelem > Beállítások > Alkalmazások és webhelyek


Alkalmazások és webhelyek menüpont (Kikapcsolt állapot)

## 4. Hirdetéskezelési beállítások a Facebookon

Bár nem kapcsolódik szorosan az internetes csalásokhoz, azonban érdemes a hirdetési beállításokról is ejteni néhány szót.

A Facebook tulajdonos Meta fő bevételi forrása abból származik, hogy hirdetési felületet árul. A hirdető cégek a Facebook felhasználókat különböző jellemzői alapján – például kor, nem, földrajzi helyzet – kategóriákba sorolja, és értékesíti a „reklámfelület tőzsdén". A hirdetők így célzottan olyan felhasználóknak jeleníthetnek meg reklámokat, akiket az adott termék célcsoportjának tartanak.

A Meta a Beállítások > Hirdetések > Hirdetési beállítások menüpont alatt így nyilatkozik erről:


Jó, ha tudjuk, hogy ugyanitt a korlátozhatók a hirdetések megjelenítéséhez felhasznált adatok.


A hirdetések megjelenítéséhez felhasznált adatok

A hirdetések megjelenítéséhez felhasznált adatok korlátozása nem jelenti azt, hogy nem fogunk hirdetésekkel találkozni a platformon, csupán azt, hogy az kevesebb rólunk gyűjtött adatot használhat fel ehhez a platform. Adatvédelmi szempontból ez egy mindenképp javasolt döntés.

# Harmadik lépés: Használjuk biztonságtudatosan!

Fontos tisztában lennünk azzal, hogy nincs az a biztonsági beállítás, ami megvédene bennünket, ha nem használjuk körültekintően a technológiai eszközöket, mint például a közösségi médiát.A tapasztalatok szerint ugyanakkor sokak számára éppen ez jelenti az igazi kihívást, ezért szeretnénk támpontot nyújtani a biztonságos használathoz.

Szögezzük le: természetesen nem csak a Facebookon és közösségi oldalakon vagyunk kitéve a pénzügyi csalóknak.

Ajánljuk megtekintésre az NBSZ NKI közreműködésével létrejött Kiperpajzs weboldalát, ahol a mindennapok során felmerülő, leggyakoribb csalástípusokról és az ellenük való védekezésről kaphatunk segítséget:

KiberPajzs
Védelem a pénzügyekben

Habár a közösségi oldalak igyekeznek szűrni az álprofilokat, még mindig túl könnyen lehet hamis profilt regisztrálni, illetve csaló hirdetéseket készíteni.

Az adatainkra és pénzünkre „éhes" csalók a közösségi média felületeken jelentkezhetnek ezekből a profilokból küldött üzenetben, posztban vagy hirdetésben.

A csalók szinte minden esetben ezek valamelyikére próbálnak rávenni bennünket:

- kattintsunk egy hivatkozásra
- telepítsünk egy alkalmazást
- adjunk meg valamilyen bizalmas adatot
- vásároljunk valamit
- küldjünk pénzt

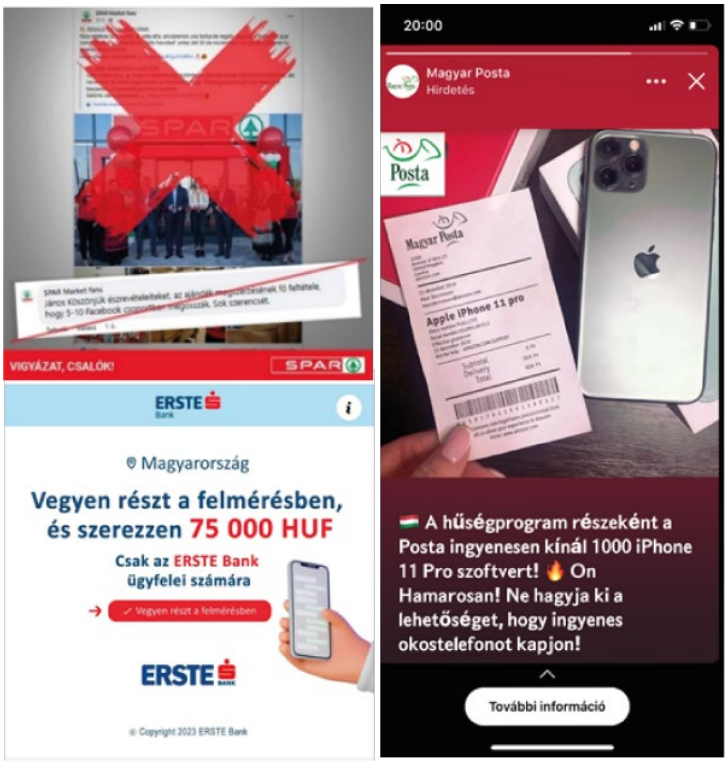
A csali pedig bármi lehet, ami felkelti az érdeklődésünket és erős érzelmeket vált ki – ezt nevezik érzelmi triggernek.

# A leggyakoribb csalástípusok ma a Facebookon

## Nyereményjátékok, ajándékok

Magyarországon is folyamatosan jelennek meg a különböző kereskedelmi cégeket, állami szerveket, bankokat megszemélyesítő álprofilok és hamis hirdetések.

- Egyszerű dolgunk van. Mindig ellenőrizzük a cég hivatalos weboldalát! Ha valós a promóció, arról kell, hogy találjunk megbízható információt.
- Ugyanígy járjunk el a felmérések, kérdőívek esetében is, amiben pénznyereményt hirdetnek! Erre jó példa a 2023 februárjában terjesztett csalás, ami az Erste bank megszemélyesítésével zajlott (lásd: 22. ábra).
- Ingyen nyereményben ne reménykedjünk, ha ilyen üzenetet látunk, biztosak lehetünk benne, hogy ez átverés.




Spar, Erste és a Magyar Posta nevével visszaélő csalások

## Hamis termékek

A közösségi média oldalakon feltűnő hirdetések esetenként hihetetlenül alacsony árakat mutatnak, és olyan weboldalakra vezetnek, amelyek első ránézésre egy jól ismert márka valódi webhelyének tűnnek, azonban ezek sok esetben hamisak.

TIPP

- *Legyünk különösen óvatosak az olyan online hirdetésekkel és ajánlatokkal, amelyek túl jónak tűnnek ahhoz, hogy igazak legyenek!*
- *Sokkal biztonságosabb olyan termékeket vásárolni, amelyek lehet, hogy egy kicsivel drágábbak, azonban elérhetőek olyan megbízható oldalakon keresztül, ahonnan mi – vagy ismerőseink – már vásároltunk.*
- *Írjuk be az online áruház nevét vagy webcímét a keresőbe, hogy megtudjuk, mit mondtak róla mások! Keressünk olyan kifejezéseket, mint például: „csalás", „átverés", „soha többé" és „hamis"!*

## Romantikus átverések

A csalók esetenként romantikus kapcsolatot kezdeményeznek, az üzenetekben gyakran elváltnak, özvegynek vagy rossz házasságban élőnek adják ki magukat. A beszélgetés előbb-utóbb arra terelődik, hogy valamilyen ürüggyel, pl. repülőjegy vagy vízum címén pénzt szerezzenek az áldozattól. A bizalmunkba szeretnének férkőzni, így hetekig folyhat a beszélgetés, mielőtt pénzt kérnének.

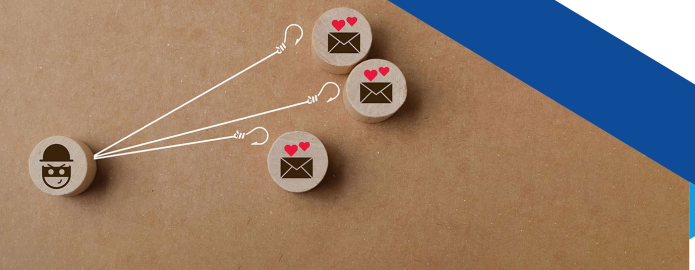
Ez egy Magyarországon is nagyon gyakori átverés típus, aminek leginkább azok kitettek, akik a közösségi oldalukon nyilvánosan megjelenítik, hogy egyedülállóak. Online ismerkedéskor platformtól függetlenül érdemes nagyon óvatosnak lenni, bármilyen társkereső portálon belefuthatunk egy ilyen csalóba.

TIPP

- *Ha bizalmas témájú üzenetváltásba kerülünk valakivel, kérjünk fotót, amire rákeresünk a Google képkeresőjének vagy a Google Lens segítségével.*
- *Ha ugyanarra a fotóra sok a találat, vagy egy teljesen másik személyt találunk, a profil feltehetőleg nem valós.*


*A Google képkereső*

- *Gyanús az is, ha valaki mielőbb beszélgetési felületet szeretne váltani, például azt kéri, hogy a WhatsAppon vagy másik csevegőplatformon folytatódjon a beszélgetés. Ebben az esetben ragaszkodjunk ugyanahhoz a felülethez, ahol kezdtük a beszélgetést, illetve kezdeményezzünk egy videóhívást.*
- *Gyűjtsünk információt, ahhoz, hogy rá tudjunk keresni az illetőre az Interneten.*
- *Ellenőrizzük, hogy hamisan adja-e meg a tartózkodási helyét. (Ha valaki mobiltelefonszámmal regisztrál a Messenger szolgáltatásra, ellenőrizni tudjuk, hogy milyen országhoz tartozik a szám. Ha attól tartunk, hogy egy oldal csaló, ellenőrizhetjük az oldal helyét.)*
- *Kérjünk tanácsot egy rokonoktól, vagy bizalmas ismerőstől, ha nem vagyunk biztosak a dolgunkban!*
- *Léteznek olyan közösségi oldalak is, ahol az érintettek megoszthatják egymással a rossz tapasztalataikat, érdemes átolvasni a posztolt történeteket. Persze nem kell minden történetnek hitelt adni, azonban a gyakran ismétlődő esetek alapján sok tanulságot szerezhetünk.* Mások képeit azonban ne posztoljuk, ez ugyanis személyiségi jogokat sérthet!



## Befektetési csalások

Rendkívüli hozam, nulla vagy nagyon alacsony kockázat mellett. Ilyen ígéretekkel próbálnak elcsábítani a befektetési csalók. Az átverések gyakran reklámokat alkalmaznak, korábbi vásárlók „sikertörténeteit" azért, hogy meghozzák a kedvet a befektetéshez, azonban ezek nem valósak. A leggyakrabban valamilyen kriptovaluta vagy ingatlan megvásárlására próbálnak rávenni bennünket és a kifizetést is kriptovalutában vagy más, nem hagyományos fizetési formában kérik.


- *Ezeket a csalásokat úgy kerülhetjük el, ha nem adunk hitelt a túl csábító reklámoknak. Nincs garantáltan magas hozam kockázat nélkül.*
- *Ahhoz, hogy képesek legyünk dönteni egy befektetésről, célszerű előbb pénzügyi ismereteket szerezni.*

## Hitelcsalások

A hitelcsalók olyan üzeneteket, illetve olyan bejegyzéseket írnak, amelyekben alacsony kamatú gyorshitelt ajánlanak kis összegű előlegért cserébe. A hitelcsalások a nehéz gazdasági időszakokban mindig gyakoribbá válnak. Érthető módon a kiszolgáltatott pénzügyi helyzetben lévők különösen veszélyeztetettnek számítanak.


- *Ha valaki előleg fizetést kér személyes hitelért cserébe, az gyakorlatilag biztosan csalás.*
- *A különböző gyorskölcsönök, hitelek felvétele nehéz anyagi helyzetben csábító gondolat lehet, azonban ezek nem jelentenek megoldást, könnyedén csak még rosszabb helyzetben találhatjuk magunkat.*
- *Soha ne döntsünk azonnal! Kérjünk tanácsot rokonoktól, ismerősöktől, munkatársaktól!*
- *Ha személyi hitel felvételében gondolkodunk, tájékozódjunk a Magyar Nemzeti Bank (MNB) Hitel- és lízingtermékválasztó programjának segítségével:*

TIPP

https://alk.mnb.hu/portal/fogyasztoknak/bal_menu/ptilekerdezo

- *Pénzügyi döntésekhez pedig segítséget kaphatunk az MNB Pénzügyi navigátor szolgáltatásának weboldalán:*

https://www.mnb.hu/fogyasztovedelem/hitel-lizing/fogyasztasi-hitelek/szemelyi-kolcson


A Magyar Nemzeti Bank Pénzügyi Navigátor oldala

a pénzügyi tudatossághoz nyújt segítséget

## Álláshirdetéses csalások:

Az álláshirdetéses csalók félrevezető vagy hamis álláshirdetések segítségével próbálják megszerezni személyes adatainkat vagy a pénzünket.

TIPP

- *Egyszerűen hagyjuk figyelmen kívül az előrefizetést kérő álláshirdetési bejegyzéseket!*
- *Amikor rákattintunk egy álláshirdetés hivatkozására, kerüljük el az olyan webhelyeket, amelyek nem kapcsolódnak az eredeti álláshirdetéshez, vagy kényes adatokat (például hivatalos azonosítót) kérnek biztonságos (https) böngészés használata nélkül. További tippekért olvasd el facebookos álláskeresési útmutatónkat.*
- *Keressünk rá a hirdető cégre egy megbízhatónak tartott portálon!*

## Hozzáférésikód-lopások:

Hivatkozást osztanak meg velünk, amelyben hozzáférést kérnek a Facebook-fiókhoz vagy -oldaladhoz. Úgy tűnhet, hogy a hivatkozás legitim alkalmazásból származik, ám valójában olyan módszer, amellyel a csalók hozzáférést szerezhetnek a fiókhoz.

A Facebook fiók jelszavát nagyon gyakran adathalász üzenetekben próbálják megszerezni tőlünk. Ez érkezhet valamilyen csevegőappon (pl. Messengeren) vagy sok esetben e-mailben.


- *Legyünk óvatosak, ha olyan e-mailt vagy Messenger üzenetet kapunk, amiben az szerepel, hogy valaki megpróbálta feltörni a fiókunkat, ezért állítólag jelszót kellene cserélnünk az üzeneteben feltüntetett linkre kattintva! Ez egy gyakori csalás, az üzenetben szereplő link hamis weboldalra vezet, ami csak úgy néz ki, mintha a Facebook bejelentkező oldala lenne.*
- *Ha szeretnénk ellenőrizni, hogy valóban érkezett-e rendszerüzenet a Facebooktól, azt a profilban itt érhetjük el: Beállítások > Biztonság és bejelentkezés > A Facebooktól érkezett legutóbbi e-mailek megtekintése*

## Csalások a Facebook Marketplace-en

Ahogy a különböző online piactereken, a Facebook Marketplace-en is előfordulnak csalások.

Használt termék vásárlása — a konkrét piactértől függetlenül — mindig hordoz magában biztonsági kockázatot. Tényleg azt kapjuk, ami a képen szerepel? Megbízható az eladó? Létezik egyáltalán a termék? Valóban olyan állapotú, mint amit az eladó állít?

Érdemes megjegyezni azt is, hogy a másik oldalon állva, eladóként is csalás áldozatává válhatunk. A Marketplace-en is előforduló, manapság gyakori csalástípus, hogy a csaló vevőként jelentkezik és a beszélgetést egy másik platformra tereli, például a Whatsappra vagy egy másik weboldalra.

TIPP

- *Általánosságban azt mondhatjuk, hogy célszerűbb azokat az online piactereket használni – mind eladóként, mind vevőként – ahol az eladók* vásárlói értékelésekkel *rendelkeznek, mert a Facebook Marketplace profilok alapján a másik félről nem tudunk elegendő információhoz jutni.*
- *Az adásvételre azt javasoljuk, hogy személyes találkozás során kerüljön sor, amennyiben az lehetséges.*
- *Csak a biztonságos fizetési módokat használjuk és inkább kerüljük el az ajándékkártyákat és a különböző pénzküldési és fizetési szolgáltatásokat!*
- *Egyes online piacterek garanciát is vállalnak arra, hogy amennyiben probléma merül fel az adásvétel során, visszatérítik a pénzt.*

## Az aktuális „forró téma”

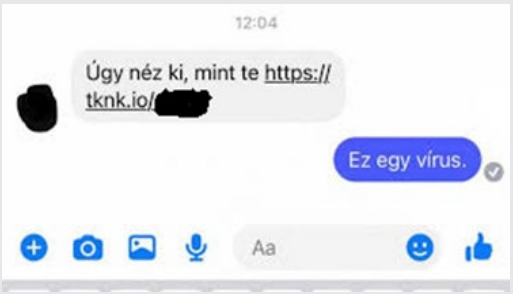
A kiberbűnözők a félelemkeltés mellett leggyakrabban a kíváncsiságot használják ki. Ehhez bármilyen témát felhasználnak, ami után aktuálisan nagy a közérdeklődés. Ezért legyünk extrán óvatosak minden olyan üzenettel/hirdetéssel, ami aktuálisan „forró” témának számít. Néhány példa a közelmúltból:

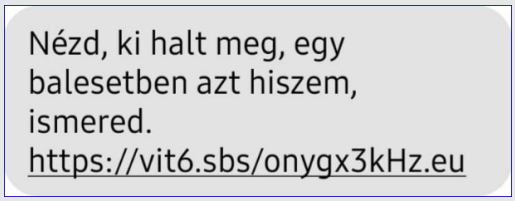
- A Covid-19 járvány kirobbanásakor a koronavírussal és vakcinákkal kapcsolatos csalások száma emelkedett meg. (A Covidscamekkel a „Kibertámadások a koronavírus árnyékában” című kiberbiztonsági elemzésünkben foglalkoztunk.)
- Az ukrán háború kitörése után pedig az adományozási csalások terjedtek el. (A jótékonysági és katasztrófahelyzeteket kihasználó csalásokkal is foglalkoztunk már korábban.)
- Minden évben az adózási időszak fontosabb dátumai előtt (például: február 25, május 20.) tapasztalható, hogy megnő a NAV nevével visszaélő csalások száma.

# Általános biztonsági tanácsok

- A jelszavakat, hozzáférési kódokat, bankkártyán szereplő információkat soha ne adjuk ki másnak!
- Ne kattintsunk üzenetben/e-mailben/SMS-ben érkező linkekre!
- Azt se feledjük, hogy ismerőseink fiókjait is feltörhetik, ezért legyünk óvatosak minden olyan üzenettel kapcsolatban, amiben fájlt, vagy linket kapunk, szöveg nélkül, vagy nagyon általánosan megfogalmazott szöveggel, mint például:

„Szia! Ez érdekelhet" vagy „Úgy néz ki, mint te." „Nézd, ki halt meg."




- Hívjuk fel az ismerőst, és kérdezzünk rá, hogy valóban ő küldte-e az üzenetet!
- Gyanús lehet, ha egy hosszú évek óta nem látott ismerős egyszer csak egy ilyen üzenetet küld.
- Soha ne jelentkezzünk be online fiókba nyilvános hálózatról, vagyis olyan hálózatra, aminek a jelszavát más is ismeri rajtunk kívül (pl: ingyenes szállodai, éttermi, stb. Wi-Fi hálózat). Ennek egyszerű az oka: sosem tudhatjuk, hogy a hálózathoz csatlakozik-e rosszindulatú személy.

Túl könnyen érhetőek el olyan szoftverek, amelyek egy alacsony informatikai képzettségű támadó is képes lehet a hálózati csomagok elfogásával (network sniffing) olyan érzékeny információkhoz jutni, mint a hálózatra csatlakozás után begépelt jelszavak vagy olyan technikai adatok (pl. session tokenek), amelyek birtokában hozzáférhet a fiókunkhoz.

- Legyünk válogatósak az ismerősnek jelöléssel! Ne tévesszen meg egy jól beállított (rendszerint stúdió) kép! Használjuk bátran a romantikus csalásoknál is javasolt Google képkeresőjét a kamuprofilok szűréséhez!
- Üzleti fiókok esetében külsős cégnek semmiképp se adjunk hozzáférést és a használt bankkártyánál állítsunk be fizetési limitet! Gyanús tranzakciók esetén pedig mielőbb tiltsuk le a bankkártyát!

# Online zaklatás

A pénzügyi csalások mellett meg kell említeni a másik hatalmas problémakört, az online bántalmazást, zaklatást.

A közösségi oldalak a gyors kapcsolatteremtés, és az anonimitás által lehetőséget adnak a társadalmilag nem elfogadható magatartásformáknak, mint például a másokat megalázó, sértő, megfélemlítő vagy éppen szexuális tartalmú üzenetek küldése.

Bárki válhat online zaklatás áldozatává, ezt biztonsági beállításokkal nem tudjuk megelőzni, biztonságtudatos használattal is csupán csökkenteni tudjuk a lehetőségét. A közösségi oldalak általában biztosítanak arra lehetőséget, hogy a zaklató személyeket letiltsuk, azonban önmagában ez a lépés nem mindig elegendő a probléma kezeléséhez.

A témával egy korábbi elemzésünkben is foglalkozunk.

## Tiltások kezelése

A zaklató felhasználók vagy ismerősök tiltása — vagy korlátozása — indokolt lehet. (Érdemes azt is megjegyezni, hogy Facebook alkalmazásokat és oldalakat is lehetséges tiltani.)

A tiltási lehetőségekről és ezek használatáról bővebb információt itt találunk: Kattintsunk a profilképünkre > Beállítások és adatvédelem > Beállítások > Adatvédelem > Tiltás

Ha úgy gondoljuk, hogy a Facebookon valamilyen tartalom sérti a személyiségi jogainkat, vagy más, érvényben lévő jogszabályt, a visszaélést jelentő vagy kéretlen tartalmakat a legkönnyebben a tartalom közelében található „Jelentem" hivatkozás használatával lehet jelezni a szolgáltató felé. Erről bővebb információ a Facebook súgóközpontjában található.

Fontos tudnunk, hogy mások zaklatása jogszabályokban meghatározottak szerint kimerítheti a bűncselekmény fogalmát, ezért feljelentést tehetünk a rendőrségen.

Az online zaklatásnak különösen a gyermekek kitettek, ezért gondviselőként, szülőként – ha már mi magunk képesek vagyunk biztonságtudatosan kezelni a közösségi médiát – érdemes felkészíteni a gyermeket is, arra, hogy

- nem mindenki az az Interneten, mint akinek láttatja magát
- merjen beszélni arról otthon, ha az Interneten kellemetlen élmények érik.

Jó ha tudjuk, hogy krízis esetén tinédzserként és szülőként is kérhetünk tanácsot szakembertől!

További hasznos információkat találhat például a

- Nemzeti Média- és Hírközlési Hatóság Internet hotline;
- a Kék vonal gyermekkrízis alapítvány;
- a Magyar Rendőrség;
- illetve az Igazságügyi Minisztérium áldozatsegítő szolgálatának weboldalán.

## Tájékozódás és álhírek a közösségi médiában

A koronavírus járvány jelentős változásokat hozott az élet számos területén. A távmunka előretörése mellett hangsúlyosabbá vált az online kapcsolattartás és a médiafogyasztás, ami az internetes csalások mellett az álhírek fokozott terjedésére is hatással volt.

Mik azok az álhírek?

Általánosságban elmondható, hogy az álhírek olyan téves információkat tartalmazó hírek, amelyeket úgy tesznek közzé és hirdetnek, mintha azok valódiak lennének. A motiváció, hogy miért hoznak létre és terjesztenek hamis híreket, épp olyan sokféle lehet, mint ahány egyéni vélemény létezik. Míg néhány álhír látszólag ártalmatlan vagy csupán egy vicc, sok olyan is akad köztük, amelyik kifejezetten káros és veszélyes is lehet. Az álhírek sok esetben azért készülnek, hogy megváltoztassák az emberek nézeteit, véleményüket vagy felfogásukat, ezáltal befolyásolva a döntéseiket.

A Nemzeti Média- és Hírközlési Hatóság a lakosság médiahasználati és hírfogyasztási szokásait vizsgálta a koronavírus-járvány első szakaszában. A tanulmány által — habár az elsősorban a koronavírussal kapcsolatos hírekre fókuszálva készült — jobban megérthetjük a Facebook szerepét a társadalmunkban és az álhírek terjedésében.

A tanulmány többek között rámutat arra, hogy

- A közösségi oldalak közül a Facebook domináns szerepet töltött be a járvánnyal kapcsolatos informálódás tekintetében — a megkérdezettek 96 százaléka használta és 90 százalékuknak ez volt a fő használt közösségi oldala a járványhelyzet ideje alatt.
- Fontos kiemelni, hogy a legtöbb internethasználó az online hírportálokon keresztül szokott tájékozódni a járványról (64%), azonban
- egy nem elhanyagolható felhasználói réteg (23%) elsődlegesen a Facebookról és videómegosztó oldalakról értesült a járvánnyal kapcsolatos hírekről.
- A rémhírek megjelenése és terjedése kapcsán valós problémáról beszélhetünk, hiszen a járványhelyzet alatt a felnőtt lakosság 59 százaléka találkozott olyan hírrel a koronavírus-járványról, amelyről azt gondolta, hogy elferdítik vagy akár meg is hamisítják a valóságot.

- A megkérdezettek szerint a vezető médiatípusok közül egyértelműen az Internet a forrása, a közvetítő közege ezeknek az információknak (81%), és az interneten belül elsősorban a közösségi média (Facebook) fertőzöttségét említik meg a válaszadók (66%).

Az álhírek felismerése néha nagyon egyszerű, ám esetenként nagyon nehéz is lehet. Könnyebb dolgunk van a szenzációhajhász vagy félelemkeltő hírekkel.


A pandémiás időszakban az Országos Korányi Pulmonológiai Intézetről terjesztettek valótlan állításokat. Erről egy korábbi kiberbiztonsági elemzésünkben írtunk.

TIPP

- *Ha egy hír vagy poszt erős érzelmeket vált ki belőlünk addig soha ne tekintsük addig 100%-ban hitelesnek, amíg legalább több forrást el nem olvastunk a témában.*
- *Az álhíreket tartalmazó posztok sok esetben nem hírportálokra, tanulmányokra, hanem blogokra hivatkoznak. A blogok lényegében internetes naplók, amit bárki létrehozhat, ezért kevésbé tekinthetők hiteles forrásnak, mint például egy tudományos folyóirat, aminél szigorú tényellenőrzési folyamatot követően jelenhet csak meg információ.*
- *Az álhírek terjesztése sok esetben automatizált programokkal – amelyeket botoknak is hívunk – kamuprofilokkal történik, ezért mindig ellenőrizzük a szerzőt. Valós-e a profil egyáltalán?*

Az álhírek felismeréséről további hasznos tanácsokat találhat a SANS Intézettel közös hírlevelünk 2020 októberi számában.

## Moderálás a Facebookon

A közösségi média a kommunikáció mellett az önkifejezésre is lehetőséget ad. Véleményt formálhatunk a világról, felhívhatjuk ismerőseink figyelmét a szerintünk érdekes és fontos történésekre, azonban vannak szabályok, amelyeket figyelembe kell vennünk.

Amikor regisztrálunk a platformra (ezt 13 éves kortól lehet megtenni), elfogadjuk annak felhasználási feltételeit. Ennek részeként a platform moderálja a felületén szereplő tartalmakat. A Facebook a moderálási elveit az ún. közösségi alapelveiben egyfajta etikai kódexben határozza meg. A Meta szabályozásának célja, hogy visszaszorítsa például a gyűlöletkeltő, erőszakra uszító, álhíreket terjesztő tartalmakat.

A Meta így nyilatkozik arról, hogy melyek azok a tartalmak, amelyek „valószínűleg sértik" a közösségi alapelveket:

- Hamis fiókok által létrehozott és terjesztett tartalom;
- Olyan tartalmak, amelyekben ismert gyűlöletkeltő kifejezések szerepelnek;
- Olyan tartalmak, amelyek potenciálisan súlyos erőszakot szíthatnak vagy segíthetnek elő;
- Megfélemlítés és zaklatás;
- Kéretlen tartalom;
- Durva erőszak;
- Felnőtt meztelenség és szexuális tevékenység;
- Hamis állítások a Covid19-ről, amelyek feltehetően közvetlenül növelnék az egészségkárosodás komoly kockázatát;
- Korlátozott áruk vagy szolgáltatások adásvételére vagy népszerűsítésére irányuló bejegyzések.

A Meta alapvetően algoritmusokkal vizsgálja a tartalmakat, az eltávolításról pedig általában küld értesítést. Amennyiben úgy érezzük, hogy a tiltás nem volt jogos, kérhetünk újraellenőrzést, bizonyos esetekben pedig az Ellenőrző Bizottsághoz is fordulhatunk felülvizsgálatért, ami egy független szakértőkből álló testület.


- *A közösségi alapelvek mellett tekintettel kell lennünk mások* személyiségi jogaira *is. Legyünk különösen körültekintőek* fényképek, videók *megosztásakor!*
- *A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) tájékoztatóban is felhívja a figyelmet arra, hogy „GDPR fogalom-meghatározása alapján* egy ember arca, képmása személyes adatnak, *a képfelvétel készítése, valamint az adatokon elvégzett bármely művelet adatkezelésnek, az adatok kezelésének célját és eszközeit önállóan vagy másokkal együtt meghatározó természetes vagy jogi személy, egyéb szervezet pedig – így akár egy közösségi oldal is – adatkezelőnek minősül."*
- *Jogellenes adatkezelés –* például mást kellemetlen, kínos helyzetben bemutató fénykép önkényes posztolása, becsületsértő kommentelés, tiltott tartalmak megosztás *a stb. – esetén a magánszemély adatkezelő is felelősségre vonható és súlyos jogi következményekkel számolhat."*
- *Ugyanez ránk is érvényes: amennyiben személyiségi jogainkkal visszaélő tartalommal találkozunk, a NAIH javaslata szerint először az adatkezelőhöz kell fordulni: az esetet jelenteni kell az érintett oldalnak, illetve lehet kérni az adat törlését is. Bizonyos esetekben (például ún. rajongói oldalak) a Facebook és az oldal üzemeltetője közös adatkezelőnek minősül, így bármelyiküknél lehet eljárást kezdeményezni.*
- *Használjuk saját névvel a platformot! Így ha korlátoznák vagy feltörnék a fiókunkat, személyi okmánnyal igazolhatjuk magunkat.*
- *Amennyiben úgy érezzük, hogy egy adott tartalom sérti a platform elveit, azt, az adott bejegyzés három pöttyre koppintva, majd a bejegyzés jelentését kiválasztva tudjuk jelenteni.*

NEMZETI
KIBERVÉDELMI INTÉZET


nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast


2023