

Biztonságos bankolás – ügyféltájékoztató (2026)

A Trive Bank Hungary Zrt. kiemelt figyelmet fordít az elektronikus bankolás biztonságára. Az alábbi tájékoztató célja, hogy ügyfeleink naprakész, közérthető és gyakorlatias információkat kapjanak az online pénzügyi visszaélések megelőzéséhez, valamint a digitális eszközök biztonságos használatához.

1. Általános biztonsági alapelvek

- A Trive Bank **soha nem kér** e-mailben, SMS-ben vagy telefonon:
 - teljes bankkártya-adatokat (CVV/CVC kód),
 - internetbanki vagy mobilbanki jelszót,
 - egyszer használatos megerősítő kódot.
 - Mindig a **hivatalos csatornákat** használja (www.trive.hu, mobilalkalmazás).
 - Közösségi médiában megjelenő banki hirdetésekre, üzenetekre ne kattintson.
-

2. Adathalászat és digitális csalások (2026-ban jellemző formák)

Az elmúlt években a csalások módszerei jelentősen fejlődtek:

- **SMS-alapú (smishing) támadások:** csomagértékesítésnek, banki riasztásnak álcázva.
- **QR-kódos csalások:** hamis fizetési vagy bejelentkezési oldalakra irányítanak.
- **Mesterséges intelligenciával generált hanghívások:** valós személy vagy banki ügyintéző hangját utánozzák.
- **Hamis mobilalkalmazások:** külső forrásból letölthető, bankinak tűnő appok.

Ha egy üzenet sürget, megfélemlít vagy „azonnali intézkedést” kér, az szinte biztosan csalás.

3. Internetes és mobilbankolás biztonsága

- Csak **frissített operációs rendszerrel** és alkalmazásokkal bankoljon.
 - Használjon **biometrikus azonosítást** (ujjlenyomat, arcfelismerés), ahol elérhető.
 - Ne használjon nyilvános, jelszó nélküli Wi-Fi hálózatot bankoláshoz.
 - Banki alkalmazást kizárólag hivatalos alkalmazás-áruházból telepítsen.
-

4. Jelszavak és hitelesítés

- Minden szolgáltatáshoz **egyedi jelszót** használjon.
 - Javasolt a **jelszókezelő alkalmazások** használata.
 - Kapcsolja be a **kétlépcsős azonosítást**, ahol lehetséges.
 - Ne mentse el jelszavait böngészőben megosztott vagy idegen eszközön.
-

5. Online vásárlás és digitális fizetés

- Csak megbízható webáruházban vásároljon.
 - Ellenőrizze a fizetési oldal címét és tanúsítványát.
 - Ne mentse el bankkártya-adatait ismeretlen oldalon.
 - Használjon virtuális vagy limitált bankkártyát online fizetéshez, ha elérhető.
-

6. Telefonos és „social engineering” csalások

Gyanús, ha:

- pénz „biztonságba helyezésére” kérik;
- távoli hozzáférést kérnek az eszközéhez;
- banki incidensre hivatkozva adatokat kérnek;
- Önnek kell bediktálnia egy SMS-ben kapott kódot.

A Trive Bank **nem végez ilyen jellegű egyeztetést telefonon.**

7. Külön figyelem fiataloknak és online játékosoknak

- Játékon belüli üzenetekben érkező linkekre ne kattintson.
 - Ingyenes jutalom, skin vagy „cheat” ígérete gyakran kártékony kódot rejt.
 - Használjon külön e-mail címet és erős jelszót játéksiókokhoz.
-

8. Mit tegyen gyanú esetén?

Ha úgy érzi, hogy adatai veszélybe kerültek:

- azonnal lépjen kapcsolatba ügyfélszolgálatunkkal:
 -  + 36 1 215 1206
 -  ugyfelszolgalat@trive.hu
 - módosítsa jelszavait,
 - ellenőrizze számlatörténetét.
-

9. Hasznos külső források

- Kiberpajzs program (www.kiberpajzs.hu)
 - Nemzeti Kibervédelmi Intézet (NKI) (nki.gov.hu)
-

10. Kiegészítés – Digitális működési ellenállóképesség (DORA)

A Trive Bank Hungary Zrt. a pénzügyi szektorra vonatkozó **Digitális Működési Ellenállóképességről szóló rendelet (DORA)** előírásainak megfelelően kiemelt figyelmet fordít az információs és kommunikációs technológiák (IKT) biztonságára és az ügyfeleket érintő digitális kockázatok kezelésére.

A DORA célja, hogy a pénzügyi intézmények – így a Trive Bank is – képesek legyenek:

- megelőzni a digitális működést érintő zavarokat,
- gyorsan reagálni az informatikai incidensekre,
- biztosítani a szolgáltatások folytonosságát.

Mit jelent ez az ügyfelek számára?

- A Bank **folyamatosan monitorozza** digitális rendszereit és azonosítja a kockázatokat.
- Informatikai vagy kibertámadással összefüggő incidensek esetén a Bank **meghatározott eljárásrend szerint jár el**, és szükség esetén tájékoztatja az érintett ügyfeleket.
- A Bank kizárólag olyan technológiai és szolgáltatói megoldásokat alkalmaz, amelyek megfelelnek a vonatkozó biztonsági és felügyeleti elvárásoknak.

Az ügyfelek szerepe a digitális ellenállóképességben

A digitális biztonság közös felelősség. Az ügyfelek részéről különösen fontos:

- a jelen tájékoztatóban foglalt biztonsági ajánlások betartása,
- a gyanús események haladéktalan jelzése a Bank felé,
- az elektronikus csatornák rendeltetésszerű használata.