

Fontos biztonsági figyelmeztetések az online bankolással és értékpapír-kereskedéssel kapcsolatban

Tisztelt Ügyfelünk!

Az Ön biztonsága számunkra a legfontosabb. A növekvő kiberbűnözési fenyegetésekre való tekintettel szeretnénk felhívni figyelmét a jelenlegi kockázatokra, és ajánlásokat adni arra, hogyan védheti meg a lehető legjobban önmagát és vagyonát.

A jelenlegi fenyegetések áttekintése:

- **Adathalász (Phishing) e-mailek és SMS-ek (Smishing):** Csalók megpróbálják megszerezni az Ön bejelentkezési adatait (felhasználónév, jelszó, TAN), hamis e-mailek vagy SMS-ek küldésével, amelyekben bankunk nevében lépnek fel. Ezek az üzenetek gyakran arra ösztönzik Önt, hogy kattintson egy hivatkozásra, amely egy hamis bejelentkezési oldalra vezet.
- **Káros szoftver (Malware) és trójai programok:** A kártékony szoftverek észrevétlenül települhetnek az Ön eszközére, érzékeny adatokat figyelhetnek meg, vagy manipulálhatják az Ön tranzakcióit.
- **Telefonos csalás (Vishing):** Csalók telefonon banki alkalmazottnak vagy informatikai támogatónak adják ki magukat, és megpróbálják rávenni Önt, hogy adja meg bejelentkezési adatait vagy hagyjon jóvá tranzakciókat. Felhívjuk figyelmét, hogy soha nem fogjuk Önt előzetes kérdés nélkül arra kérni, hogy adja meg teljes bejelentkezési adatait vagy TAN-kódjait.
- **Befektetési csalás (Scam):** Legyen óvatos a túlzottan magas hozamokat ígérő ajánlatokkal szemben, különösen ismeretlen szolgáltatóktól vagy közösségi médián keresztül. Alaposan ellenőrizze az ilyen ajánlatok megbízhatóságát, és tájékozódjon az illetékes felügyeleti hatóságoknál (Ausztriában ez a FMA – Pénzüpiaci Felügyelet).

Így védekezhet – Top 10 ajánlás:

1. **Soha ne adja meg bejelentkezési adatait vagy TAN-kódjait e-mailben, SMS-ben vagy telefonon keresztül:** Soha nem fogjuk Önt előzetes kérdés nélkül arra kérni, hogy ezeken a kommunikációs csatornákon keresztül adja meg vagy ossza meg bejelentkezési adatait vagy TAN-kódjait.
2. **Alaposan ellenőrizze a feladót és a linkeket:** Ne nyisson meg e-maileket, és ne kattintson az SMS-ben kapott linkekre, amennyiben nem biztos a feladó személyében. Figyeljen a szokatlan megfogalmazásokra, helyesírási hibákra vagy a hiányzó személyes megszólításra.
3. **Kizárólag a hivatalos weboldalunkat használja:** A bankunk címét mindig közvetlenül írja be a böngészőbe. Mentse el az oldalunkat könyvjelzőként, és használja azt a jövőbeni látogatásokhoz.
4. **Ellenőrizd az URL-t (webcímet):** Ügyelj arra, hogy bankunk címe helyes legyen, és „https://”-sel kezdődjön. Ez azt jelzi, hogy a kapcsolat titkosított és biztonságos.
5. **Rendszeresen frissítse a szoftvereit:** Tartsa naprakészen operációs rendszereit, böngészőit és vírusirtó programjait, hogy bezárja a ismert biztonsági réseket.
6. **Használjon biztonságos jelszavakat:** Alkalmazzon erős, egyedi jelszavakat online bankolásához, és változtassa meg azokat rendszeresen. Kerülje ugyanazon jelszavak ismételt használatát.
7. **Rendszeresen ellenőrizze számlamozgásait:** Folyamatosan figyelje online banki tranzakcióit és értékpapírszámla-kivonatait. Ha szokatlan műveletet észlel, azonnal vegye fel velünk a kapcsolatot.
8. **Használja biztonsági eljárásainkat:** Ismerkedjen meg az általunk kínált biztonsági módszerekkel (pl. mobile-TAN, pushTAN stb.), és aktívan alkalmazza azokat.
9. **Legyen óvatos a befektetési ajánlatokkal szemben:** Különösen az értékpapírszolgáltatások területén sok a megbízhatatlan szolgáltató. Mindig tájékozódjon független forrásokból, és ellenőrizze a szolgáltatók, illetve termékek megbízhatóságát a pénzügyi felügyeleti hatóságnál (FMA).

Teendők gyanú esetén:

Azonnal lépjen kapcsolatba velünk: Ha gyanítja, hogy bejelentkezési adatait illetéktelenül használták fel, gyanús e-mailt vagy SMS-t kapott, vagy szokatlan tranzakciót észlelt, azonnal zárolja online banki hozzáférését, és haladéktalanul értesítsen minket.

Tegyen feljelentést a rendőrségen: Csalás esetén ajánlott a rendőrségen is feljelentést tenni. Mindent megteszünk annak érdekében, hogy pénzügyi tranzakciói biztonságát folyamatosan biztosítsuk.

Az Ön együttműködése elengedhetetlen ebben.

Köszönjük bizalmát.

Az Ön PARTNER BANK AG