

Dôležité bezpečnostné upozornenia pre Váš Online Banking a obchodovanie s cennými papiermi

Vážená klientka, vážený klient,

Vaša bezpečnosť je našou najväčšou prioritou. Vzhľadom na rastúcu hrozbu kyberkriminality Vás dôrazne upozorňujeme na aktuálne riziká a poskytneme Vám odporúčania, ako čo najlepšie ochrániť seba a svoj majetok.

Prehľad aktuálnych hrozieb:

- **Phishingové e-maily a SMS (Smishing):** Podvodníci sa snažia získať Vaše prihlasovacie údaje (používateľské meno, heslo, TAN) tým, že zasielajú falošné e-maily alebo SMS v mene našej banky. Tieto správy Vás často nabádajú kliknúť na odkaz vedúci na podvodnú prihlasovaciu stránku.
- **Malware a trójske kone:** Škodlivý softvér sa môže nepozorovane nainštalovať do Vášho zariadenia a sledovať citlivé údaje alebo manipulovať s Vašimi transakciami.
- **Podvod cez telefón (Vishing):** Podvodníci sa telefonicky vydávajú za zamestnancov banky alebo IT podpory a snažia sa Vás presvedčiť, aby ste im prezradili svoje prihlasovacie údaje alebo schválili transakcie. Upozorňujeme, že Vás nikdy nebudeme žiadať o poskytnutie úplných prihlasovacích údajov alebo TAN kódov bez predchádzajúceho vyzvania.
- **Investičný podvod (Scam):** Buďte obozretní pred sľubmi o neprimerane vysokých výnosoch, najmä od neznámych poskytovateľov alebo prostredníctvom sociálnych sietí. Dôkladne si overte dôveryhodnosť takýchto ponúk a informujte sa u príslušných dohľadových orgánov (v Rakúsku je to FMA – Úrad pre dohľad nad finančným trhom).

Takto sa ochránite – Top 10 odporúčaní:

1. **Nikdy neposkytuje svoje prihlasovacie údaje, TAN kódy prostredníctvom e-mailu, SMS alebo telefonátu:** Nikdy Vás nebudeme bez predchádzajúceho vyzvania žiadať o zadanie alebo poskytnutie Vašich prihlasovacích údajov či TAN kódov prostredníctvom týchto komunikačných kanálov.
2. **Dôkladne si overte odosielateľa a odkazy:** Neotvárajte e-maily ani neklikajte na odkazy v SMS správach, ak si nie ste istí, kto je odosielateľom. Všímajte si nezvyčajné formulácie, pravopisné chyby alebo chýbajúce osobné oslovenie.
3. **Výlučne používajte našu oficiálnu webovú stránku:** Adresu našej banky zadávajte vždy priamo do svojho prehliadača. Uložte si našu stránku do záložiek a používajte ju pri budúcich návštevách.
4. **Skontrolujte URL (webovú adresu):** Dbajte na to, aby adresa našej banky bola správna a začínala na „https://“. To znamená, že spojenie je šifrované a bezpečné.
5. **Pravidelne aktualizujte svoj softvér:** Udržiavajte svoje operačné systémy, prehliadače a antivírusové programy vždy aktuálne, aby ste zavreli známe bezpečnostné diery.
6. **Používajte bezpečné heslá:** Využívajte silné, jedinečné heslá pre Váš Online Banking a pravidelne ich meňte. Vyhnite sa opakovaniu rovnakých hesiel.
7. **Pravidelne kontrolujte pohyby na účte:** Priebežne sledujte svoje transakcie v Online Bankingu a výpis z účtu cenných papierov. Ak si všimnete nezvyčajné operácie, ihneď nás kontaktujte.
8. **Využívajte naše bezpečnostné postupy:** Oboznámte sa s ponúkanými bezpečnostnými metódami (napr. mobileTAN, pushTAN a pod.) a aktívne ich používajte.
9. **Buďte skeptickí pri investičných ponukách:** Najmä v oblasti služieb s cennými papiermi sa vyskytuje veľa neseriózných poskytovateľov. Vždy získavajte informácie z nezávislých zdrojov a overujte dôveryhodnosť poskytovateľov a produktov u finančného dohľadu (FMA).

Čo robiť v prípade podozrenia:

Kontaktujte nás okamžite: Ak máte podozrenie, že Vaše prihlasovacie údaje boli zneužitú, dostali ste podozrivý e-mail alebo SMS, alebo ste zaznamenali nezvyčajnú transakciu, ihneď zablokujte prístup do Online Bankingu a bezodkladne nás kontaktujte.

Podajte trestné oznámenie na políciu: V prípade podvodu je vhodné podať aj trestné oznámenie na políciu. Snažíme sa neustále zabezpečiť bezpečnosť Vašich finančných transakcií.

Vaša spolupráca je pri tom nevyhnutná.

Ďakujeme Vám za dôveru.

Vaša PARTNER BANK AG