

Důležitá bezpečnostní upozornění pro Vaše online bankovníctví a obchodování s cennými papíry

Vážená klientko, vážený kliente,

Vaše bezpečnost je naší nejvyšší prioritou. Vzhledem k rostoucímu riziku kybernetické kriminality Vás důrazně upozorňujeme na aktuální hrozby a poskytneme Vám doporučení, jak co nejlépe chránit sebe i svůj majetek.

Přehled aktuálních hrozeb:

- **Phishingové e-maily a SMS (Smishing):** Podvodníci se snaží získat Vaše přihlašovací údaje (uživatelské jméno, heslo, TAN) tím, že zasílají falešné e-maily nebo SMS jménem naší banky. Tyto zprávy Vás často vybízejí ke kliknutí na odkaz vedoucí na podvodnou přihlašovací stránku.
- **Malware a trojské koně:** Škodlivý software se může nepozorovaně nainstalovat do Vašeho zařízení a sledovat citlivé údaje nebo manipulovat s Vašimi transakcemi.
- **Telefonní podvod (Vishing):** Podvodníci se po telefonu vydávají za zaměstnance banky nebo IT podpory a snaží se Vás přesvědčit, abyste jim sdělili své přihlašovací údaje nebo potvrdili transakce. Upozorňujeme, že Vás nikdy nebudeme žádat o poskytnutí úplných přihlašovacích údajů nebo TAN kódů bez předchozí výzvy.
- **Investiční podvod (Scam):** Buďte obezřetní vůči slibům o nepřiměřeně vysokých výnosech, zejména od neznámých poskytovatelů nebo prostřednictvím sociálních sítí. Důkladně si ověřte důvěryhodnost těchto nabídek a informujte se u příslušných dozorových orgánů (v Rakousku je to FMA – Úřad pro dohled nad finančním trhem).

Takto se ochráníte – Top 10 doporučení:

1. **Nikdy neposkytujte své přihlašovací údaje ani TAN kódy prostřednictvím e-mailu, SMS nebo telefonního hovoru:** Nikdy Vás nebudeme bez předchozí výzvy žádat o zadání nebo sdělení vašich přihlašovacích údajů či TAN kódů prostřednictvím těchto komunikačních kanálů.
2. **Důkladně si ověřujte odesílatele a odkazy:** Neotevírejte e-maily ani neklikejte na odkazy v SMS zprávách, pokud si nejste jisti, kdo je odesílatelem. Všímejte si neobvyklých formulací, pravopisných chyb nebo chybějícího osobního oslovení.
3. **Používejte výhradně naše oficiální webové stránky:** Adresu naší banky zadávejte vždy přímo do svého prohlížeče. Uložte si naši stránku do záložek a používejte ji pro budoucí návštěvy.
4. **Zkontrolujte URL (webovou adresu):** Ujistěte se, že adresa naší banky je správná a začíná na „https://“. To znamená, že připojení je šifrované a bezpečné.
5. **Pravidelně aktualizujte svůj software:** Udržujte svůj operační systém, internetový prohlížeč a antivirový program vždy aktuální, abyste předešli zneužití známých bezpečnostních chyb.
6. **Používejte bezpečná hesla:** Vytvářejte silná, jedinečná hesla pro své online bankovníctví a pravidelně je měňte. Vyhýbejte se opakovanému používání stejných hesel.
7. **Pravidelně kontrolujte pohyby na účtu:** Sledujte své transakce v online bankovníctví a výpisy z účtu cenných papírů. Pokud zaznamenáte neobvyklé operace, neprodleně nás kontaktujte.
8. **Využívejte naše bezpečnostní postupy:** Seznamte se s námi nabízenými bezpečnostními metodami (např. mobileTAN, pushTAN apod.) a aktivně je používejte.
9. **Buďte obezřetní při investičních nabídkách:** Zejména v oblasti služeb s cennými papíry působí mnoho neseriózních poskytovatelů. Vždy si informace ověřujte z nezávislých zdrojů a prověřte si důvěryhodnost poskytovatelů a produktů u finančního dohledu (FMA).

Co dělat v případě podezření:

Kontaktujte nás okamžitě: Pokud máte podezření, že došlo ke zneužití Vašich přihlašovacích údajů, obdrželi jste podezřelý e-mail nebo SMS, nebo jste zaznamenali neobvyklou transakci, ihned zablokujte přístup do online bankovníctví a neprodleně nás kontaktujte.

Podejte trestní oznámení na policii: V případě podvodu je vhodné podat také trestní oznámení na policii. Neustále se snažíme zajistit bezpečnost Vašich finančních transakcí.

Vaše spolupráce je v tomto ohledu nezbytná.

Děkujeme Vám za důvěru.

Vaše PARTNER BANK AG