BEZPEČNOSTNÍ ZÁSADY PRO ELEKTRONICKÉ BANKOVNICTVÍ PPF BANKY A.S.

Banka nenese žádnou odpovědnost za ztrátu dat, únik Osobních údajů ani za jiné skutečnosti nastalé v důsledku nerespektování zde uvedených doporučení.

Uživatelská podpora pro Elektronické bankovnictví (dále jen „ELB“) je poskytována Zákaznickým servisem. Kontakty na Zákaznický servis a jeho Provozní dobu naleznete na Internetových stránkách banky.

1. **Navštěvujte pouze známé internetové stránky. Používejte pouze bezpečná hesla a důkladně je chraňte.**

   Vždy, když se dostanete na nějakou stránku, zkontrolujte, zda doména odpovídá obsahu stránek.

   Využívejte pouze důvěryhodných služeb a vždy se ujistěte, že opravdu komunikujete se správným serverem.

   Pro přístup do svých emailových účtů, účtů na sociálních sítích apod. používejte silná hesla – minimálně 8 znaků, kombinace malých a velkých písmen, číslic a speciálních znaků.

   Nepoužívejte stejná hesla pro různé služby. Používejte správce hesel.

   Používejte vícefaktorové ověřování u všech služeb a aplikací, kde je to možné. Vícefaktorové ověřování výrazně zvyšuje bezpečnost vašich osobních a finančních údajů.

2. **Neotevírejte emaily od neznámých adresátů nebo s podezřelým názvem. Stahujte a pouštějte pouze soubory, které očekáváte a které jsou od známých odesílatelů.**

   Neotevírejte přiložené soubory ani neklikejte na odkazy v takových emailech a **nikdy nesdělujte citlivé údaje na základě obdrženého emailu**. Nestahujte a nespouštějte soubory s neznámým obsahem.

   Banka nikdy neposílá nevyžádané zprávy obsahující odkazy na svoje webové stránky ani jejich prostřednictvím nevyžaduje zadávání nebo sdělování přístupových údajů do ELB.

   Prověřte telefonicky nezvyklé emaily od svých obchodních partnerů, zejména pokud se týkají změny účtu pro platby. Takové změny zkontrolujte, i když přijdou ze známého emailu.

   V poslední době se zvyšuje počet pokusů o podvodné získání přístupových údajů prostřednictvím falešných webových stránek (phishing), SMS zpráv (smishing) a telefonátů (vishing).

   Banka nikdy nevyžaduje sdělení Vašich přístupových údajů, ověřovacích kódů, nebo instalaci jakéhokoli softwaru prostřednictvím telefonu, emailu či SMS.

   Pokud obdržíte podobnou výzvu, okamžitě ukončete komunikaci a kontaktujte Zákaznický servis Banky.

3. **Používejte zařízení s výrobcem podporovanou verzí operačního systému:**

   - Android 14 a vyšší
   - Apple iOS 18 a vyšší
   - Windows 11 a vyšší
   - MacOS 18 a vyšší

   Tyto verze systémů poskytují nejnovější bezpečnostní aktualizace a ochranu proti kybernetickým hrozbám, což zajišťuje bezpečnější přihlašování do Internetového bankovnictví (dále jen „IB“), Mobilního bankovnictví (dále jen „MB“), e-Tokenu a Klientského API (dále jen „API“). Starší verze těchto systémů již nedostávají pravidelné bezpečnostní aktualizace od jejich výrobců, což je činí více náchylnými ke zneužití.

4. **Před instalací nebo aktualizací aplikace Mobilního bankovnictví nebo e-Tokenu vždy ověřte, že aplikaci poskytuje oficiálně „PPF banka a.s.“ v obchodu Google Play nebo Apple App Store.**

   Nikdy neinstalujte aplikace z neznámých zdrojů, které se vydávají za aplikaci PPF banky.

5. **Nainstalujte si antivirový software a antispyware a aktivujte jejich pravidelnou aktualizaci. Instalujte důležité aktualizace aplikací a zejména operačního systému.**

   Na všechna využívaná zařízení instalujte dostupné aktualizace operačního systému, prohlížečů a veškerých nainstalovaných programů a aplikací.

   Používejte pouze legální verze softwaru – nelegální verze mohou obsahovat viry, trojské koně a jiný malware. Takové programy mohou např. Vaše hesla odesílat jejich autorovi. Programy do počítače stahujte z webových stránek výrobce. Do mobilních telefonů instalujte pouze aplikace z oficiálních zdrojů (Google Play, Apple Store).

   Omezte přístup ostatních lidí ke svému počítači. Nikdy nepoužívejte veřejně přístupný počítač, tablet nebo mobilní telefon pro přístup k API, IB nebo MB.

   Ke svému počítači nebo mobilnímu telefonu nikdy nepřipojujte nalezená nebo neznámá média (USB flashdisky, paměťové karty, CD, DVD apod.).

   Pokud ukládáte dokumenty obsahující finanční nebo osobní údaje (např. výpisy, potvrzení o platbách), doporučujeme je chránit heslem nebo šifrovaným úložištěm.

   Neodesílejte důvěrné informace emailem bez šifrování nebo jiné formy ochrany.

6. **Pro běžnou práci, zejména při práci s internetem, nepoužívejte uživatelský profil s administrátorskými právy. Neumožňujte jiné osobě, aby se připojovala k síti prostřednictvím Vašeho uživatelského profilu.**

   Na počítač se přihlašujte jako běžný uživatel a pod administrátorskými právy se přihlašujte pouze tehdy, je-li to nezbytně nutné. **Před odchodem od počítače vždy uzamkněte obrazovku nebo ukončete všechna spojení s API a odhlaste se z IB.**

7. **IB spouštějte pouze na známém počítači a z odkazu na hlavní stránce Banky. Při přístupu do IB zkontrolujte, zda je spojení řádně zabezpečeno a komunikujete s Bankou.**

   Pokud musíte použít neznámý počítač, před přihlášením k IB zavřete všechna okna prohlížeče, poté otevřete jedno nové okno prohlížeče. Po odhlášení z IB vymažte historii prohlížení a zavřete okno prohlížeče.

   Nepřipojujte se k internetu pomocí veřejných wi-fi sítí, používejte mobilní data svého operátora nebo důvěryhodné wi-fi sítě.

8. **Pro přístup do MB využívejte biometrii.**

9. **Pro uložení Podpisového certifikátu k API použijte zabezpečené úložiště, které pro přístup k tomuto certifikátu vyžaduje použití hesla nebo PINu.**

10. **Pravidelně kontrolujte pohyby na svých účtech a platby Debetní kartou, v IB si nastavte zasílání SMS nebo emailových oznámení o vybraných událostech, v MB a ve svém mobilním telefonu povolte push notifikace.**

    V IB si můžete nastavit zasílání oznámení o přihlášení Uživatele do IB, o provedených transakcích na Účtech a Debetními kartami apod. **Je možné nastavit zasílání oznámení i jiným osobám, než jsou Uživatelé IB** – např. účetním nebo Držitelům Debetních karet.

    V MB můžete povolit push notifikace pro stejné události, jako v IB.

11. **Nastavte Uživatelům Limity pro Platební příkazy. V IB alespoň jednomu Uživateli umožněte autorizovat žádosti za Klienta.**

    Můžete nastavit Časové i Transakční limity, příp. jejich kombinace.

    V IB může Uživatel s právem autorizovat žádosti za Klienta rovněž požádat o zablokování jiných Uživatelů v případě jakéhokoli podezření na zneužití IB nebo MB – zablokování je provedeno v řádu několika minut. Doporučujeme proto vždy alespoň jednomu z Uživatelů IB toto právo udělit.

12. **Dávejte pozor, zda autorizujete Vámi zadaný Platební příkaz nebo žádost pro Banku.**

    Před jejich potvrzením vždy nejdříve zkontrolujte správnost údajů (např. proti faktuře, složence apod.), zejména údaje platby v autorizační SMS.

13. **Chraňte Bezpečnostní prvky. Své přístupové údaje nikomu nesdělujte a zabraňte odpozorování při jejich zadávání. Přístupová hesla do ELB si pravidelně měňte.**

    Veškeré dokumenty z Banky (např. smluvní dokumentaci, obálky s přístupovými jmény a hesly do ELB atd.) považujte za důvěrnou a uchovávejte na bezpečném místě. **Umožníte-li komukoliv přístup ke svým osobním údajům nebo Bezpečnostním prvkům, dáváte takové osobě možnost tato data zneužít nebo sdělit je další osobě**.

    Při tvorbě přístupového hesla do ELB nepoužívejte snadno odhadnutelné informace, jako jsou jména, data narození, telefonní čísla apod.

14. **Mobilní telefon určený pro zasílání SMS kódů pro IB nebo s nainstalovaným e-Tokenem a/nebo MB mějte neustále při sobě. Token ukládejte na bezpečné místo, pokud jej zrovna nepoužíváte.**

    Údaje v paměti mobilního telefonu chraňte PIN kódem či dalšími ochrannými prostředky, které jsou k dispozici v konkrétním přístroji. Přístup do MB zabezpečte PINem nebo biometrií. Token ukládejte nejlépe do uzamykatelné skříňky.

    Neprovádějte nelegální zásahy do operačních systémů mobilních telefonů (tzv. Jailbreak nebo root), ani si takové mobilní telefony nepořizujte.

15. **Věnujte dostatek pozornosti upozorněním vašeho počítače a na webových stránkách Banky a řiďte se jimi.**

16. **Neváhejte kontaktovat Banku v případě jakýchkoliv pochybností a podivného chování počítače při přístupu do ELB nebo k jiným službám, zejména:**

    - obdržíte-li elektronickou poštou zprávu obsahující odkaz na internetové stránky Banky;
    - v případě podezření na vyzrazení přístupových údajů;
    - v případě zavirování vašeho počítače nebo zjištění vyděračského software (ransomware) ve vašem počítači;
    - podezřelého chování ELB, např. nepřicházející SMS kódy, jiné údaje o platbě v SMS kódu, neobvyklé jméno serveru, jiný vizuální dojem, nové kroky během přihlášení, apod.;
    - ztráty Tokenu nebo mobilního telefonu, na který je zasílán SMS kód nebo je v něm nainstalován e-Token;
    - zjištění nesrovnalostí v provedených Platebních transakcích.

17. **Jak se bránit:**

    - Nesdílejte citlivé údaje, pokud si nejste jistí, s kým komunikujete.
    - Neposílejte platbu na účet, o němž nevíte, komu ve skutečnosti patří.
    - V případě nejasnosti/podezření si ověřte, zda na telefonním čísle nebo emailu osoby, kterou znáte, je skutečně ten, kdo Vás kontaktoval.

18. **Závěrečná ustanovení**

    Tyto Bezpečnostní zásady nabývají platnosti a účinnosti dnem 10. 11. 2025 a k tomuto dni ruší stávající „Bezpečnostní zásady pro Elektronické bankovnictví PPF banky a.s.“ účinné od 21. 3. 2025.

PPF banka a.s. | Evropská 2690/17 | P.O. Box 177 | 160 41 Praha 6
T +420 224 175 888 | F +420 224 175 980 | info@ppfbanka.cz | www.ppfbanka.cz

Registrováno Městským soudem v Praze, oddíl B, vložka 1834 | IČ 47116129 | DIČ CZ47116129