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, který můžete kontaktovat v Pracovních dnech od 8:00 do 18:00 na telefonním čísle +420 224 175 901 pro Internetové bankovnictví (dále jen „IB“) a API nebo +420 224 175 995 pro Homebanking (dále jen „HB“), případně na e-mailové adrese customer.service@ppfbanka.cz.

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 poskytovatelem.

   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.

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.

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

   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 chytrých telefonů stahujte aplikace z oficiálních zdrojů (Google Play, Apple Store, Windows Phone Store).

   Omezte přístup ostatních lidí ke svému počítači. Nikdy nepoužívejte veřejně přístupný počítač pro přístup k API, IB nebo HB.

4. **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 IB, resp. ukončete práci v HB a zavřete celou aplikaci.**

5. **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, po odhlášení z IB vymažte historii prohlížení.

6. **Podpisový certifikát pro HB neukládejte do počítače, ale na USB disk, který po ukončení práce s HB odpojíte od počítače.**

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, E: info@ppfbanka.cz
www.ppfbanka.cz

PPF Banka

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

8. **Pravidelně kontrolujte pohyby na svých účtech a platby Debetní kartou, v IB si nastavte zasílání SMS nebo emailových oznámení o vybraných událostech.**

   V IB si můžete nastavit zasílání oznámení o přihlášení Uživatele do IB, o provedených transakcích na Účtech a platebních kartách apod. **Je možné nastavit zasílání oznámení i jiným osobám, než jsou Uživatelé IB** – např. držitelům Debetních karet. Podrobnosti naleznete v části III. Uživatelské příručky pro IB.

9. **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 – zablokování je provedeno v řádu několika minut. Podrobnosti k žádostem naleznete v Obchodních podmínkách PPF banky a.s. pro Internetové bankovnictví a v části III. Uživatelské příručky pro IB.

10. **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.).

11. **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.

12. **Mobilní telefon určený pro zasílání SMS kódů pro API nebo IB mějte neustále při sobě. OTP Token, resp. USB disk s Podpisovým certifikátem k HB 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. OTP Token, resp. USB disk ukládejte nejlépe do uzamykatelné skříňky.

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

14. **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 OTP Tokenu nebo mobilního telefonu, na který je zasílán SMS kód;
    - ztráty USB disku, na kterém je uložen Podpisový certifikát;
    - zjištění nesrovnalostí v provedených transakcích.

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, E: info@ppfbanka.cz
www.ppfbanka.cz