PPF Banka

BEZPEČNOSTNÍ ZÁSADY PRO INTERNETBANKING PPF banky a.s.

Obsah:

Následující dokument popisuje zásady pro bezpečný provoz Internetbankingu (dále jen „IB“) PPF banky a.s. (dále jen „Banka“). Doporučujeme řídit se všemi těmito zásadami na všech počítačích, na kterých bude IB provozován. Banka nenese žádnou odpovědnost za ztrátu dat, únik Osobních údajů ani za jiné skutečnosti nastalé v důsledku nerespektování zde uvedených doporučení.

Více informací o aplikaci IB, Bezpečnostních zásadách, Bezpečnostních prvcích nebo aktuálních bezpečnostních hrozbách můžete nalézt na stránkách Banky, v IB nebo je získat v Obchodních místech Banky, na telefonním čísle +420 224 175 901 nebo na e-mailové adrese customer.service@ppfbanka.cz.

Jsou-li v textu těchto Bezpečnostních zásad použity pojmy nebo slovní spojení začínající velkým písmenem, mají význam stanovený v článku Výklad pojmů *Všeobecných obchodních podmínek PPF banky a.s.* (dále jen „VOP“) a/nebo *Obchodních podmínek PPF banky a.s. pro využívání služeb Internetbankingu* (dále jen „KOP“), případně význam specifikovaný v jednotlivých ustanoveních VOP a/nebo KOP. Aktuální znění KOP a VOP je k dispozici na Internetových stránkách www.ppfbanka.cz.

Uživatelská podpora pro IB je poskytována Zákaznickým servisem, který můžete kontaktovat v Pracovních dnech od 8:00 do 18:00 na telefonním čísle +420 224 175 901 nebo na e-mailové adrese customer.service@ppfbanka.cz.

PPF banka a.s., Praha 6, Evropská 2690/17, PSČ 160 41 Česká republika, IČ 47116129, DIČ CZ47116129
Společnost zapsaná v Obchodním rejstříku vedeném městským soudem v Praze, oddíl B, vložka 1834
Tel.: (+420) 224 175 888, fax: (+420) 224 175 980

1. BEZPEČNOSTNÍ PRVKY A POJMY

IB je nedílně spjato se dvěma internetovými portály:
- https://ibs.ppfbanka.cz – portál IB, a
- https://ibcc.ppfbanka.cz – portál Certifikačního centra.

Bezpečnostní prvky sloužící pro přístup do IB a pro Autorizaci Platebních příkazů a žádostí pro Banku se nazývají tzv. autentifikátorem. Autentifikátorem je Uživatelské jméno do IB a dále:
a) Certifikát a PIN k Certifikačnímu Tokenu, na kterém je Certifikát uložen (speciální zařízení, které se připojuje k počítači přes USB port), nebo
b) Přístupové heslo do IB a OTP kód generovaný OTP Tokenem, nebo
c) Přístupové heslo do IB a SMS kód zasílaný na mobilní telefon Uživatele.

2. OBECNÉ BEZPEČNOSTNÍ ZÁSADY

Doporučujeme využít možnosti nastavení Limitů pro Platební příkazy, a to pro všechny Uživatele IB (více o Uživatelích, nastavení Limitů a přistupových Oprávnění naleznete v KOP).

Uživatelská jména do IB, Přístupová hesla do IB, PIN, ale i Osobní údaje a Token sloužící k přístupu k IB nebo ke kterékoliv související části IB (např. přístupová jména a hesla pro přístup do Certifikačního centra) uchovávejte na bezpečném místě.

Cílem zneužití se může stát i *Smlouva o Internetbankingu* a její přílohy (dále jen „Smlouva o IB“). Tyto dokumenty považujte za důvěrné, chraňte je před ztrátou a uchovávejte je rovněž na bezpečném místě.

V případě podezření na prozrazení uživatelských jmen, hesel nebo dalších citlivých údajů neprodleně kontaktujte Zákaznický servis Banky a požádejte o zablokování IB nebo přístupů do IB.

3. BEZPEČNOSTNÍ ZÁSADY PRO POUŽÍVÁNÍ INTERNETBANKINGU

Zabezpečení systému IB je tak silné, jak silný je jeho nejslabší článek. Systém IB se skládá ze serverů Banky, sítě internet, sítě GSM, Uživatelova počítače, případně i Uživatelova mobilního telefonu, a lidského faktoru.

Servery Banky jsou zabezpečeny serverovými certifikáty, soustavou firewallů, ochranných zón, monitorovacích zařízení a dalších mechanismů, které v celém systému IB tvoří velmi silný článek.

Komunikace přes internet je provedena šifrovaným spojením mezi serverem Banky a Uživatelovým počítačem.

Síť GSM je využívána pouze pro přenos dílčích informací, které samy o sobě nemohou být zneužity k prolomení bezpečnosti IB.

Další dva články – Uživatelův počítač a případně Uživatelův mobilní telefon – jsou potenciálně nejzranitelnější místa celého systému, protože za jejich zabezpečení nemůže a neodpovídá Banka, ale pouze sám Klient, resp. Uživatel. Ochranu mobilního telefonu lze zabezpečit relativně snadno, mobilní telefon je doporučeno mít neustále při sobě a údaje v jeho paměti chránit PIN kódem či dalšími ochrannými prostředky, které jsou k dispozici v konkrétním přístroji.

Již obtížnější může být pro laického Uživatele zajištění bezpečnosti počítače, aby na něj nikdo nemohl nainstalovat programy umožňující dálkovou správu včetně odečítání klávesnice (získání hesla nebo PIN), kopírování souborů (Certifikátu), případně podvržení zobrazované informace. Je proto nezbytné věnovat zabezpečení Uživatelova počítače náležitou pozornost a případně bezpečnostní nastavení také konzultovat s odborníkem. Doporučujeme používat antivirové/antispyware řešení.

Relativně samostatnou kapitolou tvořící potenciálně nejslabší článek zabezpečení je tzv. lidský faktor. Jedná se o fakt, že Uživatel může vyzradit důležité součásti zabezpečení potenciálnímu útočníkovi, který by je pak mohl zneužít. Zabezpečení IB (a dalších jejích součástí) by mělo být natolik důkladné, aby ani v případě vyzrazení některých citlivých informací neoprávněné osobě nemohlo dojít k jeho zneužití. Systém bezpečnostních prvků vždy tvoří jeden či několik údajů, které by měl znát pouze Uživatel, a dalšího zařízení, které slouží k ověřování jeho identity (Certifikační Token s PINem, OTP Token s OTP kódem, mobilní telefon s SMS kódem). Každý

PPF banka a.s., Praha 6, Evropská 2690/17, PSČ 160 41 Česká republika, IČ 47116129, DIČ CZ47116129
Společnost zapsaná v Obchodním rejstříku vedeném městským soudem v Praze, oddíl B, vložka 1834
Tel.: (+420) 224 175 888, fax: (+420) 224 175 980

Uživatel by si měl být vědom citlivosti všech údajů, které slouží k ověřování jeho identity v souvislosti s používáním IB, a za žádných okolností tyto údaje nesdělovat. Banka za žádných okolností nebude po Uživateli vyžadovat sdělení těchto údajů mimo jejich zadávání do IB.

4. PHISHING

Využívejte pouze důvěryhodných služeb a vždy se ujistěte, že opravdu komunikujete se správným poskytovatelem služeb. Při přístupu na BÚ a zadávání Platebních příkazů a žádostí pro Banku zkontrolujte, zda je spojení řádně zabezpečeno a komunikujete s Bankou (zkontrolujte si platnost a údaje v certifikátu SSL zabezpečení, certifikáty Banky jsou vydány společností „thawte, Inc.“). Jestliže si nejste jisti, zda opravdu komunikujete s Bankou, obraťte se na Zákaznický servis Banky.

Přístupová hesla do IB a PINy volte tak, aby nebyly snadno uhádnutelné nebo odvoditelné z informací o Vaší osobě. Banka nikdy nevyžaduje zadání nebo potvrzení těchto údajů prostřednictvím elektronické pošty; pokud po vás budou jménem Banky takové informace požadovány, informujte prosím Zákaznický servis Banky.

Dávejte pozor, zda potvrzujete Vámi zadaný Platební příkaz nebo žádost pro Banku. Před jejich potvrzením vždy nejdříve zkontrolujte správnost údajů (např. proti faktuře, složence apod.).

Pravidelně kontrolujte pohyby na svých účtech a platby platební kartou. V případě zjištění jakýchkoli nesrovnalostí se neprodleně obraťte na Banku.

Neotvírejte podezřelé elektronické zprávy (zprávy od neznámých odesilatelů, zprávy s nesmyslným předmětem apod.), zejména neotevírejte přílohy takových zpráv. Banka nikdy neposílá nevyžádané zprávy obsahující odkazy na svoje webové stránky. Obdržíte-li elektronickou poštou zprávu obsahující takový odkaz, nereagujte na ni a informujte prosím Zákaznický servis Banky. Pokud máte podezření, že bylo Vaše heslo nebo PIN prozrazeno, kontaktujte Zákaznický servis Banky a požádejte o zablokování IB.

Buďte všímaví – neváhejte kontaktovat Banku v případě jakýchkoliv pochybností a podivného chování počítače při přístupu do IB nebo k jiným službám. Podezřelé chování může být např. nepřicházející SMS kódy, jiné údaje o platbě v SMS kódu, "divné" jméno serveru, jiný vizuální dojem, nové kroky během přihlášení (zvláště pokud by požadovaly SMS kód nebo PIN), apod. Pokud si nevíte rady, kontaktujte Zákaznický servis Banky.

5. DOPORUČENÉ POSTUPY A NASTAVENÍ

Doporučujeme pravidelně měnit Přístupové heslo do IB a PIN. Při jejich tvorbě nepoužívejte snadno odhadnutelné informace, jako jsou jména, data narození, telefonní čísla apod.

Své Přístupové heslo do IB a PIN nikomu nesdělujte a zabraňte odpozorování při jejich zadávání.

Certifikát sloužící k ověřování Uživatelovi identity je umístěn na Certifikačním Tokenu, jehož specifikace znemožňuje bez použití správného PINu jeho zneužití. Pro správnou funkčnost tohoto zařízení je nutné, aby na počítači byly nainstalované aplikace umožňující čtení dat z jeho paměti. Toto de facto také brání tomu, aby byl Certifikační Token jednoduchým způsobem používán na cizích nebo veřejných počítačích. Nezapomeňte si pravidelně alespoň jednou ročně obnovovat Certifikát. Certifikát je vždy vydáván s platností jednoho roku. V případě, že Uživatel neprovede včas jeho obnovu, je mu znemožněn jakýkoliv přístup do IB. Uživatel nebo Klient se v takovém případě musí dostavit do Obchodního místa banky a vyžádat pro Uživatele nové přístupové jméno a heslo do Certifikačního centra pro vygenerování nového Certifikátu.

V případě ztráty Tokenu nebo ztráty mobilního telefonu, na který je zasílán SMS kód, ihned kontaktujte Banku a nechte Uživateli zablokovat přístup do IB.

Nainstalujte si antivirový software a pravidelně (nejméně jednou týdně) provádějte jeho aktualizaci. Nainstalujte si antispyware software a pravidelně (nejméně jednou týdně) provádějte jeho aktualizaci. Doporučujeme chránit počítač programy typu "Personal firewall“.

Při použití antivirového programu věnujte pozornost případným změnám v systémových souborech, projeví se zde útoky typu “trojský kůň“ (vir importovaný např. souborem připojeným k e-mailu).

PPF banka a.s., Praha 6, Evropská 2690/17, PSČ 160 41 Česká republika, IČ 47116129, DIČ CZ47116129
Společnost zapsaná v Obchodním rejstříku vedeném městským soudem v Praze, oddíl B, vložka 1834
Tel.: (+420) 224 175 888, fax: (+420) 224 175 980

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; před odchodem od počítače vždy uzamkněte obrazovku nebo ukončete všechna spojení s IB. Token bezpečně uložte. Mobilní telefon pro zasílání SMS kódů mějte vždy při sobě.

Nedoporučujeme instalovat software získaný z nedůvěryhodných zdrojů (veřejné knihovny SW, přílohy v elektronické pošty apod.). Zejména nelegálně získaný SW může obsahovat tzv. "trojské koně" a Vaše hesla odesílat autorovi těchto (nelegálně upravených) programů. Věnujte zvýšenou pozornost příjmu elektronické pošty s přílohami – viry šířené tímto způsobem často obsahují tzv. "zloděje hesel".

Instalujte důležité aktualizace (pro operační systém a další software od společnosti Microsoft: http://windowsupdate.microsoft.com).

Pamatujte, že umožníte-li komukoliv přístup ke svým osobním údajům nebo Bezpečnostním prvkům, dáváte takové osobě možnost tato data zneužít nebo sdělit je další osobě.

Jako jistá prevence zneužití pak může sloužit i nastavení:

- různých Limitů pro zadávání Platebních příkazů (transakčních, časových nebo jejich kombinací),
- zasílání oznámení o vybraných událostech – zejména oznámení o přihlášení Uživatele do IB, případně i o provedených transakcích na BÚ.

PPF banka a.s., Praha 6, Evropská 2690/17, PSČ 160 41 Česká republika, IČ 47116129, DIČ CZ47116129
Společnost zapsaná v Obchodním rejstříku vedeném městským soudem v Praze, oddíl B, vložka 1834
Tel.: (+420) 224 175 888, fax: (+420) 224 175 980