PPF Banka

BEZPEČNOSTNÍ ZÁSADY PRO HOMEBANKING PPF banky a.s.

Obsah:

1. ZABEZPEČENÍ PŘÍSTUPU DO HB A AUTORIZACE 2
2. OBECNÉ BEZPEČNOSTNÍ ZÁSADY 2
3. BEZPEČNOSTNÍ ZÁSADY PRO POUŽÍVÁNÍ HOMEBANKINGU 2
4. PHISHING 3
5. DOPORUČENÉ POSTUPY A NASTAVENÍ 3

Následující dokument popisuje zásady pro bezpečný provoz Homebankingu (dále jen „HB“) PPF banky a.s. (dále jen „Banka“). Doporučujeme řídit se všemi těmito zásadami na všech počítačích, na kterých bude HB 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 HB, Bezpečnostních zásadách, Bezpečnostních prvcích nebo aktuálních bezpečnostních hrozbách můžete nalézt na stránkách Banky, v HB nebo je získat v Obchodních místech Banky, na telefonním čísle +420 224 175 995 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 Homebankingu* (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 HB je poskytována Zákaznickým servisem, který můžete kontaktovat v Pracovních dnech od 8:00 do 18:00 na telefonním čísle +420 224 175 955 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. ZABEZPEČENÍ PŘÍSTUPU DO HB A AUTORIZACE

Způsob přihlašování Uživatele do HB nastavuje Systémový administrátor ve správě HB. Doporučujeme nastavit přístup s použitím Bezpečnostních prvků zajišťujících autentizaci (ověření identity) Uživatele a omezujících zneužití přístupu do HB – Uživatelské jméno do HB v kombinaci s Přístupovým heslem do HB.

Platební příkazy a žádosti pro Banku je vždy nutné Autorizovat s použitím Elektronického podpisu. Elektronický podpis představuje šifrované údaje v elektronické podobě, které jsou připojené k předávaným datům a které umožňují ověření identity Uživatele. Skládá se z Podpisového certifikátu a Podpisového klíče. Uživatel musí při Autorizaci rovněž zadat Heslo k Podpisovému klíči.

2. OBECNÉ BEZPEČNOSTNÍ ZÁSADY

Doporučujeme využít možnosti nastavení Limitů pro Platební příkazy, a to pro všechny Uživatele HB (více o Uživatelích, nastavení Limitů a Autorizačních oprávnění naleznete v KOP).

Bezpečnostní prvky uchovávejte na bezpečném místě.

Cílem zneužití se může stát i *Smlouva o Homebankingu* a její přílohy (dále jen „Smlouva o HB“). 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 by měl Systémový administrátor neprodleně zablokovat přístupy Uživatelům do HB. Následně kontaktujte Zákaznický servis Banky a požádejte o zablokování HB nebo přístupů do HB i na straně Banky.

3. BEZPEČNOSTNÍ ZÁSADY PRO POUŽÍVÁNÍ HOMEBANKINGU

Zabezpečení systému HB je tak silné, jak silný je jeho nejslabší článek. Systém HB se skládá ze serverů Banky, telekomunikačních prostředků pro spojení s Bankou a přeno dat (modem, internet apod.), Uživatelova počítače a lidského faktoru.

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

Další dva články – Uživatelův počítač a telekomunikační prostředky pro spojení s Bankou a přenos dat – jsou potenciálně nejzranitelnější místa celého systému, protože za jejich zabezpečení nemůže a neodpovídá Banka, ale pouze sám Klient, resp. Uživatel.

Samotný přenos dat z počítače Uživatele do Banky a naopak je prováděn zabezpečeným kanálem (128 bit SSL), samotná data jsou navíc chráněna šifrováním (algoritmus RSA – 1024 bitů) a dalšími ochrannými prvky, aby byla zajištěna co nejvyšší úroveň zabezpečení.

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), kopírování souborů (certifikátu). 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 HB (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 (certifikát, heslo). Každý Uživatel by si měl být vědom citlivosti všech údajů, které slouží k ověřování jeho identity v souvislosti s používáním HB, a za žádných okolností tyto údaje nesdělovat. Banka za žádných okolností nebude po Uživateli vyžadovat sdělení těchto údajů mimo jejich zadávání do HB.

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

4. PHISHING

Využívejte pouze důvěryhodných služeb a vždy se ujistěte, že opravdu komunikujete se správným poskytovatelem služeb. Jestliže si nejste jisti, zda opravdu komunikujete s Bankou, obraťte se na Zákaznický servis Banky.

Hesla související s HB 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 jeho 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 prozrazeno, kontaktujte Zákaznický servis Banky a požádejte o zablokování HB.

Buďte všímaví – neváhejte kontaktovat Banku v případě jakýchkoliv pochybností a podivného chování počítače při přístupu do HB nebo k jiným službám. Pokud si nevíte rady, kontaktujte Zákaznický servis Banky.

5. DOPORUČENÉ POSTUPY A NASTAVENÍ

Doporučujeme pravidelně měnit Přístupové heslo do HB (viz bod 1.). Při jejho tvorbě nepoužívejte snadno odhadnutelné informace, jako jsou jména, data narození, telefonní čísla apod.

Svá hesla nikomu nesdělujte a zabraňte odpozorování při jejich zadávání.

Podpisový certifikát je vhodné uložit na přenosný nosič dat (např. USB), který může mít Uživatel pod vlastní kontrolou. Po ukončení práce s HB je vhodné tento nosič uložit na bezpečné místo.

Platnost Podpisového certifikátu je jeden rok. Před koncem nebo po uplynutí jeho platnosti Uživatel musí požádat o vygenerování nového Podpisového certifikátu. Pokud Uživatel nepožádá o vygenerování nového Podpisového certifikátu, bude mu znemožněno Autorizování Platebních příkazů a dalších zpráv zasílaných Bance.

Platnost Transportního certifikátu, který je nutný pro příjem zpráv z Banky, je rovněž jeden rok. Před koncem nebo po uplynutí jeho platnosti Systémový administrátor musí požádat o vygenerování nového Transportního certifikátu. Pokud Systémový administrátor nepožádá o vygenerování nového Transportního certifikátu, nebude možné prostřednictvím HB přijímat šifrované zprávy a informace z Banky (výpisy z účtů, informace o zúčtovaných transakcích atd.).

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).

Pro běžnou práci, zejména při práci s internetem, nepoužívejte uživatelský profil s administrátorskými právy.

Neumožňujte jiné osobě, aby se přihlašovala do HB prostřednictvím Vašeho uživatelského profilu; před odchodem od počítače vždy uzamkněte obrazovku nebo ukončete aplikaci HB.

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".

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

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).

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