

## **NEDÁVEJTE ŠANCI PODVODNÍKŮM**

Na důvěrná data se Vás nikdy aktivně neptáme telefonicky nebo e-mailem. To znamená, že banka sama neoslovuje klienty telefonicky či prostřednictvím elektronické nebo jiné pošty a nevyzývá klienty k tomu, aby jí poskytli důvěrná data.

Identifikační prvky po Vás vyžadujeme pouze tehdy, pokud si ověřujeme, že jste oprávněni provést určitý obchod (například při přihlášení do systému telefonního bankovníctví vyžadujeme PIN a náhodně generované znaky z hesla; podobně může banka například požádat o další autorizaci platby kartou. Vždy se však jedná o případy, kdy aktivně provádíte transakci).

To je základní pravidlo bezpečné komunikace, které Vám pomůže rozpoznat, že se někdo může pokusit vylákat z Vás důležité osobní informace a získat tak přístup k Vašemu účtu.

Podvodné e-maily a internetové stránky dokáží působit skutečně velmi věrohodně, ale jedná se o tzv. phishing – tedy pokus „vylovit“ důvěrná data a poté je zneužít.

Chceme Vás upozornit také na jiný typ podvodných transakcí, které mohou směřovat ke zneužití Vašeho účtu pro legalizaci výnosů z trestné činnosti (tzv. praní špinavých peněz), což je problematika, které KB věnuje velkou pozornost. Někteří podvodníci se mohou pokusit přesvědčit Vás, pod záminkou snadného zisku, abyste poskytli svůj účet právě k těmto účelům, aniž byste byli o těchto zločinných záměrech informováni.

Jedinou možností, jak se takového rizika vyvarovat, je neodpovídat na e-maily, které vám slibují procento ze zisku, pokud přijmete peníze na svůj účet, poté je v hotovosti vyzvednete a rovněž v hotovosti odešlete na určenou adresu, zpravidla do některé ze zemí bývalého Sovětského svazu. V případě, že se do takové aktivity zapojíte, vystavujete se riziku trestního stíhání a pochopitelně i možného zneužití Vašich údajů.

### **Na co je třeba dát si pozor?**

- Na emaily či telefonáty, ve kterých se od Vás údajný zaměstnanec banky snaží získat data jako je PIN, heslo, certifikát a jeho uložení a podobně. Může při tom uvádět velmi vážné důvody, jako je stoplistace platební karty, zablokování účtu, nesrovnalosti v interní dokumentaci, připsání značného finančního obnosu a podobně. Takto se banka ale nikdy nechová a každý takový požadavek je vždy podezřelý! V některých případech je sice možné, že Vám zavolá Váš bankovní poradce a bude se dotazovat na důvod konkrétní transakce na Vašem účtu, ale nikdy po Vás nebude požadovat sdělení PIN, hesla, certifikátu a podobně.
- Objeví-li se ve Vaší elektronické poště e-mail, který na základě předchozí informace identifikujete jako podezřelý, nikdy na něj neodpovídejte. Podvodné emaily mohou obsahovat odkaz na podvrženou internetovou stránku, kde po Vás může být požadován PIN, certifikát a Vaše osobní údaje. Tato stránka

může vypadat zcela autenticky, ale nenechte se zmýlit. Touto cestou nikdy nepostupujeme.

- K internetovému bankovníctví KB MojeBanka se připojujte pouze prostřednictvím adresy [www.mojebanka.cz](http://www.mojebanka.cz) nebo [www.kb.cz](http://www.kb.cz). Provádění aktivních operací v aplikaci MojeBanka pomocí osobního certifikátu v souboru je nyní také podmíněno dodatečnou autorizací pomocí autorizačního SMS kódu zasláného na Váš mobilní telefon.

Zasílání upozornění o blížícím se ukončení platnosti osobního certifikátu

Snahou KB je maximálně chránit klienty před možným zneužitím osobních a důvěrných informací, a proto jsme také přistoupili ke změně režimu zasílání e-mailových upozornění o blížícím se konci platnosti osobního certifikátu.

Tyto e-maily neobsahují aktivní odkaz na aplikaci Certifikační průvodce. To znamená, že banka Vás prostřednictvím e-mailu upozorní na konec platnosti Vašeho certifikátu. Budete-li s ním chtít dále pracovat, otevřete si sami stránku, odkud si bezpečně spustíte aplikaci Certifikační průvodce.

Pro práci s certifikáty (např. vyzvednutí certifikátu, prodloužení platnosti certifikátu, apod.) používejte pouze aplikaci Certifikační průvodce, kterou si spustíte ze stránky [www.mojebanka.cz](http://www.mojebanka.cz).

Jak postupovat v případě, že jste dostali podezřelý e-mail, nebo se někdo pokusil vylákat z Vás důvěrné informace telefonicky?

Především nikdy na takový kontakt nereagujte, a to ani tehdy, když bude vyhrožovat zrušením účtu, karty nebo třeba peněžní ztrátou, či sankcí. Neprodleně, prosím, v takovém případě kontaktujte Klientskou linku Komerční banky na čísle +420 955 551 552.

## Důležitá pravidla pro bezpečné používání internetového bankovníctví

### 1. Chraňte svůj osobní certifikát

Osobní certifikát nahrazuje Váš vlastnoruční podpis a je tedy „přístupovým klíčem“ k Vaším účtům a financím. Proto chraňte svůj osobní certifikát proti zneužití třetími osobami. Doporučujeme Vám uchovávat osobní certifikát na přenosném médiu (např. na USB disku, disketě nebo CD) a tyto nosiče mít pod kontrolou na bezpečném místě.

Upozorňujeme, že pokud přes přímé bankovníctví obsluhujete jak své osobní účty, tak firemní nebo jiné než Vaše účty, ke kterým máte zmocnění (např. jako zaměstnanec firmy) používáte v obou případech stejný certifikát. Sdílením tohoto certifikátu v rámci firmy byste tak porušili podmínky bezpečnosti a umožnili jiným osobám přístup i na Vaše osobní účty.

Pro zvýšení bezpečnosti uložení Vašeho osobního certifikátu nabízíme využití čipové karty MůjKlíč.

## **2. Nepoužívejte jednoduché heslo / PIN**

Jednoduché heslo nebo PIN se dá snadněji rozluštit a zneužít. Nepoužívejte proto slova a čísla, která mají souvislost se jmény rodinných příslušníků, jejich datem narození, jejich telefonním číslem, apod. U hesla doporučujeme zvolit kombinaci velkých a malých písmen, číslic a speciálních znaků (tečka, vykřičník, otazník atd.). Heslo by mělo mít minimálně osm znaků.

PIN k čipové kartě Můjklíč si zvolte odlišný od ostatních PINů.

## **3. Ochraňujte své heslo / PIN**

Heslo nebo PIN si nezaznamenávejte na poznámkové papírky, do diářů, do telefonů, na čipovou kartu apod. V žádném nastavení počítače nepovolujte zapamatování hesel.

Dodržujte zásadu, že hesla se nikomu nesdělují, a to ani rodinným příslušníkům, kolegům v práci!

## **4. Nastavte si zaslání zpráv**

Doporučujeme Vám nastavit si zaslání zpráv (SMS nebo e-mail), které Vás budou informovat o veškerých platbách provedených z Vašeho účtu nebo platební karty. Nastavení snadno zvládnete v internetovém bankovníctví MojeBanka a Expresní linka Plus v menu Nastavení oznámení. Autorizační SMS obsahují informace o transakci, vždy při autorizaci tyto informace kontrolujte. Rovněž Vám doporučujeme sledovat přehled historie přihlašování, který aplikace MojeBanka a Expresní linka Plus nabízejí.

Komerční banka může zasílat i nevyžádané SMS zprávy související s vymáháním pohledávek. Tyto zprávy jsou zasílány z následujících SMS bran: 991051, 99061 (Telefonica O2), 5270 (T-Mobile) a 65430 (Vodafone). Pokud obdržíte nevyžádanou SMS z jiné SMS brány, neváhejte prosím kontaktovat klientskou podporu KB na lince +420 955 551 552.

## **5. Pravidelně aktualizujte operační systém a veškeré programové vybavení**

Pravidelně instalujte aktualizací soubory, které odstraňují chyby a zranitelnosti programového vybavení a snižují bezpečnostní rizika. Používejte pouze legálně nabyté programové vybavení, jehož výrobce vám garantuje podporu ve formě pravidelných bezpečnostních aktualizací.

Na adrese [www.microsoft.com/cze/athome/security/default.msp](http://www.microsoft.com/cze/athome/security/default.msp) jsou popsány základní kroky k zabezpečení nejrozšířenějšího operačního systému Windows.

## **6. Používejte svůj počítač**

K využívání služeb přímého bankovníctví doporučujeme používat pouze svůj domácí, příp. firemní počítač. Neumožňujte práci s Vaším počítačem neznámé osobě. Svůj počítač zabezpečte vždy, když s ním právě nepracujete. Po dobu krátké nepřítomnosti ho uzamkněte klávesovou zkratkou Win + L, v případě dlouhodobé nepřítomnosti počítač vypněte. S počítačem pracujte pod účtem neprivilegovaného uživatele (user), práce s vyššími oprávněními

(Administrator, root), umožňující instalaci programového vybavení, je bezpečnostním rizikem.

## **7. Používejte programy, které chrání Váš počítač, jako jsou antivirové programy, anti-spywarové programy a osobní firewally**

Vždy mějte na svém počítači nainstalovaný antivirový program, který zvyšuje ochranu před škodlivými programy (viry, červi, trojskými koni). Stejně tak je vhodné používat anti-spywarový program, který zvyšuje ochranu Vašeho soukromí. Veškeré programové vybavení udržujte aktuální, včetně virových a spywarových definic.

**TIP:** Někteří výrobci software nabízejí antivirové programy pro domácí využití zdarma.

K minimalizaci rizika neoprávněného přístupu na Váš počítač během připojení k internetu slouží tzv. osobní firewall. Jedná se o programové vybavení nebo samostatné zařízení, které dokáže odlišit oprávněné a neoprávněné požadavky na datovou výměnu mezi Vaším počítačem a internetem.

**TIP:** Některé operační systémy jako Windows XP a Linux obsahují vestavěný osobní firewall. Lze ale využít i široké nabídky výrobců, z nichž někteří nabízejí firewally pro domácí použití zdarma.

## **8. Nenavštěvujte neznámé stránky a nestahujte z internetu neznámé soubory**

Navštěvujte na internetu pouze známé a důvěryhodné stránky. Stránky, kterým jejich tvůrci nevěnují patřičnou péči jsou nejčastějším zdrojem nákazy Vašeho počítače. Vyvarujte se také stahování a spouštění souborů s neznámým obsahem, které mohou společně se svým proklamovaným účelem vykonávat činnost, ke které nejsou oprávněny (trojské koně, spyware).

**TIP:** Především stránky s erotickým obsahem a stránky distribuující nelegální software mnohdy obsahují škodlivé programy, které mohou infikovat Váš počítač a následně provádět činnost, kterou nemáte pod kontrolou.

Kontrolujte na přihlašovací stránce řádek pro zadání internetové adresy. Vždy se přesvědčte, že se jedná opravdu o stránku, kterou požadujete zobrazit. Před samotným přihlášením poklepejte na ikonu zámku buď v pravé dolní části okna prohlížeče nebo vedle řádku pro zadání internetové adresy (dle typu prohlížeče), a ověřte, že certifikát zabezpečující připojení byl vydán pro [www.mojebanka.cz](http://www.mojebanka.cz).

**TIP:** Jakákoliv změna vzhledu přihlašovací stránky portálu [www.mojebanka.cz](http://www.mojebanka.cz) je zákazníkům předem komunikována. Pokud narazíte na podezřelé chování nebo neobvyklý vzhled, neváhejte prosím kontaktovat klientskou podporu KB na lince +420 955 551 552

## **9. Otvírejte pouze důvěryhodné e-maily**

Neotvírejte e-mailové zprávy od adresátů, které neznáte nebo zprávy, které mají podezřelý název obsahující zkomolená slova, nezvyklé slovní obraty

a pravopisné chyby. Nepracujte s přílohami takovýchto zpráv a raději je smažte.

Nesděľujte osobní údaje, hesla či kódy PIN formou e-mailu. Komerční banka, a. s. tyto údaje nikdy nepožaduje.

Komerční banka, a. s. nezasílá nevyžádané e-maily s odkazy na internetové adresy. V případě, že obdržíte nevyžádaný e-mail obsahující internetový odkaz na stránky Komerční banky, na e-mail nereagujte a na odkaz neklikujte. Kontaktujte naši klientskou podporu KB na lince +420 955 551 552 a poskytněte nám bližší informace o podezřelé zprávě, abychom mohli podniknout příslušné kroky.

### **10. Kontaktujte nás při jakýchkoliv pochybnostech**

Pokud budete mít jakékoliv pochybnosti při přihlašování nebo práci s bankovním účtem prostřednictvím internetového bankovníctví, kontaktujte prosím neprodleně klientskou podporu KB na lince +420 955 551 552. Nevyžádaný e-mail obsahující internetový odkaz na stránky Komerční banky, na e-mail nereagujte a na odkaz neklikujte.

### **Ochrana podpisových vzorů**

Nedostatečně chráněný nebo nevhodně zvolený podpisový vzor může být zneužitý podvodníky k provádění podvodných platebních transakcí z Vašeho účtu. Proto je nezbytné dodržovat maximální obezřetnost při jeho výběru, uchování a používání.

Nikomu nepředávejte Váš podpisový vzor k účtům, a to ani v případě, kdy Vám jiná osoba nabídne, že na základě jeho uvedení pro Vás zajistí jakékoliv služby.

Doporučujeme, abyste používali odlišný podpisový vzor, než jakým se běžně podepisujete, nebo který je v souvislosti s Vaší obchodní společností veřejně dostupný například v obchodním rejstříku. Navíc doporučujeme doplnit jej o číselný nebo textový údaj, který je znám výlučně jen Vám.

Bezpečnost autorizace operací na pobočce (např. výběr hotovosti) je možno významně zvýšit použitím karty optického klíče (OPK).