



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 nebo 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 www.mojebanka.cz, 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.

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 bezplatnou klientskou linku Komerční banky na čísle 800 152 152.

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. 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!

4. Nastavte si zasílání zpráv

Doporučujeme Vám nastavení zasílání 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 mojobanka a Expresní linka Plus.

5. Pravidelně aktualizujte operační systém

Pravidelně instalujte aktualizací soubory, které odstraňují některé chyby či bezpečnostní rizika. Aktualizační soubory jsou zdarma k dispozici na domovských webových stránkách výrobců operačních systémů. Pokud používáte operační systém Windows, můžete navštívit například adresu <http://www.microsoft.com/cze/security/protect/>, kde jsou popsány základní kroky k zabezpečení Vašeho systému.

6. Používejte svůj počítač

K využívání služeb přímého bankovníctví doporučujeme používat pouze svůj domácí, příp. firemní počítač. Neumožňujte práci s Vaším počítačem neznámé osobě. Před každým odchodem od počítače použijte CTRL+ALT+DEL pro uzamknutí počítače, nebo u starších operačních systémů si aktivujte spořič obrazovky chráněný heslem.

K využívání služeb přímého bankovníctví nedoporučujeme používat počítač, o kterém nic nevíte (např. počítač v internetové kavárně).

7. Používejte antivirový a anti-spyware program

Vždy mějte na svém počítači nainstalovaný antivirový program, který zvyšuje ochranu před škodlivými programy - viry. Stejně tak je vhodné používat anti-spyware program (např. Ad-aware, Spybot), který zvyšuje ochranu před sledováním Vaší činnosti na PC pomocí parazitních programů. Antivirový a anti-spyware program pravidelně aktualizujte.



KB

8 Připojte se k internetu přes firewall

K minimalizaci rizika neoprávněného přístupu na Váš počítač při připojení k internetu slouží tzv. firewall. Jedná se o ochranný program nebo technické zařízení, které zpracovává pouze Vámi zadané dotazy do sítě internet a všechna ostatní příchozí (potencionálně nebezpečná) data odfiltruje. U Windows XP lze zaktivovat firewall, který je součástí operačního systému. Osobní firewall lze zakoupit a stáhnout například z www.sunbelt-software.com, www.symantec.com nebo www.agnitum.com.

9. Nestahujte z internetu neznámé soubory

Navštěvujte na internetu pouze známé a důvěryhodné stránky. Vyvarujte se stahování neznámých souborů z internetu na Váš počítač, které mohou společně se svým původním účelem nainstalovat i nebezpečné programy.

10. Otvírejte pouze důvěryhodné e-maily

Neotvírejte e-mailové zprávy od adresátů, které neznáte nebo zprávy, které mají podezřelý název či obsah. Nespouštějte přílohy takovéto e-mailové zprávy a zprávu bez otevření smažte. Nesdělujte osobní údaje, hesla či kódy PIN formou e-mailu. Komerční banka tyto údaje nikdy nepožaduje. Komerční banka rovněž 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

Ochrana podpisových vzorů

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. Navíc máte možnost jej doplnit 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).