**Zásady bezpečného užívání elektronického bankovnictví**

1. Chraňte si své identifikační číslo a PIN pro přístup do elektronického bankovnictví. Identifikační číslo a PIN si nikam nezaznamenávejte. Zcela nevhodný je zápis přihlašovacích údajů do mobilního telefonu, počítače, diáře nebo na papírky (např. nalepené na monitoru či uložené v peněžence). V počítači nikdy nepovolujte zapamatování PIN. PIN nikomu nesdělujte (ani rodinným příslušníkům). Originál obálky s PIN zničte nebo uschovejte na bezpečném místě (např. v trezoru).
2. Nepoužívejte jednoduchý PIN. PIN pro přístup do služby nebo k čipové kartě můžete podle svého přání měnit. Vždy volte PIN, který není jednoduchý a snadno odvoditelný. Zásadně nepoužívejte data narození, části telefonních čísel, po sobě jdoucí číslice apod. Pokud jste delší dobu PIN neměnili, služba vás po přihlášení upozorní, že je vhodné ho změnit.
3. Chraňte svůj mobilní telefon. Necháváte-li si zasílat autorizační kód SMS zprávou, chraňte svůj mobilní telefon, neponechávejte ho bez dozoru a nepůjčujte jej jiným osobám. Používáte-li tzv. „chytrý“ telefon (telefon s operačním systémem iOs, Android, Windows apod.), neinstalujte do něj neznámé aplikace a aktualizace stahujte pouze z důvěryhodných zdrojů.
4. Nepoužívejte „chytré“ telefony pro přístup do elektronického bankovnictví pomocí internetového prohlížeče. To platí zvláště tehdy, je-li vám na stejné telefonní číslo zasílán i autorizační SMS kód. V žádném případě nepovolujte ukládání přihlašovacích údajů do paměti internetového prohlížeče.
5. Zvyšte si zabezpečení autorizačních SMS zpráv – některé banky nabízejí službu zasílání šifrovaných autorizačních a informačních SMS zpráv, jejich přečtení chrání PINem.
6. Při přihlašování na stránkách internetového bankovnictví buďte obezřetní.
7. Chraňte si svůj privátní klíč na čipové kartě. Používáte-li čipovou kartu, mějte na paměti, že elektronický podpis nahrazuje váš vlastnoruční podpis. Proto jej chraňte před zneužitím třetími osobami, neponechávejte svou čipovou kartu bez dozoru a nikomu nesdělujte její PIN ani si ho nikam nezaznamenávejte. Pokud kartu nepoužíváte, uložte ji na bezpečné místo.
8. Chraňte svůj počítač (vč. operačního systému, internetového prohlížeče a instalovaných aplikací). Sledujte a instalujte včas opravy vydávané výrobci softwaru. Snížíte tak riziko zneužití známých chyb útočníky. U operačního systému MS Windows ponechte jeho nastavení po instalaci, které automaticky provádí vyhledání a instalaci oprav.
9. Používejte bezpečný počítač. Pro práci s internetovým bankovnictvím používejte pouze bezpečné počítače, které máte plně pod kontrolou (můžete ovlivnit jejich bezpečnostní nastavení). Za bezpečné počítače se považují domácí a firemní počítače, jejichž systém a aplikace jsou aktualizované a chráněné bezpečnostním SW. V žádném případě nedoporučujeme používat neznámé počítače (např. v internetových kavárnách, hotelech nebo klubech).
10. Chraňte svůj počítač proti virům a spyware. Používejte antivirové a anti-spyware programy. Pravidelně je aktualizujte, aby jejich účinnost byla co nejvyšší.
11. Připojujte se k internetu přes firewall (bezpečnostní zeď). Připojujte se k internetu přes firewall (program nebo technické zařízení), který minimalizuje rizika neoprávněného přístupu k vašemu počítači z internetu. Ponechte aktivován osobní firewall, který je standardní součástí operačního systému Windows XP SP3 a výše.
12. Pozor na nedůvěryhodné e-maily. Neotvírejte e-mail od neznámého adresáta nebo s podezřelým předmětem či obsahem. V žádném případě nespouštějte jeho přílohy a tento e-mail rovnou bez otevření smažte. Nikdy nereagujte na e-mail, který po vás požaduje sdělení vašich osobních údajů, hesla nebo PINu. Banka od vás nebude nikdy vaše údaje touto formou požadovat!
13. Nestahujte z internetu neznámé soubory. Navštěvujte na internetu pouze známé a důvěryhodné stránky. Vyvarujte se stahování neznámých souborů z internetu (zejména s příponou EXE) na svůj počítač. Tyto soubory mohou společně se svým původním účelem nainstalovat na váš počítač i nebezpečné programy.
14. Zvyšte svoji bezpečnost zasíláním zpráv SMS nebo e-mailem. Nastavte si ve službě své banky zasílání zpráv o veškerých operacích na vašem účtu nebo s vaší platební kartou.

(Podle podkladů Dr. Klufy)