Doporučení pro práci s internetovým bankovnictvím

Vzhledem k neustále se zvyšujícímu riziku kybernetických zločinu bychom Vám rádi tímto materiálem připomněli několik základních pravidel pro bezpečnou práci s citlivými daty a informačními systémy zejména internetovým bankovnictvím.

Vytvořte si silné heslo

- Délka minimálně 12 znaků
- Nepoužívat celá slova, pokud je použijete kvůli snazším zapamatování, rozdělte je speciálním znakem či velikostí písmene např. místo JihlavaSkola lze použít jiH-LavaskO!La
- Nepoužívejte notoricky známá či lehce odvoditelná hesla např. 12345, 123456789, heslo, qwertz, qwerty, asdfgh, Kamil, kamil84, kamil1984
- Nikdy nepoužívejte heslo do internetového bankovnictví jako heslo do jiného systému, musí být unikátní. Ideálně co systém to jiné heslo.

Využívejte více faktorovou autentizaci

- používejte minimálně dvoufaktorovou autentizaci v různých zařízeních
- kromě uživatelského jména a hesla například certifikát uložený v kryptografickém HW zařízení (USB token, čipová karta), jednorázové heslo s omezenou platnosti zaslané pomocí SMS na mobilní telefon nebo generované speciálním HW zařízením.

Do banky se přihlašujte pouze z bezpečných prostředí

- přihlašujte se pouze z takových počítačů, nad kterými máte kontrolu
- připojujte se pouze z důvěryhodných sítí, nikdy z veřejné Wifi
- využívejte softwarovou klávesnici buď přímo v aplikaci, nebo v MS Windows dostupné pomocí (Win + U > Spustit funkci Klávesnice na obrazovce)
- na počítači, ze kterého se přihlašujete k internetovému bankovnictví, nepoužívejte nelegální SW, nenavštěvujte rizikové webové stránky

Dávejte pozor na odkazy

- než kliknete na odkaz v emailu nebo otevřete přílohu, zamyslete se, jestli se jedná o důvěryhodný zdroj (odesilatel, elektronický podpis)
- žádná bankovní instituce Vás nikdy nebude žádat o zadání Vašich přístupových údajů nebo o instalaci aplikace prostřednictvím emailu. Takové emaily ihned vymažte.
- při přístupu na portál internetového bankovnictví si vždy kontroluje certifikát zabezpečení stránky. Věnujte pozornost bezpečnostním upozorněním internetového prohlížeče. Kontrolujte přítomnost „zeleného pruhu“ v adresním řádku.

Zabezpečte svůj počítač a udržujte ho aktualizovaný

- bezpečnostním minimem je používání aktualizovaného Antivirového řešení výhodou je používaní dalšího antimalware řešení

- pravidelně aktualizujte nejen operační systém, ale i Vámi používaný software např. Internetový prohlížeč, java, adobe reader,…

Správa bankovního účtu

- nastavte si notifikace o prováděných platbách nebo přihlášení k Vašemu bankovnímu účtu
- pravidelně kontrolujte pohyby na účtu, v případě zjištění podezřelé transakce ihned kontaktujte banku
- pro ukončení práce v internetovém bankovnictví se vždy korektně odhlaste. Po odhlášení zavřete internetový prohlížeč
- před a při práci v internetovém bankovnictví mějte spuštěné jen nezbytné aplikace. Ukončete zejména aplikace IM (Skype, ICQ), odpojte se ze sociálních sítí (Facebook) atd.