

# DESATERO BEZPEČNÉHO POUŽÍVÁNÍ INTERNETBANKINGU



1. Internetbanking je jako vaše peněženka, kterou si chráníte. Proto dopřejte i svému internetovému bankovníctví a počítači obecně ochranu před napadením pomocí spolehlivého a aktuálního antivirového programu.
2. Přístupové heslo do Internetbankingu je vaším osobním tajemstvím. Chovejte ho v tajnosti a nesdělujte jej ani nejbližším osobám.
3. Čím složitější heslo bez vazby na vaši osobu zvolíte, tím obtížnější je jeho prolomení. Kombinujte číslice, malá a velká písmena a zvláštní znaky. Vyhněte se osobním jménům, přezdívkám či osobně významným datům jako jsou např. narozeniny, rodné číslo apod.
4. Riziko zachycení vstupního hesla můžete podstatně snížit používáním grafické klávesnice při jeho zadávání. Použití grafické klávesnice doporučujeme především v okamžiku, kdy se do Internetbankingu přihlašujete na veřejně přístupném zařízení.
5. Jedno z největších rizik pro váš Internetbanking představují útoky prostřednictvím tzv. malware, nebo-li škodlivého softwaru. K jeho průniku na váš počítač může dojít mimo jiné tím, že dáte souhlas k instalaci aplikace neznámého původu.
6. Škodlivý software cílící na data z vašeho počítače se nejčastěji maskuje jako užitečná aplikace nebo počítačová hra zdarma. Jeden z posledních útoků byl veden prostřednictvím aplikace, která se vydávala za nástroj pro sledování poštovních zásilek.
7. Dalším rizikem skrývající škodlivý software jsou podezřelé emaily, které se mohou tvářit například jako upomínka, falešný příkaz k exekuci či zpráva o výhře v loterii. E-mail představuje pro bezpečnost vašeho počítače jedno z největších rizik a je třeba obezřetnosti při otevírání jeho příloh. Škodlivý software cílící na data z vašeho počítače se může ukrývat právě v příloze emailu nebo pod odkazem na webovou stránku.
8. Každá výzva k povolení instalace nové aplikace představuje potenciální riziko proniknutí škodlivého softwaru na váš počítač. Povolujte instalaci jen těm aplikacím, o jejichž původu a účelu nemáte žádné pochybnosti.
9. Obáváte se, že by vaše platební karta mohla být zneužita k transakci na internetu? Řešení je jednoduché a rychlé: nastavte na vaší kartě nulový limit pro internetové platby a pouze v případě vlastní potřeby jej dočasně navyšte. Po uskutečnění transakce limit zase snižte na nulu. Změnu limitů lze provádět v Internetbankingu online a zdarma!
10. Platby na internetu musí být vždy potvrzeny CVC kódem, který je uveden na zadní straně vaší platební karty. Pokud se obáváte zneužití platební karty na internetu v případě, že by se dostala do cizích rukou, doporučujeme tento kód z rubu karty odstranit a uchovávat jej, stejně jako váš PIN, jen ve své paměti.