

DESATORO BEZPEČNÉHO POUŽÍVANIA INTERNETBANKINGU



1. Internetbanking je ako vaša peňaženka, ktorú si chránite. Preto doprajte aj svojmu internetovému bankovníctvu a počítačom všeobecne, ochranu pred napadnutím pomocou spoľahlivého a aktuálneho antivírusového programu.
2. Prístupové heslo do Internetbankingu je vaším osobným tajomstvom. Spravujte ho v tajnosti a nezverejňujte ho ani najbližším osobám.
3. Čím zložitejšie heslo bez väzby na vašu osobu zvolíte, tým ťažšie je jeho prelomenie. Kombinujte čísllice, malé a veľké písmená a špeciálne znaky. Vyhýbajte sa osobným menám, prezývkam či osobne významným dátam ako sú napr. narodeniny, rodné číslo apod.
4. Riziko zachytenia vstupného hesla môžete podstatne znížiť používaním grafickej klávesnice pri jeho zadávaní. Použitie grafickej klávesnice odporúčame predovšetkým v okamihu, kedy sa do Internetbankingu prihlasujete na verejne prístupnom zariadení.
5. Jedno z najväčších rizík pre váš Internetbanking predstavujú útoky prostredníctvom tzv. Malware, resp. škodlivého softvéru. K jeho prieniku na váš počítač môže dôjsť okrem iného tým, že dáte súhlas k inštalácii aplikácie neznámeho pôvodu.
6. Škodlivý softvér zacielený na dáta z vášho počítača sa najčastejšie maskuje ako užitočná aplikácia alebo počítačová hra zadarmo. Jeden z posledných útokov bol vedený prostredníctvom aplikácie, ktorá sa vydávala za nástroj pre sledovanie poštových zásielok.
7. Ďalším rizikom skrývajúcim škodlivý softvér sú podozrivé emaily, ktoré sa môžu tváriť napríklad ako upomienka, falošný príkaz na exekúciu alebo správa o výhre v lotérii. E-mail predstavuje pre bezpečnosť vášho počítača jedno z najväčších rizík a je potrebná obozretnosť pri otváraní jeho príloh. Škodlivý softvér zacielený na dáta z vášho počítača sa môže ukrývať práve v prílohe emailu alebo pod odkazom na webové stránky.
8. Každá výzva k povoleniu inštalácie novej aplikácie predstavuje potenciálne riziko preniknutia škodlivého softvéru na váš počítač. Povoľujte inštaláciu len tým aplikáciám, o ktorých pôvode a účele nemáte žiadne pochybnosti.
9. Obávate sa, že by vaša platobná karta mohla byť zneužitá k transakcii na internete? Riešenie je jednoduché a rýchle: nastavte na vašej karte nulový limit pre internetové platby a iba v prípade vlastnej potreby ho dočasne navýšte. Po uskutočnení transakcie limit zase znížte na nulu. Zmenu limitov možno vykonávať v Internetbankingu online a zadarmo!
10. Platby na internete musia byť vždy potvrdené CVC kódom, ktorý je uvedený na zadnej strane vašej platobnej karty. Ak sa obávate zneužitia platobnej karty na internete v prípade, že by sa dostala do cudzích rúk, odporúčame tento kód z rubu karty odstrániť a uchovávať ho, rovnako ako váš PIN, len vo svojej pamäti.