

MAGYAR BANKSZÖVETSÉG
SAJTÓKÖZLEMÉNY

2012. december 15.

A Bankszövetség figyelemfelhívása az év végén megnövekvő pénzforgalom biztonságára érdekében

Régóta tudjuk, hogy az ünnepi időszakban érdemes fokozottan odafigyelni **készpénzes fizetéseink** során, hogy a forgalmas bevásárló helyeken elkerüljük, hogy zsebtolvajok, csalók áldozataivá váljunk.

Ugyancsak fontos, hogy elővigyázatosan használjuk **bankkártyánkat**, mind a fizetések, mind a készpénzfelvételek alkalmával. Érdemes alkalmazni a sokat emlegetett SMS kontrollt, és arra is odafigyelni, hogy a PIN kód beütésekor takarjuk el kezünket.

Emellett ne feledkezzünk el az az óvatosságról az internetes fizetések és az internetbank használata során sem! Számítógépes bűnözők – Európában és most már hazánkban is – egy új módszerrel próbálják meg a banki ügyfelek számláit jogosulatlanul használni. A módszer szerint a számítógépes bűnözők a nem megfelelő védelemmel rendelkező ügyfelek számítógépe, tablet PC-je vagy okostelefonja felett egy kémprogram segítségével átveszik a teljes felügyeletet, miután az ügyfél interneten bejelentkezik. Ezt követően az adott bank logójával ellátott, adategyeztetésre felhívó és az ügyfél türelmét kérő üzenetet jelenítenek meg a számítógép képernyőjén. Mialatt az ügyfél várakozik, a háttérben jogosulatlan pénzáttalásokat kezdeményeznek az ügyfél számlájának terhére.

A visszaélések odafigyeléssel és az internetbanki műveletekre alkalmazott számítógépek megfelelő védelmével (jogtisztaság és biztonsági szempontból folyamatosan frissített operációs rendszer, naprakész vírus és kémprogram védelmi megoldás használata, tűzfal használata, stb.) megakadályozhatóak!

Ezért felhívjuk minden elektronikus csatornát használó ügyfelünk figyelmét, hogy amennyiben az internetbanki szolgáltatás használata során, a szokásostól eltérő működést tapasztal (pl. adategyeztetésre történő felhívás jelenik meg, amely alatt a szolgáltatást nem tudja használni; az üzenetnek furcsa a nyelvezete, azaz hibás magyar nyelvtani szerkezetű, szóhasználatú, a megszokottól eltérő képernyőelem, beviteli mező jelenik meg, a szokásostól eltérő, pl. ismételt SMS kommunikációra történik kísérlet az adott tranzakció hitelesítés során), azonnal szakítsa meg az internetkapcsolatot az adott weboldallal, és vegye fel a kapcsolatot a számlavezető bankjával. Internetbanki műveletek előtt minden esetben győződjön meg arról, hogy való-

ban bankja weboldalán jár-e! Ezt a számítástechnikában járatosabb felhasználók az adott oldal tanúsítványának ellenőrzésével tehetik meg. Ha böngészője tanúsítványhibát jelez, hagyja el az oldalt, és jelezze ezt bankjánál! Fontos, hogy a bankok adategyeztetést kérő üzenetet nem jelenítenek meg honlapjukon, vagy internet banki rendszerükben. Az ilyen kérés szinte bizonyosan csalárd próbálkozás. Javasoljuk továbbá, hogy minden problémás esetben ellenőrizze, illetve szakemberrel ellenőriztesse számítógépét és gondoskodjon a megfelelő vírusvédelmi eszközök alkalmazásáról!

A bankok biztonsági szakértői folyamatosan, magas szinten ellenőrzik a bankfiókok fizikai biztonságát, a bankkártyás és elektronikus banki rendszerek sértetlenségét, biztonságát. Kérjük, Ön is legyen elővigyázatos pénze biztonsága érdekében.