Tanácsok Elektronikus Banki Szolgáltatások Felhasználóinak

Az MBH Bank üzletpolitikájának egyik legfontosabb eleme a biztonság, amelyet szolgáltatásainkban is messzemenően érvényesítünk. Különösen igaz ez az elektronikus úton igénybe vehető szolgáltatásainkra, amelyek használata során biztonságának megőrzése az Ön részéről is körültekintést, elővigyázatosságot tesz szükségessé.

A következőkben néhány rendkívül fontos gyakorlati teendőre, biztonsági szabályra hívjuk fel tisztelt figyelmét:

- Ne válaszoljon olyan - állítólag - a bankjától érkező e-mailekre, amelyekben jelszavának, bankkártyás és egyéb személyes adatainak megadására kérik.
- Bankunk ezen adatokat nem kéri Öntől e-mailben. Amennyiben ilyen tartalmú e-mailt kap, kérjük, azonnal értesítse számlavezető bankját.
- Önre vonatkozó banki információkat Interneten keresztül kizárólag indokolt esetben adjon meg. Amennyiben elektronikus banki szolgáltatást vesz igénybe, ellenőrizze a bank weboldalának eredetiségét. Amennyiben az MBH Netbank (korábban MKB) szolgáltatásunk használata során a megszokottól eltérő megjelenést, vagy azonosítási kérést tapasztal, kérjük, hívja Telebank ügyfélszolgálatunkat a +36 1 373-3399-es, vagy a 06 80 350 350-es telefonszámon.
- A lehető legnagyobb körültekintéssel járjon el banki adatainak megadásakor. Tegye fel magának a kérdést, hogy vajon a webhelyen kért információ megadása indokoltnak tűnik-e az Ön által éppen végzett tevékenység során. Nem indokolt például, hogy egy online aukciós webhelyen jogosítványának / útlevelének számát vagy hitelkártyájának PIN-kódját kérjék Öntől. Amennyiben egy webhelyen vagy emailben indokolatlanul banki adatokra kérdeznek rá, ne válaszoljon.
- Olyan vállalkozások online szolgáltatásait vegye igénybe, amelyeket ismer és megbízhatónak tart. Amennyiben egy weboldalt gyanúsnak talál, esetleg kétségei merülnek fel adatainak biztonságát illetően, kérjük, ne adja meg adatait és hagyja el a weboldalt.
- A kártékony programok ellen Ön úgy tud védekezni, hogy megvásárolja és szakszerűen telepíti a saját gépére a megfelelő jogtiszta szoftvereket. Olyan programokat használjon, melyek a legújabb biztonsági frissítésekkel működnek. Az operációs rendszer (pl. WINDOWS) ilyen irányú karbantartása különösen fontos.
- A megfelelő programok kiválasztása, telepítése során – amennyiben nem rendelkezik szakmai ismeretekkel – ajánlott vírusvédelmi szakember tanácsát, segítségét igénybe venni.
- Mindig legyen frissített vírusadatbázissal működő és aktív vírusirtó, valamint folyamatosan frissített tudásbázison működő kémprogram elhárító (antispyware) a számítógépen.
- Az ingyenes, un. trial vagy freeware programok használatát nem javasoljuk, mivel nem mindig a legfrissebb vírus adatbázissal kerülnek kiadásra.

- Azt ajánljuk, hogy nyilvános helyen, könyvtárban, repülőtéren, internet kávézóban, stb. ne használja azon banki szolgáltatásokat, amelyekhez szükséges megadnia banki adatait, titkos jelszavát.
- A számítógépet használat közben ne hagyja felügyelet nélkül! Ügyeljen rá, hogy a használt gépen nem maradjon Önre vonatkozó érzékeny adat, ezeket gondosan törölje le a gépről („lomtár", vázlatok, elküldött üzenetek, internet cache).
- Használjon nagy biztonságot nyújtó jelszót, amely nem köthető Önhöz, így születési időpontjához vagy családtagjaihoz. Amennyiben lehetséges, válasszon olyan jelszót, amely számok és betűk kombinációja. Ne írja le jelszavát, PIN kódját, és ne adja át őket senkinek!

Amennyiben felmerül Önben a gyanú, hogy a jelszava, PIN kódja illetéktelen kezekbe került, javasoljuk, hogy azonnal változtassa meg!

Ezekkel a biztonsági, karbantartási tevékenységekkel sikeresen meg lehet előzni, hogy az elektronikus banki szolgáltatások használata során Önt kár érje.