Informatikai biztonsági tájékoztatás

Az azonosító és jelszó segítségével Ön a Banknál vezetett értékpapír- és ügyfélszámláinak a megelőző hó utolsó napjára vonatkozó egyenleg adatait anonim módon lekérdezheti a Magyar Nemzeti Bank (MNB) által biztosított elektronikus felületen. Az azonosító, ill. a jelszavak kizárólag az Ön tájékozódási lehetőségének biztosítása érdekében lettek kialakítva, ezért fontos, hogy azokat minden esetben kezelje bizalmasan, más személynek ne adja át, ne tárolja együtt, és legyen tisztában a kockázatokkal és a megelőzéssel, amihez jelen informatikai biztonsági tájékoztatásunk segítséget nyújt Önnek.

Milyen fenyegetésekkel kell szembenézni?

- Külföldi és hazai pénzintézetek ügyfelei ellen is történtek olyan, adathalászatnak (phishing) nevezett csalási kísérletek, amelyek során az elkövetők különböző indokokra hivatkozva megkísérelték az ügyfelektől megtudni titkos azonosítóikat és titkos jelszavaikat (pl. sms-ben, telefonon, e-mailen). Az adathalászat egyik módja a pharming, amely során a csalók a bank nevében e-mail-t küldenek, mellyel a felhasználót a banki weboldalhoz hasonló - hamisított -honlapra csalják, ahol arra próbálják rávenni, hogy adja meg a bejelentkezéshez használt nevét és jelszavát.
- Rosszindulatú (pl. adware, spyware, trójai, stb.) programok a felhasználó figyelmetlenségét, a számítógép sérülékenységeit, vagy a hálózati kommunikációs programjainak (pl. Web böngésző) gyenge pontjait kihasználva közvetlenül beférkőzhetnek a számítógépre. (pl. e-mailben csatolt állományként érkező program, vírus, fájlmegosztó helyekről letöltött állomány formájában)
- Rosszindulatú személy fizikailag hozzáfér a számítógéphez és titokban ártó szándékú programot telepít rá, bizalmas információkat másol le, módosít, vagy titokban billentyűzet figyelő eszközt (keyloggert) csatlakoztat rá, mellyel jelszavakat lophat.

<u>Biztonsági tanácsok számítógép használatához</u>

Számítógép védelme

- Fontos, hogy használjon vírusirtó programot friss (legfeljebb egy hetes, de inkább egy napos) vírusmintával, lehetőleg malware (pl. adware, spyware, trójai, stb.) program eltávolítás lehetőségével.
- A vírusok és egyéb kártékony alkalmazások, valamint a régen frissített rendszer komoly biztonsági kockázatot jelentenek. Tartsa mindig naprakészen a számítógép operációs rendszerét és az Internetes böngészőt is. Ha lehet, a legfrissebb verziót és a legújabb javítócsomagokat telepítse. Béta tesztverziókkal (pl. kereskedelmi forgalomban nem megvásárolható verziókkal) ne bankoljon. Jogtiszta (frissíthető) operációs rendszert és programokat (pl. levelező programot) használjon.
- Az operációs rendszert és a főbb programokat/komponenseket legalább havonta frissítse (a Microsoft rendszerek esetén a hónap második kedd estéjén már elérhetők az aktuális frissítések).
- Használjon aktuális, személyes tűzfalat. (pl. ügyeljen a tűzfal szabályrendszerének aktualizálása, új verzió nyomon követésére).
- Javasoljuk, hogy az alkalmazott böngésző adatbiztonsági beállításait lehetőség szerint a szükséges legnagyobb biztonságot garantáló szintre állítsa be. (Ezt a böngészőben az Eszközök / Internet beállítások / Biztonság menüpontban teheti meg.) Ebben az esetben a program figyelmezteti Önt minden, a böngésző használata során potenciálisan kárt okozó tartalom megnyitása előtt.
- Kezelje óvatosan az ismeretlen forrásból, vagy ismert feladótól, de szokatlan tárggyal vagy szöveggel érkező leveleket. Ne nyissa meg bizonytalan forrású csatolásokat, linkeket stb. Ezzel megelőzheti a rosszindulatú programok bejutását a levelező rendszeren keresztül.
- Ne töltsön le és ne telepítsen kétes eredetű, licence nélküli szoftvereket számítógépére, mert ezeken keresztül hozzáférhetnek adataihoz.

Azonosító, titkos adatok kezelése

- Ne ossza meg illetéktelen személyekkel azonosítóit és jelszavait.
- Az MBH Bank e-mailen soha nem kéri személyes adatait, azonosító kódjait és nem kéri fel ezek módosítására. Ha ilyen üzenetet kap, kérjük, ne reagáljon rá és mielőbb értesítse bankunkat. Az ilyen – adategyeztetésre felszólító - levélben szereplő link hamis weboldalra továbbíthatja, így ne kattintson a linkre! Még ha nem is adja meg a kért adatokat, egyszerűen a linkre való kattintással lehetővé teszi a tolvaj számára, hogy hozzáférjen az Ön számítógépéhez, és figyelje az Ön által leütött billentyűket és jelszavakat, amikor a különböző weboldalakra bejelentkezik.
- A mobiljában ne legyen (publikus módon, pl. sms-ben, kapcsolatként, jegyzetként, vagy teendőként) eltárolva a belépési azonosítója és/vagy jelszava.
- Az Internet használatakor győződjön meg arról, hogy senki sem figyeli jelszó megadása közben. A belépési azonosítóját és a jelszavait tartsa titokban. Ne fogadja el az Internet böngészők jelszómegjegyzési ajánlatát kritikus oldalaknál (lehetőleg egyáltalán ne használja ezt a funkciót).
- Lehetőleg ne végezzen tranzakciót az interneten publikus helyekről (pl. kávézókban, könyvtárakban).

Adatkapcsolat

- Hamis Internetbank weboldal legkönnyebben arról ismerhető fel, hogy a címsorban nem https://, hanem http:// kezdetű címzés szerepel. A hiányzó "s" betű a secured, azaz biztonságos adatkapcsolat hiányát jelzi.
- A böngésző jobb alsó sarkában található lakat ikon a biztonságos Internet kapcsolatot szemlélteti. Nézze meg a kis lakatot, mint a biztonság jelét és rákattintva a tanúsítványt (a titkosítás adatai: a titkosított oldal neve, a tulajdonos, a lejárat, a kiállító cég). Ha nincs lakat, akkor Ön nem valódi Internetbanki kapcsolatot használ.
- Bizalmas oldalak Internet címeit gépelje be kézzel (netbank, elektronikus boltok, stb.). Mindig a "Kijelentkezés" gombbal jelentkezzen ki, a böngészőt csak ez után zárja be.

Speciális ajánlások tippek

- Mindig gyanakodjon, ha e-mail alapján (nem válaszlevélben, hanem egy, a levélben elhelyezett linkre kattintva) azonosító adatokat kérnek be Öntől. Gyanakvóan olvasson minden hivatalosnak tűnő levelet, mely "az Ön biztonsága érdekében" kér Öntől olyasmit, amit eddig még sohasem (pl. látogasson meg egy adott oldalt, ahova írja be kártyaszámát, PIN-kódját, jelszavát, stb.).
- Ne tartson nyitva más böngésző ablakot és ne futtasson az Internetbank használata során más programokat. A használat után a böngészőt zárja be.

Nem saját gépről történő lekérdezések veszélyei, kockázatai

- Nem saját gépről történő, valamint a nyilvános internet pontokon keresztüli használat során fokozott az illetéktelen adathozzáférés veszélye. Lehetőség szerint tartózkodjon a banki internetes szolgáltatás mások jelenlétében, illetve nyilvános helyen (pl. Internet Kávézó, munkahelyen sokak által közösen használt gép) stb.) történő használatától.
- Amennyiben a szolgáltatást mások jelenlétében, nem saját gépről, illetve nyilvános helyen használta, javasoljuk, hogy
- Ellenőrizze a vírus és tűzfal védelmi beállításokat. Megfelelő védelem hiányában lévő számítógépen a szolgáltatás használatát nem javasoljuk!
- Ne engedélyezze az ideiglenes internet fájlok tárolását vagy a kilépést követően törölje böngészőjében az Ideiglenes Internet File könyvtár (Temporary Internet Files) tartalmát.