



Netbankot használ? Az Ön pénze is veszélyben lehet!

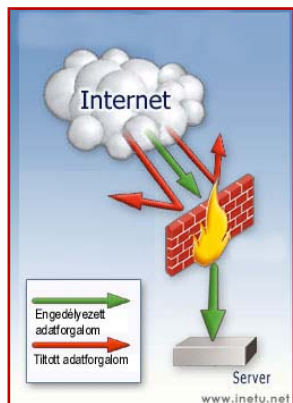


A magyar felnőttek fele használ netbankot, 100-ból 8-an pedig a mobiljukon keresztül is bankolnak. Érdekes azonban vigyázni, hiszen könnyen lehet, hogy veszélyben van a pénzünk. Mutatjuk a biztonsági alapszabályokat.

Bár egyre többen használják a netbankot és a mobilbankot, sokan nincsenek tisztában az alapvető biztonsági kérdésekkel. A Magyar Nemzeti Bank (MNB) tájékoztatása alapján mutatjuk, mire kell nagyon figyelni. (<http://www.mnb.hu/fogyasztovedelem/dontenem-kell/alapveto-penzugyeink/bankszamlak/e-banking/e-banking-biztonsag>)

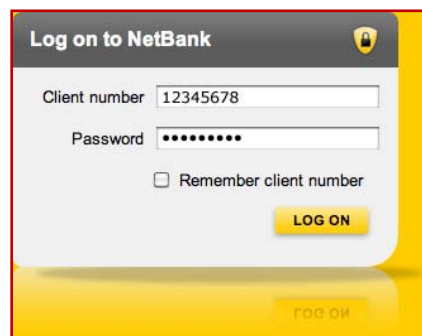
A bankunktól kapott jelszót az első használat során érdemes megváltoztatni. Ha más biztonsági azonosítás (például sms-kód) nincs, a jelszócserét a bank bizonyos időközönként a továbbiakban is kérheti.

Olyan jelszót adjunk meg, amely nem kapcsolható hozzánk, így nem fejthető vissza egyszerűen (például ne kedvenc háziállatunk nevét vagy egy szimplán növekvő sorszámot, vagy születési dátumot adjunk meg jelszónak). A netbanki jelszót ne adjuk meg senkinek! Ne készítsünk olyan feljegyzést (pl. számítógépen és mobiltelefonon sem), amely illetéktelen kezébe kerülve lehetővé teszi a belépést a mi nevünkben!



Elektronikus kódjainkat - amennyiben nem elektronikus azonosítás kapcsán kérjük - telefonon, e-mailen vagy írásban még saját bankunk sem kérheti. **Ha ilyen kéréssel találkozunk, akkor biztosak lehetünk abban, hogy ezt valójában nem az intézmény kéri.** Ilyenkor azonnal értesíteni kell a bankot, hogy megtehesse az ilyenkor szükséges lépéseket (figyelemfelhívás, rendőrség értesítése, biztonsági lépések).

Használjunk víruskereső programot és rendszeresen frissítsük azt! Telepítsünk tűzfal-szoftvert is, amit szintén rendszeresen frissítsünk!





Interneten keresztül csak biztonságos helyről intézzük pénzügyeinket!

- Ne adjunk lehetőséget arra, hogy elektronikus kódunkat más is láthassa! Csak végső megoldásként használjunk nyilvános internetet (például internet kávézóban), vagy jelszóval nem védett Wi-Fi hálózatot bankügyeink intézésére. Ha mégis ezt tesszük, saját érdekünkben tartsunk be néhány fontos biztonsági szabályt!
- Ne válasszuk azt a lehetőséget, hogy a számítógép megjegyezze a belépéshez szükséges jelszót!
- Tanácsos törölni a böngésző tárolóját is az internetes bankolás után, hogy illetéktelen személy ne tudjon adatainkkal visszaélni.
- Ha nyilvános helyen intézzük pénzügyeinket, célszerű ezt követően megváltoztatni a belépési jelszót.
- A netbankból ne a böngésző bezárásával, hanem a kilépés gombbal jelentkezzünk ki!
- Az internetbank használata közben a böngésző címsorában szereplő linket adataink biztonsága érdekében ne küldjük tovább!



Mire figyeljünk, ha mobilbankot használunk?



Az okostelefonok, tabletek ugyanúgy célpontot jelentenek az online bűnözők számára, mint a számítógépek. Fontos, hogy tisztában legyünk az ilyen készülékek használatának veszélyeivel és a kockázatok csökkentésének lehetőségeivel.

Mobilunkra is töltsünk le vírusvédő/tűzfal szoftvert. Egyes kártevők képesek a többszintű/többcsatornás azonosítást is megkerülni. Például, ha az azonosításhoz a standard azonosító mellett egy ideiglenes, csak pár percig élő azonosító (amit SMS-ben kapunk meg az intézménytől) is szükséges, az okostelefont megtámadó szoftver mindkét azonosítót megszerzi a telefonból.

Óvatosan kezeljük a letöltéseket, ellenőrizzük a forrásokat!

Ahogy internetbankolás esetében, úgy mobil netbankolás során is a kilépés gombbal jelentkezzünk ki az internetes rendszerből, továbbá a használat közben a böngésző címsorában szereplő linket adataink biztonsága érdekében ne küldjük tovább!

Forrás: (<http://www.mnb.hu/fogyasztovedelem/dontenem-kell/alapveto-penzugyeink/bankszamlak/e-banking/e-banking-biztonsag>)