BIZTONSÁGOS E-BANKOLÁS

TARTALOMJEGYZÉK

BEVEZETÉS

Kedves Ügyfelünk! Bankunk az internetes banki szolgáltatását kiemelten magas biztonsági elvárásoknak megfelelő technikai háttérrel kínálja Önnek, mindazonáltal a teljes biztonság eléréséhez Önnek is be kell tartania néhány egyszerű szabályt. Az alábbi tájékoztató lépésről-lépésre ismerteti, hogyan védekezhet a vírusok, az adathalászat és egyéb internetes veszélyek ellen.

ÁLTALÁNOS MŰVELETEK

Az alábbi tanácsok az internet biztonságos használatához általánosan érvényesek, így ezeket akkor is érdemes követnie, ha Ön éppen nem kívánja internetes banki szolgáltatásunkat igénybe venni, csupán böngészni, vagy levelezni akar a világhálón.

Végezze el a szoftverfrissítéseket

Az időről-időre azonosított, újabb biztonsági rések (sebezhető pontok) miatt érdemes az operációs rendszert és a webböngészőt rendszeresen frissítenie. Az operációs rendszerek többsége automatikus frissítési funkcióval rendelkezik, melyet minden esetben tartson bekapcsolva. A többi alkalmazást (pl. e-mail programok, médialejátszók, szövegszerkesztők, chatelő szoftverek stb.) is mindig frissítse.

Használjon vírusirtó szoftvert

Használjon általánosan elterjedt vírusirtó szoftvert, és azt az automatikus frissítési funkcióval rendszeresen frissítse. A hazánkban leggyakrabban használt vírusirtó programokhoz az alábbi linkek segítségével juthat el:

avast! (ingyenes) http://www.avast.com

AVG (ingyenes) http://www.avg.hu

NOD32 http://www.nod32.hu

Norton AntiVirus http://www.symantec.hu

A spyware [kémprogramok] és adware [reklámprogramok] elleni lehető legmagasabb fokú védelem elérése érdekében ajánlott olyan eszközöket is használni, melyek felismerik, és eltávolítják ezeket a rosszindulatú elemeket. Frissítse szoftverét, és ellenőrizze számítógépét rendszeresen! spyware/adware elleni eszközökhöz a következő linkekkel juthat el:

Ad-aware (ingyenes) http://www.lavasoftusa.com

Spybot S&D (ingyenes) http://www.spybot.info/hu

Használjon személyes tűzfalat

Használjon személyes tűzfalat a nem kívánt internetes kapcsolatok létrejöttének megakadályozására. Egyes operációs rendszerek (pl. Windows XP, Mac OS X stb.) standard beépített eszközökkel rendelkeznek. Az internetről szélesebb körű szolgáltatásokat nyújtó személyes tűzfalak is letölthetőek, melyeket az alábbi linkeken érhet el:

Sunbelt/Kerio Personal Firewall (ingyenes) http://www.sunbelt.hu

ZoneAlarm (ingyenes) http://www.zonelabs.hu

Norton Internet Security http://www.symantec.hu

Tegye biztonságossá hálózatát

Amennyiben ön router-en keresztül csatlakozik az internethez, és módjában áll annak beállításait megváltoztatni, akkor érdemes a helyi hálózatot is biztonságossá tennie. Az egyes lépések elvégzésének módja függ a berendezés típusától, részletesebb információt annak kézikönyvében találhat.

Első lépésként változtassa meg a router alapértelmezett jelszavát, ha még nem tette meg. A korszerű router-ek rendelkeznek beépített tűzfal funkcióval, ezt érdemes bekapcsolni. A router működését az úgynevezett firmware vezérli, ennek rendszeres frissítése is javasolt.

Ha vezeték nélküli (WIFI) router-t használ további beállítások is ajánlottak a biztonság érdekében. Kapcsolja be a kapcsolat titkosítását, alkalmazzon WPA titkosítást, a jelszó legyen legalább 20 karakter hosszú és tartalmazzon betűket, számokat és speciális karaktereket vegyesen. Tovább növelheti a hálózat biztonságát, ha a DHCP szolgáltatást kikapcsolja és fix IP címeket használ, valamint aktiválja a MAC szűrést, és a router-hez való csatlakozást csak saját számítógépe számára engedélyezi.

Nyilvános HotSpot-on soha ne e-bankoljon!

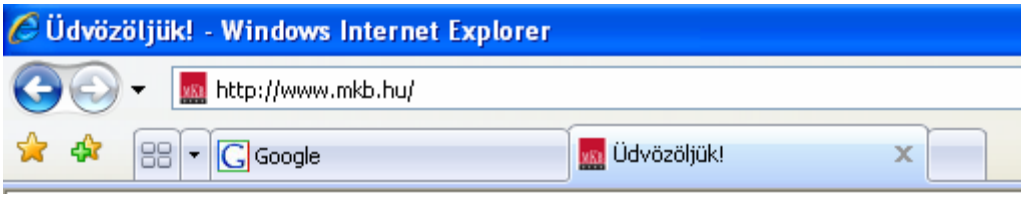
BEJELENTKEZÉS ELŐTT

Az e-bankolás megkezdése előtt ajánlatos néhány olyan lépést is megtennie, amelyek talán egy kis kényelmetlenséget jelentenek, de a biztonság fokozása érdekében szükségesek.

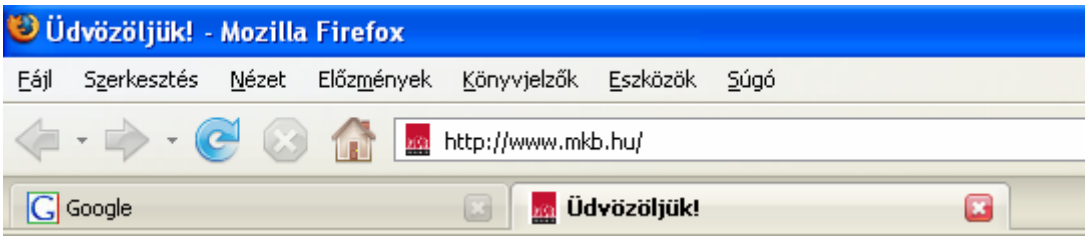
Nyissa meg a böngészőt új ablakban

Minden egyes e-bankolási folyamathoz indítsa újra a böngészőt. Minden esetben biztosítsa, hogy a folyamat során más weboldal nincs nyitva.

Bizonyos böngészők támogatják az úgynevezett „füles böngészést” (tabbed browsing), azaz azt a lehetőséget, hogy egyetlen böngésző ablakban több kapcsolatot nyisson. A böngésző ablakának a felső részén a fülsor mutatja, hogy több fül van-e nyitva:



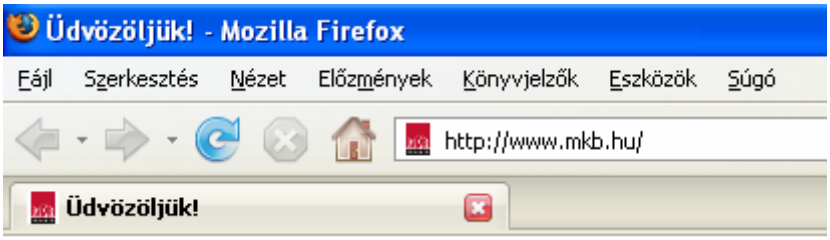
1./a ábra: Helytelen – több fül van nyitva ugyanabban a böngésző ablakban (Internet Explorer)



1./b ábra: Helytelen – több fül van nyitva ugyanabban a böngésző ablakban (Mozilla Firefox)

Az alábbi képek olyan böngésző ablakokat mutatnak, melyekben csak egy fül van nyitva:

2./a ábra: Helyes – A böngésző ablakban csak egy fül van nyitva (Internet Explorer)



2./b ábra: Helyes – A böngésző ablakban csak egy fül van nyitva (Mozilla Firefox)

Manuálisan írja be a címet

A böngésző megnyitását követően minden esetben manuálisa írja be az online bank címét (URL). Még nagyobb biztonságot érhet el, ha a bank IP címét írja be, amennyiben ismeri azt. Semmi esetre se kattintson olyan e-mailben vagy harmadik felek weboldalain található linkekre, melyek célja, hogy a kívánt honlapra vezesse Önt (még akkor sem, ha a linkek látszólag az Ön bankjától származnak). Az „adathalászat” nevű támadási módszer lényege, hogy a támadók megpróbálják megtéveszteni a felhasználókat, és egy olyan weboldalra irányítják őket, amely a bank weboldalával azonos kinézetű, de az itt megadott felhasználói nevek és jelszavak az adathalászokhoz kerülnek, melyekkel később ők visszaélhetnek.

Tartsa be a jelszavakra vonatkozó szabályokat

Olyan jelszót válasszon, melyet Ön könnyen megjegyez, de mások számára nehéz kitalálni. A jó jelszó betűket, számokat és speciális karaktereket is (összesen legalább 8 karaktert) tartalmaz. Jelszavát rendszeresen módosítsa! Soha ne adja meg a jelszavát harmadik feleknek vagy pénzügyi szolgáltatóknak. **A bank soha nem kéri a jelszó átadását!** Soha ne írja le a jelszót, semmilyen körülmények között ne mentse azt a számítógépre, és böngészőjében is kapcsolja ki a jelszavak megjegyzését az e-bankoló honlapon.

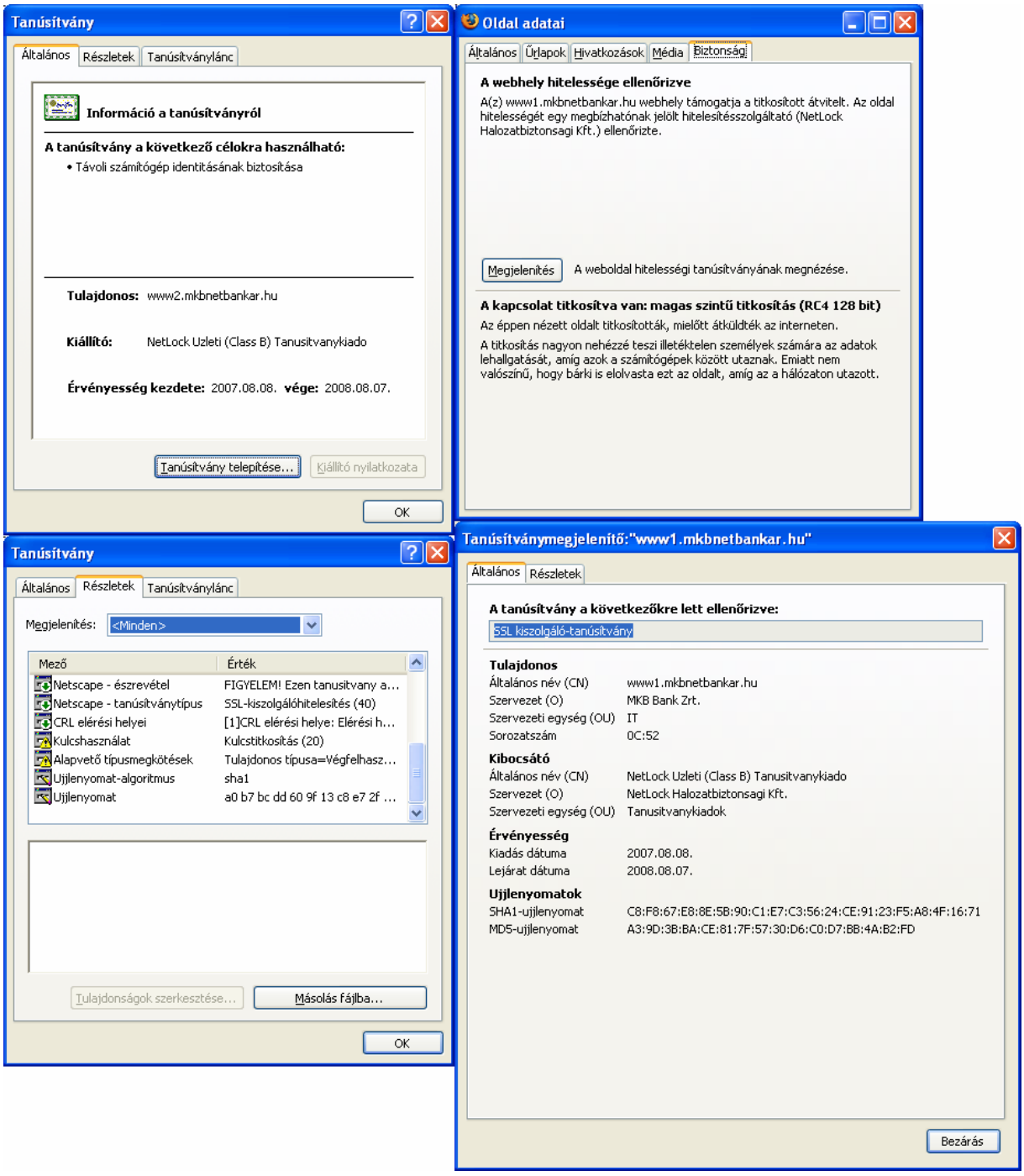
AZ E-BANKOLÁSI FOLYAMAT SORÁN

Ellenőrizze az e-bankolási oldal hitelességét és a kódolást

A bejelentkezést követően a kapcsolat kódolása és a meglátogatott weboldal hitelessége az úgynevezett tanúsítvány segítségével ellenőrizhető. Kattintson kétszer a lezárt lakat szimbólumra az állapotsoron, a böngészőablak legalsó részén (lásd a 3. ábrát).

3. ábra: Példák kódolási szimbólumokra a legnépszerűbb böngészők állapotsorán

A megnyíló ablakban a tanúsítvány tulajdonságai jeleníthetőek meg. Ellenőrizze, hogy a tanúsítvány a bank nevében került-e kiállításra. A tanúsítványon az úgynevezett ujjlenyomatot szintén ellenőrizze. Ha az ujjlenyomat azonos az e-bankolási honlapon közzétett ujjlenyomattal, a megfelelő oldalra a kódolt kapcsolat biztosítva van. Az alábbi ábrák példákat adnak a tanúsítványok tulajdonságablakaira:



4. ábra: Tanúsítványablakok Internet Explorerben (balra) és Mozilla Firefoxban (jobbra)

Az egyéb böngészők tanúsítványablakai ezekhez hasonlóak, tehát a 4. ábrán látható ablakok más böngészőkre is vonatkoztathatóak.

Használja a beépített biztonsági elemeket

Kérjen SMS értesítést a sikeres bejelentkezésekről, így Ön azonnal értesülhet róla, ha valaki más az Ön felhasználói nevével és jelszavával bejelentkezik a rendszerbe! Az utolsó sikeres bejelentkezés időpontját a képernyő jobb felső sarkában is láthatja.

Állítson be átutalási és átvezetési limiteket a rendszerben, és korlátozza a használható számlák körét az Ön által valóban használtakra.

Használjon a bejelentkezési jelszavától eltérő aláírói jelszót, így ha valaki hozzáférne felhasználói fiókjához, nem lesz képes a rendszeren keresztül megbízásokat indítani az Ön nevében. A jelszavakra vonatkozó szabályokat az aláírói jelszó esetén is tartsa be!

A megbízások biztonsága növelhető SMS-ben küldött aláírói jelszóval, amely csak az adott tranzakcióhoz használható fel és segítségével magasabb használati limitek érhetők el.

Elvégzett műveleteit ellenőrizheti a nyitóképernyőn megtalálható „Esemény napló” funkció segítségével.

Figyelje a hibaüzeneteket

Körültekintően olvasson el bármilyen megjelenő hibaüzenetet vagy figyelmeztetést. Kétséges esetekben hívja fel a bank támogató szolgálatát.

AZ E-BANKOLÁSI FOLYAMAT LEZÁRÁSA

Jelentkezzen ki helyesen

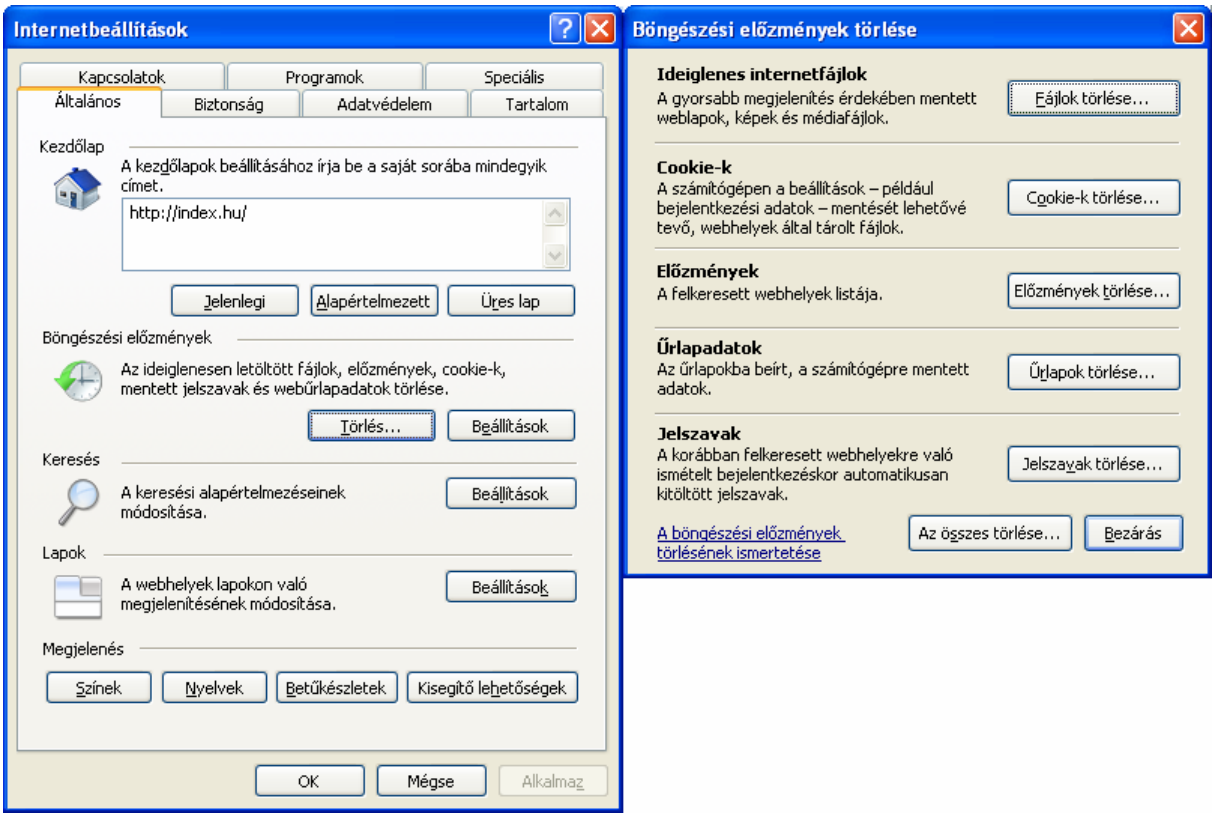
Az e-bankolási folyamatot minden esetben a „Kilépés” funkcióval zárja le. A böngésző ezt követően a helyes lezárás visszaigazolásaként egy új oldalt jelenít meg.

Törölje az ideiglenes internetes fájlokat

A kijelentkezést követően javasolt az ideiglenes internetes fájlokat, a böngésző úgynevezett „gyorsítótárát” (a múltbéli állapotot rögzítő memóriát) törölnie. Ezzel az online folyamat helyi nyomait törli a számítógépről. Ha nem saját számítógépét használta az e-bankoláshoz, minden esetben végezze el azt a lépést!

Eljárás az Internet Explorerben (Windows):

A Windows alatt futó Internet Explorerben válassza az Internetbeállítások [Internet Options] opciót az Eszközök [Tools] menüben. Az 5. ábrán látható ablak kinyílik. Ebben az ablakban kattintson a Törlés [Delete] gombra. Egy új ablak nyílik meg, melyben a műveletet a Fájlok törlése [Delete files], illetve Cookie-k törlése [Delete cookies] gombokkal végezheti el.

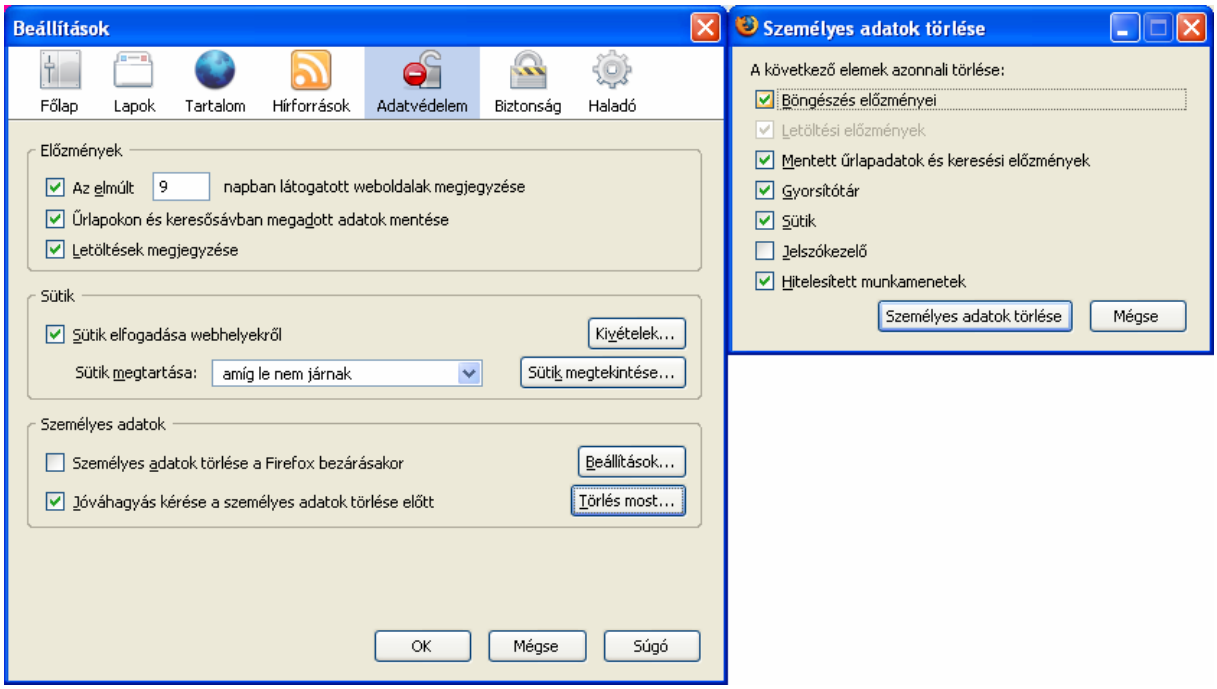


5. ábra: Ideiglenes internetfájlok, cookie-k és előzmények törlése az Internet Explorerben (Windows)

Eljárás a Firefoxban (Windows):

Válassza a Beállítások [Options] parancsot az Eszközök [Tools] menüben. A frissen megnyíló ablakban kattintson az Adatvédelem [Privacy] feliratú lakat szimbólumra (lásd 6. ábra).

Ezt követően kattintson a Törlés most [Delete now] gombra. Jelölje be a Gyorsítótár [Cache] és Sütik [Cookies] pontokat, majd kattintson a Személyes adatok törlése gombra.



6. ábra: A gyorsítótár törlése Firefoxban (Windows, Mac OS X)

ÖSSZEFOGLALÓ

A fenti rövid útmutatóban meghatározott biztonsági intézkedések betartásával kényelmesen és biztonságosan intézheti banki ügyeit az Interneten. Mindazonáltal érdemes részletesebben is megismerkedni az e tekintetben felmerülő veszélyekkel és kockázatokkal.

Figyelmébe ajánljuk a Pénzügyi Szervezetek Állami Felügyelete (PSzÁF) által közzétett anyagokat, melyek további információkkal szolgálhatnak Önnek a biztonságos e-bankolásról:

Amit az internetes csalásokról tudni kell!

Az internetes bankolás megnyugtató biztonsági megoldásai

Tegye - ne tegye, avagy mire figyeljen az elektronikus pénzügyek esetében?

Ismételten felhívjuk a figyelmet: Amit az internetes csalásokról tudni kell!