K&H Bank Zrt.

1095 Budapest, Lechner Ödön fasor 9.
telefon: (06 1) 328 9000
fax: (06 1) 328 9696
Budapest 1851
www.kh.hu • bank@kh.hu

Tájékoztató a K&H e-bank biztonságos használatáról

A K&H Bank internetbank szolgáltatása, az e-bank lehetővé teszi, hogy Ön kényelmesen és gyorsan intézhesse pénzügyeit - bárhol, bármikor a nap 24 órájában.

Mindent megteszünk azért, hogy ez az ügyintézés a lehető legbiztonságosabb legyen – ehhez azonban az Ön elővigyázatosságára, közreműködésére is szükség van.

Fontos tudni, hogy a Bank nem vizsgálja, és nem felügyeli az Internet működését, annak biztonságáért nem felelős. Az internetes csalások bűncselekménynek számítanak, ezért felderítésük a nyomozó hatóságok feladata!

1. Amit a K&H Bank tesz az e-bank szolgáltatás biztonságáért

A K&H Bank olyan biztonsági szabványok és eljárások alkalmazásával nyújtja az e-bank szolgáltatást, melyek lehetővé teszik, hogy az Ön személyes és pénzügyi adatainak bizalmassága ne sérüljön, azok ne kerüljenek illetéktelen kezekbe.

Biztonságos kapcsolat

Amikor Ön meglátogatja a K&H Bank weboldalát, automatikusan biztonságos, titkosított kapcsolat épül fel az Ön Internet böngészője és a Bank között. Minden információ, amit küld vagy fogad, titkosított formában közlekedik a világhálón, illetéktelenek sem elolvasni, sem módosítani nem tudják.

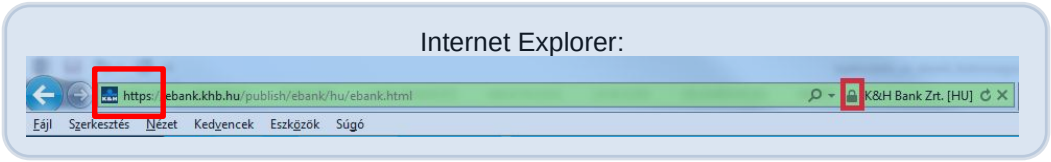
A biztonságos kapcsolat létesítésének feltétele az e-bank szerver „személyazonosságának” ellenőrzése. Ha a kapcsolat kiépült, az arra is biztosíték, hogy az Ön böngészője valóban a K&H Bankkal kommunikál, nem pedig egy rosszindulatú támadó rendszerével, aki esetleg eltérítette a kapcsolatot.

A titkosított adatátvitel és a banki szerver számítógép „személyazonosságának” ellenőrzése egy digitális tanúsítványon alapszik, mely szemléletesen a banki szerver „személyi igazolványának” tekinthető. Amikor a kapcsolat felépítés kezdetén a böngésző a banki rendszerhez fordul, a szerver elküldi a böngészőnek a tanúsítványát. Ha a böngésző úgy találja, hogy a tanúsítvány rendben van, akkor megtörténik a biztonságos kapcsolat kiépítése, egyébként pedig figyelmezteti a felhasználót a problémára.

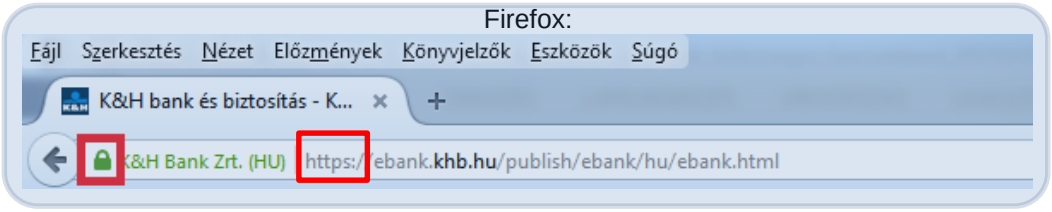
A biztonságos kapcsolat létrejötte könnyen felismerhető

- A címsorban a bank Internet címe „https” kezdetű (pl. https://ebank.kh.hu)

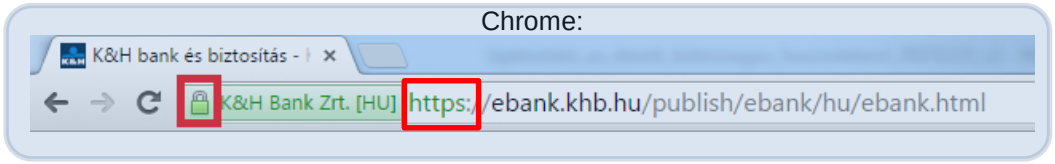
Internet Explorer:



Firefox:

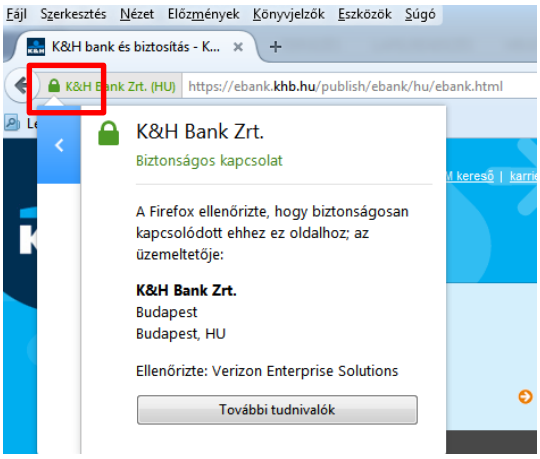


Chrome:



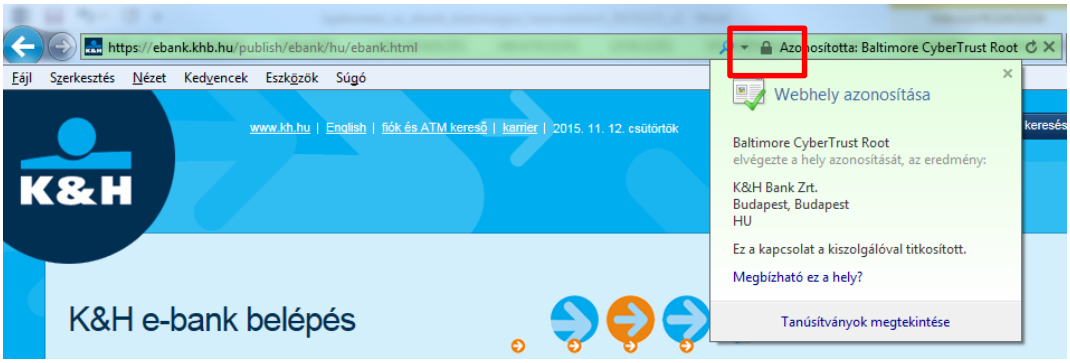
- A böngésző zárt lakat szimbólumot jelenít meg. A lakat ikon helye a böngésző típusától és verziószámától függ, rendszerint a címsor közelében, előtte vagy utána található.

A digitális tanúsítvány ellenőrzése



Firefox

Firefox



Internet Explorer

- A tanúsítványt legegyszerűbben a **lakat szimbólumra kattintva** ellenőrizhetjük. Ekkor rendszerint egy rövid összefoglalót kapunk a tanúsítvány tartalmáról, bővebb információkat (a tulajdonos adatai, a Web címek, melyeken keresztül a szerver elérhető, a tanúsítvány lejárati dátuma, stb.) az összefoglaló alatti gombra/linkre kattintva érhetünk el.

- A K&H Bank a nyilvános szervereit ún. *kiterjesztett érvényesítésű* tanúsítványokkal látja el, melyek a hagyományos digitális tanúsítványoknál is nagyobb biztonságot nyújtanak. Az új típusú böngészők ilyen típusú tanúsítványok esetén a címsor előtt a tulajdonos nevét (és a lakat ikont) zöld színnel jelenítik meg, ellenétben a hagyományos tanúsítványokkal, ahol a megjelenítés kékkel történik.

Biztonságos ügyfél azonosítás és tranzakció jóváhagyás

K&H e-bank chipkártyás, SMS vagy mobil-token azonosítással érhető el hagyományos számítógépről/laptopról.

a.) Chipkártyás azonosítású e-bank

A K&H e-bank szolgáltatás biztonsága érdekében nyilvános kulcsú infrastruktúrát (PKI) alkalmazunk, mely lehetővé teszi, hogy a bejelentkezés és a tranzakciók jóváhagyása digitális aláírással történjék. Az aláíráshoz szükséges, felhasználónként egyedi kriptográfiai kulcsok a chipkártyán tárolódnak, biztonságos körülmények között.

A megoldás lényege, hogy ebben az esetben a szerverhez hasonlóan a felhasználók is digitális tanúsítvánnyal rendelkeznek, mindkét fél tehát saját „digitális személyi igazolványával" azonosítja magát a másik felé. A felhasználó digitális tanúsítványa szintén a chip kártyán található.

A megoldás biztosítja a következő elvárások teljesülését:

- **Bizalmasság:** az üzeneteket illetéktelenek nem olvashatják, csak a bank és az ügyfél
- **Hitelesség:** az üzenetet váltó felek azonosítása és ellenőrzése erős hitelesítéssel történik. Az ügyfél a tranzakciós üzeneteit digitális aláírásával hitelesíti, illetve ennek ellenőrzésére szolgáló digitális aláírói tanúsítvánnyal rendelkezik.
- **Sértetlenség:** a digitális aláírás a tranzakciós üzenetek integritását (időszerűségét, hitelességét, teljességét) védi.
- **Letagadhatatlanság:** a digitális aláírás és egy időbélyegző együttes alkalmazása biztosítja.

Gyakorlati megvalósulás

- chipkártya behelyezése az olvasóba,
- a tranzakciók érvényesítése/aláírása a chipkártyához tartozó PIN kód segítségével

b.) SMS azonosítású e-bank

A K&H Bank az e-bank szolgáltatás elérésére a chipkártyás azonosítási módon kívül SMS-el történő belépésre is lehetőséget biztosít. Ebben az esetben a belépéshez és a banki műveletekhez a felhasználói név és jelszó ismeretén kívül a szolgáltatásban regisztrált telefonhoz való hozzáférés is szükséges.

SMS azonosítás esetén pénzügyeinek további védelmében a K&H Bank napi maximálisan átutalható összeghatárt alkalmaz, melynek mértékéről mindig az aktuális hirdetményből tájékozódhat.

A belépésre és a tranzakció aláírásra szolgáló SMS-ek érvényessége 5 perc. Időtúllépés esetén az adott – belépési vagy tranzakció aláírási – műveletet meg kell ismételni.

c.) K&H e-bank mobil-token használattal

A K&H e-bank szolgáltatás mobil-tokenes belépéssel is igénybe vehető. A mobil-token a K&H mobilbank alkalmazásba épített azonosítási mód, amely a megfelelő webáruházból tölthető le.
A K&H mobilbank alkalmazás letöltése után a mobil-tokent aktiválni kell, amelynek során a felhasználó okostelefonja összerendelésre kerül a mobil-tokennel, így biztosítva, hogy az csak az adott készüléken lesz használható.
A megoldás a számítógépen megjelenő színes kód és QR kód beolvasásával teszi lehetővé a belépést és a tranzakció aláírást.

A kapcsolat automatikus bontása

Amennyiben Ön bejelentkezett az e-bank szolgáltatásba, de azt adott ideig nem használja, a kapcsolatot a Bank automatikusan bontja. Ezután Önnek újra be kell jelentkeznie, amennyiben tovább kívánja használni az e-bank szolgáltatást. Ez az eljárás segít abban, hogy ha Ön elfelejtene kijelentkezni, más akkor se férhessen hozzá az adataihoz.

Gyanús műveletek monitorozása

A bank a szolgáltatás igénybevétele során végzett műveleteket monitorozza, és ha gyanús eseménnyel találkozik, akkor kapcsolatba lép az ügyféllel, hogy tisztázza, hogy a kérdéses művelet valóban a jogosult felhasználó akaratának megfelelően történt-e.

2. Amit Önnek kell tennie, ha biztonságosan akarja intézni pénzügyeit

A K&H e-bank biztonságos használata az Ön felelőssége is – hiszen mi nem vagyunk jelen az Ön otthonában, nem felügyeljük számítógépét, mobil eszközét. Ha az e-bank szolgáltatás igénybevételére használt eszköz megfertőződik, vírus vagy más rosszindulatú program települ rá, akkor az a banki műveletek biztonságát is fenyegetheti.

Az e-bank védelme, másképp fogalmazva pénzügyeinek védelme hasonlatos ahhoz, ahogy otthonát védi: elindulna úgy, hogy nyitva hagyja maga mögött az ajtót?

Tegye biztonságossá számítógépét!

- A szolgáltatást lehetőség szerint olyan eszközről használja, amely az Ön felügyelete alatt áll. Ne jelentkezzen be az e-bankba pl. netkávézóból vagy nyilvános, másokkal közösen használt gépről.
- Gondoskodjon az operációs rendszerhez, az Internet böngészőhöz és egyéb szoftvereihez kiadott biztonsági frissítések rendszeres telepítéséről. Használja az automatikus frissítési funkciót, amennyiben ez lehetséges. Ezzel megelőzhető, hogy a vírusok és egyéb rosszindulatú programok a rendszer ismert biztonsági sérülékenységeinek kihasználásával férkőzzenek be az Ön által használt eszközre.
- Telepítsen vírusirtó szoftvert, frissítse rendszeresen és gondoskodjon annak folyamatos működéséről!
- Használjon tűzfalat, hogy megakadályozza a nem kívánatos hozzáférést számítógépéhez!
- Ha vezeték nélküli hálózatot használ, gondoskodjon a biztonságos beállításokról. (Ne használjon WEP titkosítást, hanem WPA2-t, használjon hosszú, véletlenszerűen választott jelszót, stb.)
- Használjon spyware- és malware (kémprogramok, kártékony szoftverek elleni) szűrő programot!
- Csak megbízható forrásból telepítsen programot a gépére, mobil eszközére
- Mobil eszközének háttértárait titkosítsa, használjon képernyőzárat és jelszót a feloldáshoz

Az e-bank belépési oldalát körültekintően érje el!

- Az elektronikus banki kapcsolat idejére zárjon be minden más Internet kapcsolatot
- A weboldal címét kézzel írja a címsorba, ne használjon email-ben kapott linket. Az email-be illesztett linkek könnyen manipulálhatók, egyszerűen megoldható, hogy látszólag az e-bankra mutassanak, de valójában máshová vezetnek
- Ha kapcsolódáskor a böngésző tanúsítvány hibát jelez, akkor ne jelentkezzen be az e-bankba, hanem értesítse a bank ügyfélszolgálatát
- Mindig jelentkezzen ki az e-bank szolgáltatásból, zárja be a böngészőt és vegye ki a chipkártyát az olvasóból, ha befejezte az online ügyintézést

Ellenőrizze, hogy valóban a Bank internetes oldalán jár-e!

A következő egyszerű lépésekkel meggyőződhet arról, hogy valóban a Bank Internet oldalán jár-e, nem irányították-e át csalárd szándékkal más weboldalra:

- A címsorban helyesen szerepel a Bank Internet címe és az 'https' kezdetű? (Figyelem, a helyes címtől való eltérés lehet, hogy csak egy betű és nehéz is észrevenni, pl. *legjobbank.hu* helyett *legjobbank.hu* / kis „L" betű helyett nagy „I").
- Az Internet böngészőben fellelhető a zárt lakatot jelképező szimbólum?
- Ha arra duplán kattint, a megjelenő ablakban a tanúsítvány adatai között helyesen szerepel a K&H Bank neve és Internet címe?
- Új típusú böngésző esetén a bank neve (és a lakat ikon) a címsor előtt zöld színben jelenik meg?
- Tapasztal bármi szokatlant a weboldal használata vagy az e-bank bejelentkezés során? A megszokott weboldalakat kapja a bejelentkezést követően?

Ha nem, előfordulhat, hogy Ön egy olyan weboldalon tartózkodik, amely látszólag megegyezik a K&H Bank oldalával, ám valójában egy hamisított oldal, amelyet azzal a szándékkal hoztak létre, hogy Öntől bizalmas információkat szerezzenek meg!

Ha ezt **tapasztalja**, kérjük, **haladéktalanul** értesítse a K&H Bankot e-mailen (bank@kh.hu), telefonon (+36 (1/20/30/70) 335 3355) keresztül vagy jelezze azt személyesen bármely bankfiókunkban. Köszönjük együttműködését!

cégjegyzékszám: Cg. 01-10-041043 nyilvántartó: Fővárosi Törvényszék Cégbírósága

a KBC csoport tagja

Használja körültekintően az e-bankot!

- Vegye ki a chipkártyát az olvasóból, ha már nincs szükség rá
- Lépjen ki az e-bank alkalmazásból a használat végeztével és zárja be a böngészőt
- Kérjen SMS értesítést (MobilInfo) minden, a számláját érintő kimenő tranzakcióról és azonnal lépjen kapcsolatba a bank ügyfélszolgálatával, ha ismeretlen átutalást tapasztal

Tiltsa le az elveszett/ellopott azonosító eszközt!

- Az elveszett/ellopott chipkártyát azonnal tiltsa le a banki ügyfélszolgálaton
- Ha SMS alapú bejelentkezést használ, és a telefonja elveszett, tiltassa le a SIM kártyát a szolgáltatónál
- Amennyiben mobiltelefonját elveszti/ellopják, mobil-tokenjét tiltsa le az e-bank „beálllítások" menüpontjában, vagy hívja a K&H Telecentert, ahol a tiltást azonnal elvégzik.