Biztonsági tanácsok
az elektronikus banki szolgáltatások használatához kapcsolódóan

Tisztelt Ügyfelünk!
Az elektronikus csatornákat napjaink legbiztonságosabb fizetési eszközeként tartják számon. Ez azonban csak akkor igaz, ha a szükséges biztonsági előírásokat megismeri és a használat során ennek figyelembevételével jár el.

Az elmúlt időszakban Magyarországon is megszaporodtak az elektronikus banki termékekkel történt visszaélési kísérletek. A KDB Bank Európa Zrt. az alkalmazott különféle biztonsági megoldások révén már eddig is számos lépést tett a kockázatok csökkentése érdekében. Mivel ez kölcsönös érdekünk, ezért az ügyfeleink közreműködésére is szükség van. Ezért néhány fontos tanáccsal szeretnénk segíteni Önt, hogy Bankunk elektronikus szolgáltatásait biztonságosan használhassa.

Általános biztonsági tanácsok:

- Tegye biztonságossá hálózatát! Védje eszközeit (számítógép, mobiltelefon, táblagép) tűzfallal, valamint rendszeresen frissített antivírus és kémprogramirtó szoftverrel, és legalább havonta futtasson le velük egy teljes rendszervizsgálatot! (Ezekből a programokból lehetőleg próbaváltozatot ne, csak teljes verziót használjon, mert ezekhez jár csak a legújabb frissítés és támogatás.)
- Amennyiben routeren keresztül csatlakozik az internethez és módjában áll megváltoztatni a beállításait, változtassa meg a router alapértelmezett jelszavát, és kapcsolja be a beépített tűzfal funkciót (amennyiben van ilyen)! A router működését biztosító firmware rendszeres frissítése javasolt. Amennyiben vezeték nélküli routert használ, alkalmazzon WPA/WPA2 titkosítást, fix IP címet, kapcsolja be a MAC cím szűrést és a routerhez csak saját számítógépe számára engedélyezze a hozzáférést!
- Tartsa naprakészen az eszközei által használt operációs rendszereket (Windows, Linux, MacOS, iOS, Android) és az eszközökre telepített alkalmazásokat a gyártók által kiadott hivatalos frissítések, javító verziók rendszeres telepítésével! Lehetőség szerint kapcsolja be (illetőleg ne kapcsolja ki) az automatikus frissítés funkciót!
- Kizárólag legális szoftvereket használjon eszközein, melyekre ne telepítsen ismeretlen forrásból származó vagy kétes eredetű alkalmazásokat!
- Javasoljuk, hogy a böngésző adatbiztonsági beállításait lehetőség szerint magas fokozatú biztonsági szintre állítsa be, hogy használat közben figyelmeztesse a kárt okozó tartalom megnyitása előtt!
- **Ne telepítsen olyan alkalmazásokat, melyek a számítógép/okostelefon/táblagép távoli elérésére illetve vezérlésére szolgálnak (például: AnyDesk, TeamViewer, RustDesk)**, illetve senkinek ne adjon távoli hozzáférést a bankolásra használt eszközökhöz!
- Ne csatlakoztasson idegen, ismeretlen eredetű adathordozót (pendrive, memóriakártya, CD, DVD, külső merevlemez stb.) a számítógépéhez!
- Tiltsa le eszközei esetében az ismeretlen vezeték nélküli hálózatokhoz (Wi-Fi, Bluetooth) történő automatikus csatlakozást!
- Bankunk sem emailben, sem SMS-ben soha semmilyen körülmények között nem kér személyes, illetve bizalmas azonosító adatokat (pl. felhasználói azonosító, jelszó, telefonszám), és nem szólítja fel ezek megadására, egyeztetésére vagy megváltoztatására sem! Ha ilyet tapasztal (pl. látszólag a Banktól érkezik egy üzenet a Bank logójával/színvilágával, amely arról értesíti, hogy azonosítójával visszaélés történt, esetleg egy weboldal megnyitására kéri Önt), ne nyissa meg a linket, ne adja meg az adatait, illetve kérjük haladéktalanul értesítse erről a Bank telefonos ügyfélszolgálatát az alábbi elérhetőségeken: +36 1 473 4440, info@kdbbank.eu.
- Bankunk az ügyfelek mobiltelefon készülékére semmilyen NetBank applikációt, tanúsítványt, linket, stb. nem küld, nem telepít, és nem kéri erre az ügyfeleket sem. Az elektronikus banki szolgáltatások használatához kapcsolódóan Bankunk mobiltelefonra csak a megbízások aláírásához szükséges - 5 percig érvényes - kódot, valamint ViCA regisztrációs jelszót és kezdeti bejelentkezési jelszót küldi SMS-ben. Ha nem ezeket kapja meg, azt nem Bankunk küldte, ezért kérjük, törölje ki!
- **Bankunk a +36 70 706 0532 és a +36 30 344 4094 telefonszámokról küldi az SMS-eket**. Amennyiben másik feladó számról kap SMS-t, azt nem a Bankunk küldte!

- Kérjük, amennyiben fentiekhez hasonló tárgyú e-mailt vagy SMS-t kapna, akkor arra semmilyen formában ne válaszoljon, ne kattintson a levélben szereplő internetes hivatkozásokra (linkekre), és ne adja meg személyes adatait és az Ön azonosításához szükséges információkat (felhasználói azonosítóját, jelszavát, SMS-ben kapott kódját/jelszavát)!
- Böngészőjéhez használt kiegészítőket, bővítményeket (addon-ok, plugin-ek) használja korlátozottan! Ne telepítsen olyan bővítményt a böngészőjéhez, amelynek a fejlesztőjében/forgalmazójában nem bízik meg, vagy a bővítményt nem, vagy csak ritkán használja!
- Ismeretlen feladótól származó üzenetet, csatolmányt, linket minden esetben kezeljen kiemelt körültekintéssel, a levélre történő válaszadást vagy megnyitásukat pedig - amennyiben lehetséges - mellőzze!
- Az adatvesztés megelőzése céljából rendszeresen végezzen biztonsági mentést eszközén!

Internetbanki szolgáltatás használatával kapcsolatos biztonsági tanácsok:

- **Soha ne bankoljon nyilvános Wi-Fi hálózaton!** Saját eszközeit használja internetes bankolás céljára, és ne nyilvános (pl. internetkávézó, könyvtár) vagy sok különböző ember számára hozzáférhető eszközt!
- Minden esetben közvetlenül a KDB Bank által publikált címen, a bank honlapjáról (https://www.kdbbank.eu) indítsa el a KDB NetBank szolgáltatást, vagy közvetlenül gépelje be a NetBank oldalcímét: https://netbank.kdbbank.eu. Mindenkor ellenőrizze, hogy az internetbanki weboldal neve (https://netbank.kdbbank.eu) pontosan jelenik-e meg a böngésző címsorában. Különösen ügyeljen, hogy a cím a https:// karaktersorozattal kezdődik (nem pedig http:// sorozattal), továbbá ellenőrizze, hogy a böngészőben megjelent-e a biztonságos kapcsolatot jelölő kis lakatot formázó ikon! Nagyon fontos, hogy e-mailben kapott linken keresztül soha ne indítsa el a NetBank szolgáltatást!
- Ha azt tapasztalja, hogy a NetBank belépési felületen karbantartásra, korszerűsítésre vagy egyéb indokokra hivatkozó – olykor magyartalan, nehezen érthető, nyelvtanilag hibás – üzenetben adategyeztetés vagy bármilyen más célból személyes- vagy azonosító adatokat, jelszavakat, kódokat kérnek Öntől, azt semmiképpen ne adja meg!
- A NetBankból történő kilépéshez mindig a „Kilépés” menüpontot használja! Kilépést követően törölje a böngészőben az előzményeket (megnyitott weboldalak, gyorsítótár, sütik, aktív bejelentkezések)!
- Amennyiben a NetBankot nyilvános vagy nem megszokott helyről használja, javasoljuk, hogy amint lehetősége nyílik rá, belépési jelszavát egy biztonságosnak ítélt (jellemzően saját) számítógépen cserélje le!
- Tanúsítvány hibára történő figyelmeztetések esetében szakítsa meg a kapcsolatot és lépjen kapcsolatba Bankunkkal!
- Számítógépét bekapcsolva ne hagyja őrizetlenül és a használat felfüggesztésekor vagy befejezésekor lépjen ki az éppen látogatott weboldalról, vagy a használt programból, esetleg zárolja a képernyőt!
- Ne tartson nyitva más böngésző ablakot és ne futtasson a NetBank használata során más programokat! A használat után a böngészőt zárja be!
- A tranzakció hitelesítési SMS üzenet, valamint a belépési SMS üzenet tartalma minden esetben különböző, ezért javasoljuk, hogy minden esetben olvassa el a Banktól kapott SMS üzeneteket, mielőtt az abban szereplő kódot a NetBankban megadja!
- Amennyiben SMS kóddal ír alá, a tranzakciók aláírására szolgáló SMS szövegében ellenőrizze, hogy ténylegesen azok az adatok szerepelnek-e az üzenetben, amelyeket NetBankon/PC Kontakton megadott (egy átutalási tétel esetén összeg és kedvezményezett számlaszám, több tétel esetén tétel db szám/összesen összeg)! Amennyiben ViCA alkalmazással ír alá, jóváhagyás előtt az alkalmazásban lehetősége van tételesen ellenőrizni a megbízás adatait (összeg, kedvezményezett számlaszám). Csak ellenőrzést követően írja alá a megbízást az SMS kóddal/ViCA alkalmazással!

Jelszókezeléssel, biometrikus azonosítással kapcsolatos biztonsági tanácsok:

- Használjon összetett, legalább 8 karakter hosszú, kis- és nagybetűt, számot, speciális karaktereket tartalmazó jelszavakat! Ne használjon jelszavaiban személyes információkat (pl: név, születési dátum, telefonszám, lakcím, PIN kód stb.)! Ne használja ugyanazt a jelszót több oldalon!
- Javasolt rendszeresen, legalább háromhavonta megváltoztatni a használt jelszavát.
- Jelszavát soha senkinek ne adja meg! Ne írja le a jelszót, ne mentse azt számítógépére vagy mobil eszközére, a böngészőkben soha ne tárolja az internetes bankoláshoz szükséges jelszavakat!
- Mindig győződjön meg arról, hogy senki sem figyeli a jelszó megadása közben!

- **Amennyiben felmerül Önben a gyanú, hogy jelszava, kódja illetéktelen személy tudomásra jutott/juthatott, kérjük, hogy azonnal változtassa meg!**
- Felhívjuk figyelmét a felhasználónevének és jelszavának fokozott védelmére. Vizsgálja meg alaposan a kapott emaileket, sms-eket, és se felhasználónevét, se jelszavát soha ne adja meg sem elektronikus sem más csatornákon kapott kérésekre adott válaszban. Mindig ellenőrizze, hogy a belépési kísérletet vagy tranzakciót, melyre jóváhagyást várnak Öntől, valóban Ön kezdeményezte! Sose hagyjon jóvá ismeretlen kérést! **Ne feledje, hogy belépési adatainak kompromittálódása, idegen kézbe kerülése esetén nem csak a saját számlája, hanem azon egyéb számlák vonatkozásában is hozzáférést biztosíthat az online térben elkövetett csalások végrehajtóinak, amelyek fölött Ön meghatalmazott**. Így megtöbbszöröződhet az a potenciális kár, amelyet ezek a csalók okozhatnak a visszaéléseik során. Az Ön figyelmét is felhívjuk ezért arra, hogy csak olyan személy részére adjon meghatalmazást, akiben és akinek a digitális térben való tájékozottságában, kibertámadások elleni felkészültségében maximálisan megbízik.
- Amennyiben azt szeretné, hogy a ViCA alkalmazásban a biometrikus azonosítók (pl. ujjlenyomat) használata esetén csak az Ön azonosítójával lehessen a NetBankba/PC Kontaktba belépni/tranzakciókat jóváhagyni, akkor kérjük törölje le a készülékéről a más személyekhez tartozó rögzített biometrikus azonosítókat!
- Használja a Bankunk által nyújtott biztonsági SMS szolgáltatásokat (Teljes körű SMS szolgáltatás, Mini SMS szolgáltatás, Biztonsági bankkártya SMS szolgáltatás), és ügyeljen arra, hogy mobiltelefonja mindig Önnél legyen!

Mobil készülékekkel (okostelefon, táblagép) kapcsolatos biztonsági tanácsok:

- Használjon képernyőzár feloldás elleni védelmet, ehhez állítson be kellően erős, legalább 5 jegyű PIN kódot, jelszót, egyedi mintázatot vagy biometrikus azonosítót (pl. ujjlenyomat, arclenyomat) és állítsa be az automatikus képernyőzárat is!
- Ne telepítsen internetről közvetlenül letöltött alkalmazást/szoftvert eszközeire, helyette használja a hivatalos forrásokat vagy terjesztési csatornákat (pl. Android eszközök esetén Google Play áruház, iOS eszközök esetén App Store)!
- Mobileszközének gyári jogosultsági beállításait ne törje fel (root, jailbreak), mivel ez az eszköz általános védelmi szintjét gyengíti!
- Minden esetben ellenőrizze a telepíteni kívánt alkalmazás által használni kívánt jogosultságkérelmeket és szolgáltatásokat, és amennyiben egy alkalmazás a profiljába nem illeszkedő funkciókat is használni kíván (pl. háttérkép alkalmazás SMS-t akar küldeni), akkor ne folytassa a telepítést! Ezt az ellenőrzést az alkalmazások frissítésekor is mindig végezze el, mert az új alkalmazás verziók gyakran többlet jogosultságokat kérnek!
- Javasolt a nem használt szolgáltatásokat (Wi-Fi, Bluetooth, GPS, NFC) kikapcsolni, és csak tényleges használat idejére engedélyezni.
- Amennyiben az eszköz operációs rendszere vagy az eszköz gyártója támogatja, javasolt titkosítani az eszköz háttértárolóin tárolt adatokat.

Felhívjuk szíves figyelmét a Magyar Nemzeti Bank által kiadott Pénzügyi Navigátor füzetekben található elektronikus banki szolgáltatásokkal kapcsolatos biztonsági tanácsokra is:

- https://www.mnb.hu/fogyasztovedelem/bankszamlak/elektronikus-banki-szolgaltatasok/e-banking-biztonsag
- https://www.mnb.hu/fogyasztovedelem/bankszamlak/elektronikus-banki-szolgaltatasok/internetes-csalasok

Felhívjuk figyelmét az alábbi oldalakon található biztonsági tanácsokra is:

- KiberPajzs: https://kiberpajzs.hu/
- Nemzeti Kibervédelmi Intézet: https://nki.gov.hu/it-biztonsag/tartalom/tudaskozpont/

Ha a fentiekkel kapcsolatban bármilyen kérdése merülne fel, továbbá amennyiben anomáliáról vagy biztonsági kérdéseket érintő ügyekről kívánja értesíteni a Bankot, úgy kérjük keresse telefonos ügyfélszolgálatunkat banki munkanapokon a +36 1 473 4440-es telefonszámon, vagy emailben az info@kdbbank.eu címen.

Tisztelettel:
KDB Bank Európa Zrt.