

Tisztelt Ügyfelünk!

Bankunk kiemelt figyelmet fordít arra, hogy Ön a pénzügyeit nemcsak gyorsan, kényelmesen és hatékonyan, de biztonságosan is kezelhesse. A Bank elektronikus csatornáinak mindennapi működtetése során magasfokú biztonságra törekszünk a NetB@nk és a MobilBank felületünkön is!

Az elektronikus bankolás az előnyei mellett számos kockázattal is jár, ezért a digitális biztonság kiemelt jelentőséggel bír. Az online térben sajnálatos módon ma már mindennaposak a visszaélések. Fontos tudni, hogy minden internetre csatlakozott készülék visszaélésekre ad lehetőséget a csalók számára.

Felkészültséggel, odafigyeléssel és előrelátással csökkenthető annak az esélye, hogy bárki kiberbűncselekmény áldozatává váljon!

Tanácsok a biztonságos elektronikus bankoláshoz:

- Ha NetB@nk bejelentkezése során **szokatlan dolgot tapasztal, azonnal zárja be a NetB@nket**, szakítsa meg az internetkapcsolatot és haladéktalanul vegye fel a kapcsolatot Bankunkkal! **Soha ne kattintson ismeretlen forrásból származó, Önnek ismeretlen linkekre!**
- A Bank hivatalos oldalát mindig annak teljes begépelésével hívja elő az internet böngészőben, ne használja a google keresőjét. Mindig **ellenőrizze, hogy a honlap** url címe megegyezik-e a Bank hivatalos oldalának címével (**www.mbfdunabank.hu**).
- Bankunk **soha nem kér** sem e-mailben, sem telefonon, sem SMS-ben Öntől NetB@nk belépő és/vagy bankkártya adatokat, jelszavakat, PIN-kódokat, sem más **bizalmas jellegű adatot**.
- Mindig ellenőrizze a Banktól érkező SMS-ek tartalmát. Ha MobilBank telepítésére vonatkozó kódot lát, de **MobilBank telepítését Ön nem kezdeményezte, azonnal hívja a Bankot!**
- A Bank **soha nem kéri Öntől**, hogy „biztonsági” vagy „biztonságos” számlára utalja el a pénzét, mert azok veszélyben vannak! (ilyen kifejezés nem létezik a banki szóhasználatban)
- A Bank **soha nem kéri Ügyfelét** arra, hogy **ún. távoli hozzáférést biztosító programot** (pl. Anydesk, Teamviewer, Avica) **telepítsen** informatikai eszközeikre. Ha bárki a Bank nevében indított hívás keretében erre kéri Önt, azonnal bontsa a vonalat, ne engedelmeskedjen a telefonálónak, mert ezzel illetéktelenek számára hozzáférést biztosíthat a készüléken tárolt adataihoz! Telefonos kérésre ne telepítsen semmit készülékére!
- **Ne adja meg senkinek NetB@nk belépéséhez szükséges adatait!** Javasoljuk, hogy Internet böngészője számára ne engedélyezze a belépési adatok mentését.
- **Ne adja meg adatait amennyiben nyereményjátékokra hivatkozva kéri Öntől!** Amennyiben utalni szeretnének az Ön számlájára, ahhoz csak a számlaszámát kell ismernie az összeget elutalónak, más adataira nincs szüksége.
- A fizetési számlához kapcsolódó új meghatalmazott megadása vagy korábbi meghatalmazott esetén a részére adott elektronikus csatornához való hozzáférés kompromittálódása több veszélyt is rejt. Egy meghatalmazotti jog adásakor fontolja meg, hogy valóban szükség van-e arra, hogy a meghatalmazott a bankszámlájához elektronikus csatornán hozzáférhessen.

A Bank mobilbanki applikációjába több biztonsági elemet is beépítettünk, ilyen például:

- új MobilBank regisztráció a Bank Call Centerének hívása után fejezhető be;
- a MobilBanki alkalmazást egy felhasználó csak egy eszközén tudja használni;
- újra bejelentkezés szükséges a mobilappba, ha már nem aktív az alkalmazás;
- mPIN kód (mobilbanki hatszámjegyű, egyedi azonosító kód) alkalmazása;
- biometrikus azonosítás;
- az eszközregisztráció törlésének gyors lehetősége;
- a képernyőről készíthető fotó, képernyőtükrozés tiltása.

A beépített biztonsági funkciók mellett elengedhetetlen, hogy Ön is figyelmet fordítson a banki applikációk biztonságos használatára!

- Törekedjen a **biztonságos internet kapcsolatra!** Használja telefonja **képernyőzár** funkcióját! A képernyőzár feloldásához használjon legalább 5 számjegyű PIN kódot, vagy más biztonságos megoldást.

- Adjon **nehezen kitalálható mPIN kódot**, ne használjon számsorozatokat, ismétlődő számokat, születési dátumokat!
- Használjon **biometrikus azonosítást**. Mivel a biometrikus azonosítás során a készülék az Ön ujjlenyomatának/arcának bizonyos jellemzőit vizsgálja, biztonságosabbnak tekinthető, mint a jelszó használata. Az ujjlenyomatunk/arcunk egyedi és nehezen hamisítható, míg a jelszó kileszhető, akár kitalálható, könnyebben kitudódhat.
- **Ne tárolja** semmilyen formában (képként, hívószámként elmentve) azonosítási adatait, jelszavát a mobiltelefonján! Fordítson figyelmet az eszközein tárolt adatai titkosítására!
- Új telefon használata esetén **régi készülékéről törölje** az eszközregisztrációt és az applikációt!
- Készüléke elvesztése esetén kérje az **eszközregisztráció törlését** fiókunkban!
- Használjon naprakész, frissített **vírusvédelmi szoftvert**, végezzen rendszeres biztonsági mentést.
- Alkalmazza tudatosan a NetB@nk és MobilBank limitbeállítását! Az átutalások, a bankkártyás fizetések és készpénz felvételek limitösszegét Ön is beállíthatja. Javasoljuk a **napi limit** beállítását, az Önnek megfelelő legalacsonyabb értékekre állítsa be.
- A fizetési számlához kapcsolódó új meghatalmazott megadása vagy korábbi meghatalmazott esetén a részére adott elektronikus csatornához való hozzáférés kompromittálódása több veszélyt is rejtethet. Egy meghatalmazotti jog adásakor fontolja meg, hogy valóban szükség van-e arra, hogy a meghatalmazott a bankszámlájához elektronikus csatornán hozzáférhessen.
- Amennyiben nem biztos bankkártyája hollétét illetően, állítsa át bankkártyája státuszát **felfüggesztett** állapotra. A bankkártya applikáción keresztüli felfüggesztése nem helyettesíti annak letiltását!
- Bankkártya adatait csak megbízható kereskedői oldalon adja meg! A bankkártyával történő, ismétlődő fizetések érdekében, az adatait csak megbízható oldalon (pl. közüzemi számla fizetések) mentse el.
- Külföldre utazás előtt, jelezze a Banknak, a bankkártyáját külföldi használatát, ezzel megelőzhető a kártya zárolása a szokatlan külföldi tranzakciók miatt!
- Online vásárláskor elkövetett csalások egyik esete, amikor a kifejezetten csalárd szándékú online kereskedő a termékértékesítés során **elrejtje a termékvásárlással egybekötött, előfizetésre vonatkozó információkat**. Egy, jellemzően külföldi weboldalon, vonzó áron kínálnak terméket vagy szolgáltatást, ám a csalárd kereskedő elrejtje azt az információt, hogy a termék megvásárlásával (és a vásárlás erős ügyfélhitelesítéses jóváhagyásával), valójában ismétlődő terhelést engedélyezett a vásárlóval. A vásárló – szándéka ellenére – jóváhagyja, hogy ismétlődően, például hetente néhány ezer forinttal terheljék meg újra és újra az bankszámláját. Figyelem! Az online vásárlásnál az erős ügyfélhitelesítés nem csak egy egyszeri fizetés jóváhagyásához kapcsolódhat, hanem a fizetéssel egyben a felhatalmazását is adhatja a kereskedőnek, hogy az Ön további jóváhagyása nélkül, ismétlődően megterhelje az Ön számláját! Az online ajánlatok sokszor valóban kedvezőek, de óvakodjon a csalóktól!
- Kövesse a számláján történő tranzakciókat és az aktuális egyenlegét a Bank valós idejű üzenetküldő rendszereivel! A számláján történt tranzakciókról azonnali SMS és/vagy Push üzenetet kap. A MobilBank-ból küldött Push üzenetküldés Önnek ingyenes, javasoljuk ennek beállítását.

A Bank honlapján folyamatosan tájékoztatja Ügyfeleit a csalások legújabb formáiról és tanácsokat ad a csalások elkerülésére.

A leírt tanácsok figyelmen kívül hagyása a számláján lévő szabad és ahhoz kapcsolódó lekötött pénzének részleges vagy teljes elvesztéséhez vezethet!

Központi információ

☎: 9022 Győr, Árpád út 93. ☎: 96 / 550-720 web: www.mbhduabank.hu email: kozpont@mbhduabank.hu

Ha azt gyanítja, hogy kikerültek az internetbanki, mobilbanki fiókjának adatai, vagy a bankkártyaadatok, azonnal vegye fel a kapcsolatot a bankjával!
Ha megpróbálták megkárosítani, minden esetben tegyen bejelentést a bankjánál és a rendőrségen, még akkor is, ha a csalási kísérlet nem volt sikeres!



KiberPajzs
Védje le a pénzügyét

Vértezz fel magát a kiber csalásokkal szemben, látogasson el a KiberPajzs honlapra! (kiberpajzs.hu)