Adat- és rendszerbiztonsági feltételek, ügyfél oldali felelősség

Az OTP Bank az online kölcsönigénylési, illetve a VideóBankon történő ügyfél-azonosítási és szerződéskötési folyamatában számos olyan védelmi intézkedést alakított ki, amelyek a felhasználó biztonságát szolgálják. Emellett azonban az Ön közreműködésére is feltétlenül szükségünk van ahhoz, hogy a rendszer használatából eredő kockázatot minimálisra tudjuk csökkenteni.

A leírásunk összhangban van a Magyar Nemzeti Bank ajánlásával, valamint általános tanácsaival, amely felhívja a figyelmet az internetes banki szolgáltatások biztonságos, körültekintő használatára.

Számítógép védelme

Az igénylése során Ön a személyes adatait rögzíti az OTP Bank erre a célra kialakított, biztonságos Online áruhitel igénylési felületén.

Személyes adatai védelme érdekében javasoljuk, hogy a szolgáltatás igénybevételekor és általában az Internet használatakor a számítógépe védelme érdekében a lehető legnagyobb gondossággal járjon el, az esetleges vírusfertőzésekkel, betörési kísérletekkel és "trójai programokkal" szemben védje számítógépét tűzfalakkal, víruskeresőkkel.

A vírusok károsíthatják számítógépét, tönkre tehetik a tárolt adatokat, de sajnos az sem kizárt, hogy bizalmas adatait, valamint a használat során alkalmazott kódokat illetéktelenek részére juttatják el, amelyekkel vissza is élhetnek.

Rendszeresen töltse le az Ön által használt operációs rendszerhez, böngészőhöz elérhető frissítéseket, javító verziókat.

Az Ön számítógépére illetéktelenül bekerült programok által az adatok integritásában, vagy kezelésében beálló, az internetes szolgáltatás használata során felmerülő problémákkal és károkkal kapcsolatosan – mivel azok érdekkörén kívül állnak – az OTP Bank semmilyen felelősséget nem vállal.

Javasoljuk, hogy az alkalmazott böngésző adatbiztonsági beállításait lehetőség szerint a szükséges legnagyobb biztonságot garantáló szintre állítsa be. Ebben az esetben a program figyelmezteti Önt minden, a böngésző használata során potenciálisan kárt okozó tartalom megnyitása előtt.

Mobil készülékek, eszközök védelme

Az új generációs mobil készülékek (pl. okostelefonok, táblagépek) – ugyanúgy, mint a számítógépek és minden egyéb internetre csatlakozott eszköz – kiszolgáltatottak, célpontot jelentenek a visszaéléseknek, ezért fontos tisztában lenni az ilyen készülékek használatának veszélyeivel és a kockázatok csökkentésének lehetőségeivel.

- Ne tároljon személyes adatokat a készüléken vagy annak bővítő kártyáján. Állítsa be úgy internet böngészőjét is, hogy az automatikusan ne tároljon el adatokat.
- Használjon kellően erős PIN kódot a mobil készülékbe történő belépéshez, illetve a készülék zárolásának feloldásához. A készülék rövid időn belül (pl: 3-5 percen belül) automatikusan zárolódjon le.
- Jailbreakelt vagy rootolt telefonok használatát lehetőleg mellőzze, mert a feltöréssel a gyártó védelmi mechanizmusa kerül kiiktatásra, így a gyártó által nem engedélyezett, kártékony kódok, alkalmazások is feltelepülhetnek a készülékre, melyek például célzottan a banki adatokra vadászhatnak.
- **Javasoljuk a mobilkészülékek operációs rendszerének rendszeres frissítését.**
- Kártékony kódok (trójai program, vírus, malware) terjedésének megelőzése érdekében csak hivatalos forrásból töltsön le készülékére alkalmazásokat, nem biztonságos forrásból származó alkalmazások letöltését, linkekre történő kattintását mellőzze.
- Javasoljuk, hogy kiegészítő védelemként antivírus szoftvert is használjon, melyek a trójai, malware és egyéb típusú károkozók ellen nyújtanak védelmet. A legtöbb antivírus cég már rendelkezik mobil készülékekre szánt megoldásokkal is. A vírusvédelmi megoldásokról itt kaphat bővebb információt.
- Ha a készüléken lévő bluetooth funkció nincs használatban, kérjük, kapcsolja ki.
- Kérjük, olvasás után törölje az OTP Banktól érkezett SMS-eket a készülékről.

Személyes adatok megadása a banki honlapon

Az igénylése során Önnek meg kell adnia a személyes adatait az erre a célra kialakított igénylési felületen.

A HTML technológiából adódó sajátosságok miatt a felhasználó által látogatott oldalak tárolásra kerülnek a számítógép Temporary Internet Files (Ideiglenes Internet Fájlok) könyvtárában. A böngészők alapértelmezés szerinti beállítása mellett ez minden HTML alapú internetes oldal esetében megtörténik. Amennyiben Ön szolgáltatásunkat nem a saját gépén veszi igénybe, javasoljuk, hogy az *OTP Áruhitel belépés* oldalon ne engedélyezze az ideiglenes internet fájlok tárolását. Természetesen akkor, ha szolgáltatásunkat olyan számítógépről veszi igénybe, mely az Ön ellenőrzése alatt áll, az említett biztonsági lépések alkalmazása nem feltétlenül indokolt, hiszen elegendő a banki oldal által biztosított védelmi eljárás.

Félbehagyott vagy megszakadt igénylések kezelése

Önnek lehetősége van arra, hogy megkezdett online kölcsönigénylését félbehagyja, vagy a megszakadt VideóBanki hívást egy későbbi időpontban folytassa a már megadott adataival.

Ennek érdekében az igénylési felületen egy jelszót szükséges megadnia, így az igénylése során megadott e-mail címére küldött egyedi link segítségével 5 napon belül befejezheti igénylését jelszavának beírásával.

Jelszó kezelés

Az online kölcsönigénylés során Önnek az előzőekben említett félbehagyott igénylés vagy megszakadt VideóBanki hívás befejezéséhez szükséges jelszó.

Tanácsok a jelszó kezeléséhez

- A jelszavait kezelje bizalmasan, azokat senki tudomására ne hozza.
- A jelszót se kódolt, se kódolatlan formában, se noteszba, se mobiltelefonba ne jegyezze fel.