

MyConcorde mobilapp felhasználói tájékoztató

Concorde Értékpapír Zrt.

Tartalom

1.	Felhasználói tájékoztató	3
1.1	Alkalmazás indítása	3
1.1.1	Alkalmazás telepítése	3
1.1.2	Alkalmazás elindítása	3
1.2	Bejelentkezés után az ügyfelek által elérhető menüpontok.....	5
1.2.1	Tartalom	5
1.2.2	Portfólió.....	6
1.2.3	Tranzakciók.....	7
1.3	Beállítások	8
1.3.1	Jelszó módosítás.....	9
1.3.2	Biometrikus azonosítás bekapcsolása	10
2.	Technikai és biztonsági tájékoztatás	11
2.1	Fogalmak	11
2.2	Technikai feltételek	11
2.3	Általános biztonság.....	12
2.4	Jelszókezeléssel, bankkártya adatokkal kapcsolatos biztonság	12
2.5	Hordozható eszközökkel (táblagép, okostelefon) kapcsolatos biztonság.....	13
2.6	Elektronikus elérhetőségek védelme	13
2.7	Teendők technikai, biztonsági problémák és incidensek esetén	14

1. Felhasználói tájékoztató

Jelen segédlet célja, hogy bemutassa a MyConcorde alkalmazás okostelefonon elérhető applikáció felépítését és használatát.

1.1 Alkalmazás indítása

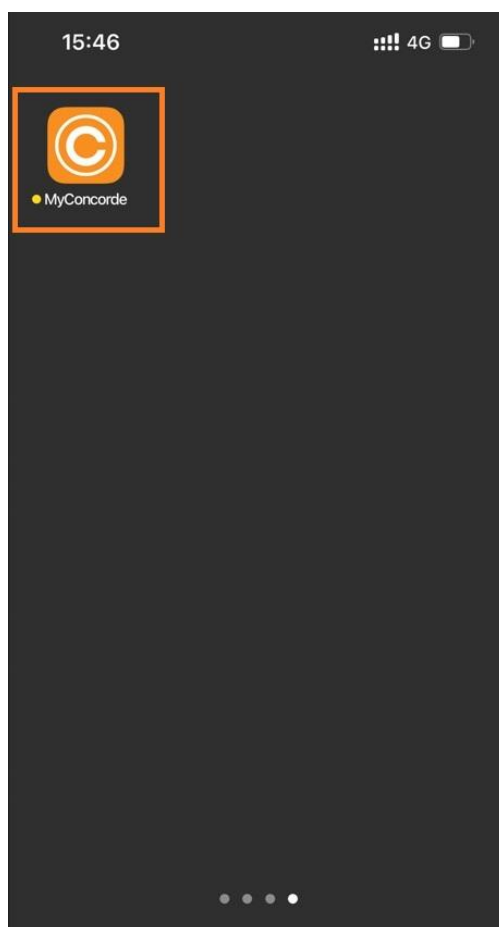
1.1.1 Alkalmazás telepítése

Töltse le készülékére a MyConcorde alkalmazást az App Store-on vagy a Google Play-en keresztül, majd telepítse.

A Concorde a MyConcorde alkalmazást kizárólag az AppStore-ban és a Google Play áruházban teszi közzé. Kérjük, hogy kizárólag az itt közzétett alkalmazást használja. Ismeretlen forrásból a MyConcorde alkalmazást ne töltsse le, ne telepítse, azokért a Concorde felelősséget nem vállal.

1.1.2 Alkalmazás elindítása

Kattintson a MyConcorde alkalmazás ikonjára



FIGYELEM! Felhívjuk szíves figyelmét, hogy a regisztrációhoz kötött szolgáltatások eléréséhez Önnek a Concorde-nál vezetett számlával kell rendelkeznie, valamint ahhoz kapcsolódó elektronikus szolgáltatást kell igényelnie.

Első bejelentkezéskor a szolgáltatás igénylésekor rögzített mobiltelefonszámra küldött megerősítő SMS kód megadásával lehet hozzárendelni a készüléket a MyConcorde szolgáltatáshoz.

17:26



BEJELENTKEZÉS

Felhasználónév
Felhasználónév

Jelszó
Jelszó 

Elfelejtett jelszó

Bejelentkezés



Bejelentkezés Face ID azonosítással

1.2 Bejelentkezés után az ügyfelek által elérhető menüpontok

1.2.1 Tartalom

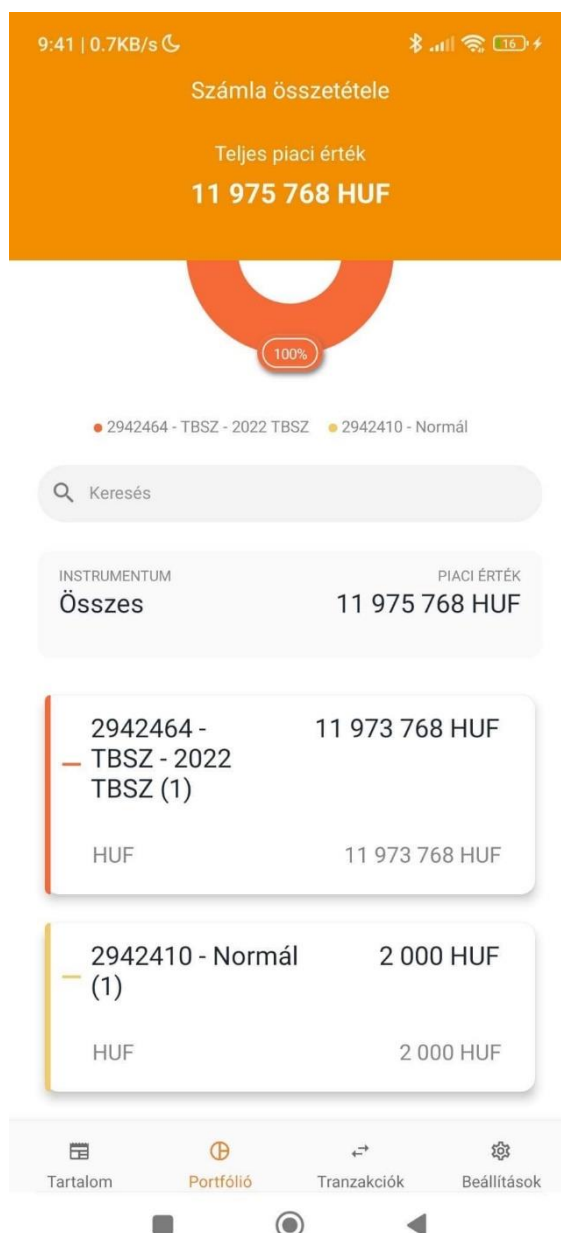
Ebben a menüpontban találhatjuk a Concorde Zrt. Által készített elemzéseket, friss híreket, heti érdekességeket, blog és podcast ajánlókat.



1.2.2 Portfólió

A Portfólió menüpontban találjuk, portfóliónk részletes adatait illetve lehetőség van arra, hogy a számlatulajdonos az összes számláját egyszerre megtekinthesse. A teljes piaci érték felületen számláink összesített értékét találhatjuk.

A számlaválasztó segítségével külön-külön is megtekinthető a számláink eszközosztály, illetve pénznem szerinti tovább bontása is.



1.2.3 Tranzakciók

A Tranzakciók menüpontban találhatjuk a folyamatban lévő még el nem számolt tranzakciókat, illetve a már lezárt tranzakcióink történetét

A felület alapértelmezetten az elmúlt 2 hónap tranzakcióit mutatja melyen a szűrés gombra kattintva változtathatunk.

A szűrőben ügyfélszámlákra, különböző tranzakció típusokra, illetve időintervallumra tudunk szűrni.



9:43 | 1.6MB/s

Tranzakciók

Folyamatban Lezárt

2022.10.07 - 2022.12.07 X Szűrés

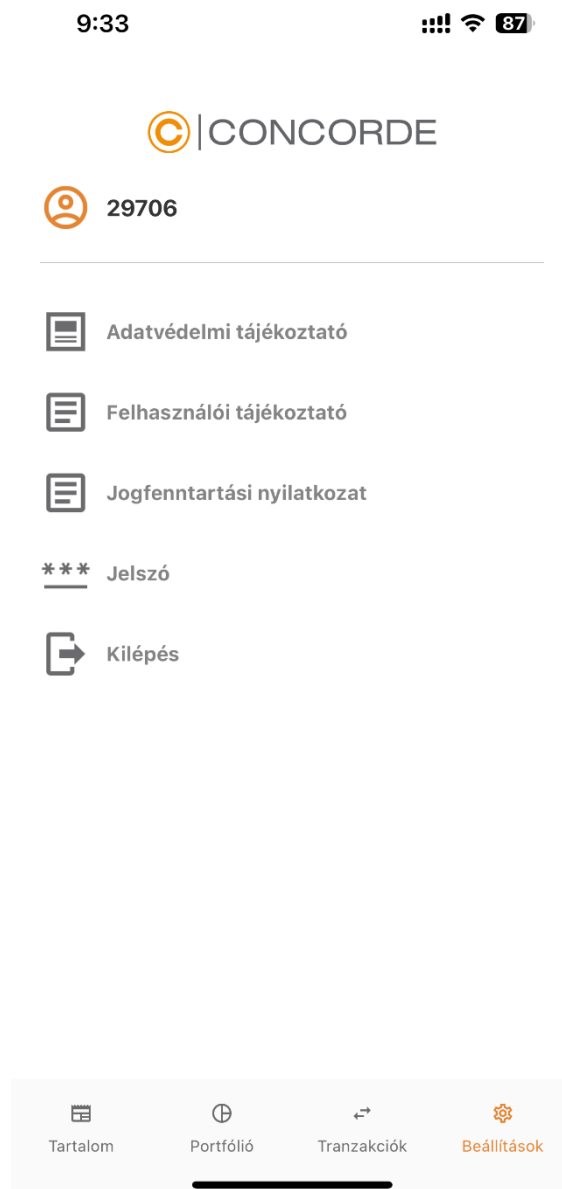
LEZÁRT TRANZAKCIÓK

Befektetővédelmi hozzájárulás MAGYAR FORINT	- 998 HUF 2022.12.06
Letétkezelési díj bps MAGYAR FORINT	- 230 HUF 2022.12.06
Utalás jóváírás MAGYAR FORINT	7 250 000 HUF 2022.11.25
CFD alapletét képzés - felszabadítás ConcordeTrader MAGYAR FORINT	2022.11.11
Utalás jóváírás MAGYAR FORINT	4 700 000 HUF 2022.11.11
Befektetővédelmi hozzájárulás MAGYAR FORINT	- 2 HUF 2022.11.03

Tartalom Portfólió **Tranzakciók** Beállítások

1.3 Beállítások

Az Egyéb menüpontban elolvashatjuk az cég üzletszabályzatát, az Üzenetek gombra kattintva elolvashatóak a korábban kapott üzenetek, a beállítások alatt pedig megváltoztathatjuk jelenlegi jelszavunkat illetve bekapcsolhatjuk a biometrikus azonosítással történő bejelentkezést.

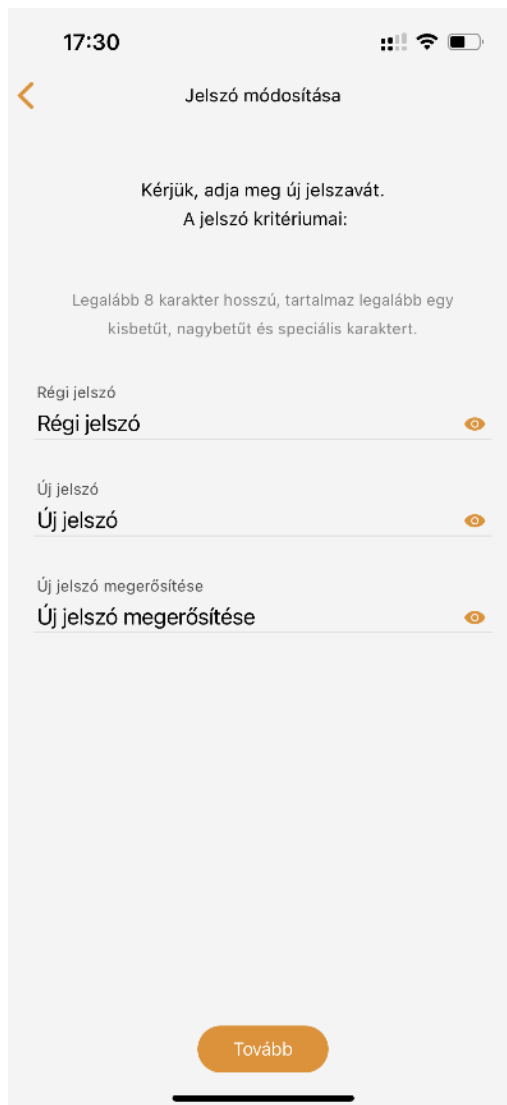


1.3.1 Jelszó módosítás

A Beállítások menüpontban a Jelszó módosításra kattintva változtathatjuk meg jelszavunkat.

A jelszavunk megváltoztatásához meg kell adnunk a jelenlegi jelszavunkat, majd pedig meg kell adnunk az új jelszót és meg kell erősítenünk azt.

A megadott jelszónak legalább 8 karakter hosszúnak kell lennie és tartalmaznia kell legalább egy kisbetűt, nagybetűt és speciális karaktert.



17:30

Jelszó módosítása

Kérjük, adja meg új jelszavát.
A jelszó kritériumai:

Legalább 8 karakter hosszú, tartalmaz legalább egy
kisbetűt, nagybetűt és speciális karaktert.

Régi jelszó
Régi jelszó

Új jelszó
Új jelszó

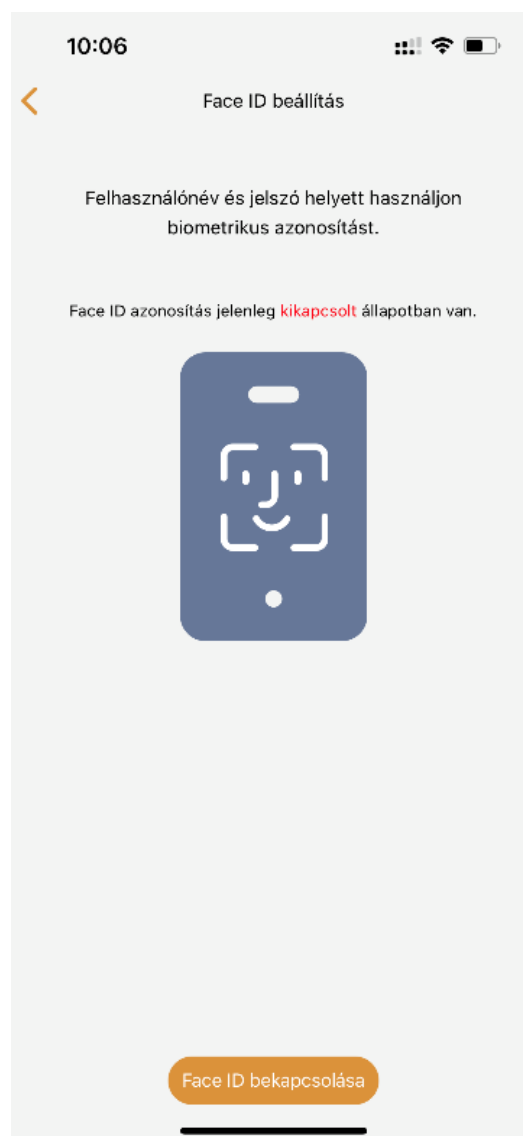
Új jelszó megerősítése
Új jelszó megerősítése

Tovább

1.3.2 Biometrikus azonosítás bekapcsolása

Ha jelszó helyett biometrikus azonosítással szeretnénk belépni az alkalmazásba, ezt a beállítások menüpontban a Biometrikus azonosítás bekapcsolásával tehetjük meg.

A biometrikus azonosítás bekapcsolásához megerősítésképpen meg kell adnunk jelenlegi jelszavunkat. Ezután a biometrikus azonosítás aktívvá válik.



2. Technikai és biztonsági tájékoztatás

A fejezet célja, hogy a MyConcorde mobilapp rendszerkövetelményeit meghatározza, valamint a szolgáltatás biztonságos használatáról tájékoztasson. A Concorde a szolgáltatásainak kialakítása során a különböző hatóságok (MNB, NAIH) hatályos ajánlásait és elvárásait vette figyelembe és közvetíti a felhasználók felé.

Felhívjuk a szolgáltatások felhasználóinak figyelmét, hogy a felhasználók felelősége a használt készülékek, eszközök és felhasználói hozzáférések (felhasználói név, jelszó) megfelelő szintű biztonsági védelméről gondoskodni!

2.1 Fogalmak

MyConcorde mobilapp: A Concorde által nyújtott, az Ügyfelek részére okostelefonon igénybe vehető pénzügyi szolgáltatás.

Felhasználónév: 6 jegyű, numerikus azonosító kód, amely a Felhasználó egyedi azonosítására szolgál.

Jelszó: Alfabetikus azonosító kód, amely a Felhasználó egyedi azonosítására szolgál.

Biometrikus azonosító: a mobileszközön alapértelmezettként beállított ujjlenyomat (TouchID), arcfelismerés (FaceID) vagy írisz leolvasás, amelyet a Felhasználó a Concorde mobilapp belépéshez, valamint tranzakciók aláírásához használhat.

Kétfaktoros hitelesítés (2FA): egy identitás- és hozzáférés-kezelési biztonsági módszer, amely kétféle azonosítást igényel az erőforrások és az adatok eléréséhez. A kétfaktoros hitelesítés lehetővé teszi a legsérülékenyebb információk védelmének biztosítását.

2.2 Technikai feltételek

Az alkalmazást az alábbi eszközökön használhatja:

- iPhone 6S és későbbi iPhone készülékek, amelyek legalább iOS 13-as operációs rendszerrel rendelkeznek;
- olyan Android operációs rendszerű okostelefonok, amelyeken legalább Android 5.0 verziójú operációs rendszer fut.
- alkalmazásunk jelenleg nem elérhető azokon a 2019 őszétől megjelenő Huawei telefonokon (pl. Huawei Mate 30, P40), amelyek nem támogatják a Google Play Services (GPS) ökoszisztémát.
- Az alkalmazás nem használható módosított (ún. rootolt vagy jailbreakelt) operációs rendszerű okostelefonokon.

2.3 Általános biztonság

- Használjon naprakész vírusvédelmi, tűzfalvédelmi programokat eszközeinek (számítógép, mobiltelefon, táblagép) vírus, kémprogram, kártékony szoftverek elleni védelme érdekében!
- 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!
- Kizárólag legális szoftvereket használjon eszközein, melyekre ne telepítsen ismeretlen forrásból származó, kétes eredetű alkalmazásokat!
- Tiltsa le eszközei esetében az ismeretlen vezeték nélküli hálózatokhoz (Wi-Fi, Bluetooth) történő automatikus csatlakozást!
- Kérjük, azonnal vegye fel a kapcsolatot a Concorde telefonos ügyfélszolgálatával, amennyiben látszólag a Concorde-tól érkező személyes vagy bizalmas adatok (név, telefonszám, E-csatorna azonosító, jelszó) megadására felszólító üzenetet kap, mert a Concorde ügyfeleitől ilyen jellegű adatokat soha nem kér e-mail üzenetben vagy SMS-ben!
- Ismeretlen feladótól származó üzenetet, csatolmányt, linket minden esetben kezeljen kiemelt körtekintéssel, a levélre történő válaszadást vagy megnyitását pedig - amennyiben lehetséges - mellőzze!

2.4 Jelszókezeléssel, bankkártya adatokkal kapcsolatos biztonság

- Ne használjon jelszavaiban személyes információkat (születési dátum, telefonszám, lakcím, kedvenc háziállat, házastárs neve, PIN vagy TPIN kód stb.), valamint szótár alapú szavakat!
- A rendszer megköveteli a komplex jelszavak használatát. A jelszó hossza minimum 8 karakter, melyben kis és nagybetűnek és minimum 2 számnak kell szerepelnie.
- Törekedjünk olyan jelszó megadására, mely nem kapcsolható hozzánk
- A szolgáltatás igénybevételéhez használt azonosítót, jelszót ne adjuk meg senkinek
- A jelszavakat csak biztonságos formában tároljuk, például jelszókezelő alkalmazás segítségével. A felhasználói jelszavakat csak titkosított formában tároljuk
- A Concorde soha nem kéri semmilyen csatornán a felhasználóktól, hogy osszák meg a jelszavakat. Kérjük jelszavát ne ossza meg senkivel!
- Kérjük, hogy a felhasználói jelszót rendszeresen, legalább háromhavonta változtassa meg. Amennyiben arról értesül, hogy felhasználói hozzáférését kompromitálták, akkor haladéktalanul változtassa meg felhasználó jelszavát és jelezze azt a Concorde elérhetőségein.

- Javasoljuk, hogy minden rendszerhez használjon egyedi, generált jelszót. Lehetőleg ne használja különböző rendszerekhez ugyanazt a jelszót, mert így nagyobb a lehetősége a visszaéléseknek.
- Amennyiben elfelejtené jelszavát, lehetősége van új jelszó igénylésére. Az új jelszót a Concorde ügyfélszolgálaton keresztül, telefonon kérheti. Biztonsági okokból kollégánk Önt azonosítani fogja és új, átmeneti hitelesítő jelszót fog küldeni a korábban megadott telefonos elérhetőségére.
- 3 sikertelen bejelentkezési kísérlet után a rendszer átmenetileg 1 órára letiltja a hozzáférést. Amennyiben elfelejtette jelszavát kérjük hívja az ügyfélszolgálatot új jelszó igényléséhez.
- Bankkártya adatait (bankkártyaszám, lejárat dátum, CVV/CVC2 kód) csak olyan weboldalakon adja meg, amelyeket ismer és megbízhatónak tart. E-mail üzenetben vagy bármilyen felugró felhívás során soha ne adja meg ezeket!

2.5 Hordozható eszközökkel (táblagép, okostelefon) kapcsolatos biztonság

- Lehetőleg ne használja a szolgáltatás használatra azt a hordozható eszközt, amelyre a Concorde-tól kapott SMS üzeneteket is kapja!
- Javasolt, hogy az eszköz gyári jogosultság beállításait ne változtassa meg; ne root-olja, ne jailbreak-elje az eszközt!
- Használjon képernyőzár feloldás elleni védelmet (PIN kód, egyedi mintázat)!
- Ne tároljon személyes adatokat (bankkártyaszám, PIN vagy TPIN kód) a készüléken!
- Ne telepítsen internetről közvetlenül letöltött alkalmazást/szoftvert eszközeire, helyette használja a hivatalos forrásokat vagy terjesztési csatornákat (pl. Google Play, Apple Appstore, Windows Market)!
- 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 (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.

2.6 Elektronikus elérhetőségek védelme

A Concorde kiemelt funkciók végrehajtásához (pl. adatmódosítás) is mobil telefonszámra küldött SMS hitelesítő kód segítségével ellenőrzi az Ön közreműködését csalás és visszaélések megelőzése miatt.

A Concorde biztonsági megfontolásból az elérhetőségek változásáról emailben értesítést küld az Ön részére. Amennyiben nem Ön kezdeményezte a módosítását, kérjük haladéktalanul jelezze ezt a Concorde ügyfélszolgálatának elérhetőségein! Kérjük ellenőrizze, hogy elektronikus levelező rendszere nem kezeli a Concorde által küldött leveleket levélszemétként!

Felhívjuk figyelmét, hogy az ön birtokában lévő személyes eszközök és hozzáférési információk védelme az Ön felelőssége!

Eszközeinek és személyes elérhetőségeinek védelme érdekében kérjük gondoskodjon azok megfelelő védelméről az alábbiak végrehajtásával:

- Ne használjon publikusan elérhető számítógépet és hálózatot
- Eszközeit mindig lássa el jelszavas védelemmel és azokat használat után mindig kapcsolja ki, vagy zárolja le
- Telepítsen eszközeire vírus és kártékony kód elleni védelmet
- Rendszeresen telepítse az eszközein található szoftverek biztonsági frissítéseit
- Használjon eszközei védelmére tűzfal megoldást

2.7 Teendők technikai, biztonsági problémák és incidensek esetén

Amennyiben problémát tapasztal, az esetleges csalások és visszaélések megelőzése érdekében kérjük haladéktalanul értesítse ügyfélszolgáلتunkat az www.con.hu/kapcsolat/ oldalon található elérhetőségeken.