ONEY NETBANK BIZTONSÁGI ELŐÍRÁSOK ÉS TECHNIKAI FELTÉTELEK

1. A BIZTONSÁGRÓL

A Társaság célja, hogy a NetBank szolgáltatáson végrehajtott ügyintézés a lehető legbiztonságosabb legyen, ehhez azonban az Ügyfél elővigyázatosságára, közreműködésére is szükség van.

A Társaság nem vizsgálja, és nem felügyeli az Internet működését, annak biztonságáért nem felelős. Az internetes csalások bűncselekménynek minősülhetnek.

1.1. A kapcsolat automatikus bontása

Többszöri sikertelen bejelentkezést, illetve az aláírást igénylő műveletek többszöri sikertelen jóváhagyását követően a rendszer biztonsági okokból letiltja a NetBank hozzáférést az Ügyfél számára. Ekkor telefonos ügyfélszolgálat (06 1 888 0000) felhívásával kérheti a letiltás feloldását az Ügyfél. Az illetéktelen hozzáférés elkerülése végett, amennyiben az Ügyfél 10 percig nem használja a rendszert, automatikusan kiléptetésre kerül az Ügyfél, a bejelentkező képernyőt megjelenítve. A belépéshez újra meg kell adni az Ügyfélazonosítót és jelszót (az ezen időpontig rögzített, de a Társaságnak még el nem küldött tételek elvesznek).

1.2. Biztonságos kapcsolat

A biztonságos kapcsolat az alábbiakról ismerhető fel:

- A címsorban a Társaság Internet címe „https" kezdetű (https://netbank.oneynet.hu/netbank).

- 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 tanúsítvány legegyszerűbben a lakat szimbólumra kattintva ellenőrizhető. Ekkor egy rövid összefoglalót kap az Ügyfél a tanúsítvány tartalmáról, bővebb információkat (a tulajdonos adatai, a Web címek, melyeken keresztül a szerver elérhető, a tanúsítvány lejárati dátuma) az összefoglaló alatti gombra/linkre kattintva érhet el.

A Társaság NetBank webszerverét a THAWTE Tanúsítványkiadó, a világszinten elismert digitális igazolványt kibocsátó cégének tanúsítványával hitelesítette.

A biztonságos kapcsolat létrejötte könnyen felismerhető. A Társaság az Ügyfél adatainak védelmében titkosított SSL protokollon keresztül biztosítja az adatok áramlását. Az SSL az Ügyfél adatait továbbítás előtt titkosítja, s így azok kódolt formában jutnak el a Társasághoz, ennek következtében illetéktelen személyek számára nem értelmezhetők. Az adatok az Ügyfél számítógépe és a Társaság között végig erős titkosítású csatornában továbbítódnak.

1.3. Gyanús műveletek monitorozása

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

1.4. Az elvégzendő műveletekhez szükséges és elégséges információk megjelenítése a felületen.

Banki adatok, mint pl. a hitelkártyaszám megjelenítése csak rejtett módon történik, azaz a kezdeti és vég karaktereken kívül a közbenső karakterek száma nem azonosítható.

1.5. Az Ügyféltől elvárt intézkedések a biztonsági kockázat minimalizálása érdekében

Az Ügyfél a szolgáltatást olyan eszközről használhatja, amely a felügyelete alatt áll. A NetBank szolgáltatás igénybevétele netkávézóból vagy nyilvános, közösen használt számítógépről, mobil eszközről nem javasolt.

Az Ügyfél felelőssége gondoskodni az operációs rendszerhez, az Internet böngészőhöz és egyéb szoftvereihez kiadott biztonsági frissítések rendszeres telepítéséről. Az Ügyfél köteles vírusirtó szoftvert telepíteni, azt rendszeresen frissíteni, és annak folyamatos működéséről gondoskodni.

Az Ügyfél köteles tűzfalat alkalmazni, hogy megakadályozza a nem kívánatos hozzáférést számítógépéhez.
Vezeték nélküli hálózat használata esetén az Ügyfél köteles a biztonságos beállításokról gondoskodni.

Az Ügyfél köteles spyware és malware (kémprogramok, kártékony szoftverek elleni) szűrő programok használatára.

Bármilyen program telepítése csak megbízható forrásból történhet.
A Windows XP támogatás megszűnése miatt az operációs rendszer cseréje indokolt, mert ennek hiányában a számítógép sebezhetőbbé válhat a biztonsági fenyegetésekkel és a vírusokkal szemben.

Mobil eszköz esetén a háttértárak titkosítása, képernyőzár és jelszó használata szükséges.

Az elektronikus banki kapcsolat idejére minden más Internet kapcsolat megszüntetése indokolt. A weboldal címét az Ügyfél kézzel írhatja a címsorba, email-en kapott link nem használható.

Ha kapcsolódáskor a böngésző tanúsítvány-hibát jelez, akkor az Ügyfél nem jelentkezhet be a NetBankba, a Társaságot haladéktalanul értesíteni köteles.

Kijelentkezés esetén törölni kell a böngésző ideiglenes háttértárját és be kell zárni a böngészőt.
Az Ügyfél köteles meggyőződni arról minden egyes alkalommal, hogy számítógépe a Társaság szerverével kommunikál megfelelő biztonsági körülmények között.

Ehhez az alábbiakat kell ellenőrizni:
- Web cím: https://netbank.oneynet.hu/netbank
- A böngésző státusz sorában található ikonok valamelyikére (biztonsági kulcs/lezárt lakat) kattintva a THAWTE által kibocsátott digitális igazolvány jelenik meg.

A THAWTE tanúsítványa igazolja, hogy az adatok a Társaság web szerveréről érkeznek. Ennek hiányában az Ügyfél értesíteni köteles a Társaságot a www.oney.hu/kapcsolat oldalon található elérhetőségeken.

A Társaság e-mailen soha nem kéri az Ügyfél személyes adatait, azonosító kódjait és nem kéri fel ezek módosítására. Ha ilyen üzenetet kap, az Ügyfél köteles erről a Társaságot a fenti elérhetőségek valamelyikén értesíteni.

2. NETBANK TECHNIKAI FELTÉTELEK

A NetBank szolgáltatás igénybevétele nem igényel semmilyen különleges böngésző beállítást, a szolgáltatás a böngészők alapbeállításaival használható.

2.1. Operációs rendszer feltételek

A NetBank felhasználói felülete desktop és mobil (telefon, tablet) eszközre is megfelelően optimalizált. A NetBank rendszer független a számítógép vagy mobil eszköz operációs rendszerétől.

2.2. Támogatott Internet böngészők asztali számítógép és laptop esetében

A hibátlan működést az alábbi böngészők biztosítják:
- Internet Explorer 10+
- Mozilla Firefox 22+
- Google Chrome 27+
- Opera 12+
- Safari 4+

A biztonságos használat érdekében ajánlott a lehető legfrissebb verziójú böngésző használata.

2.3. Támogatott mobil eszközök és operációs rendszerek

- Android operációs rendszerrel rendelkező telefonok és táblagépek (2.3 vagy ennél magasabb verzió)
- iPhone, iPad (iOS 3.0 vagy ennél magasabb verzió)
- Windows Mobile telefonok (6.5 vagy ennél magasabb verzió)

Az olyan mobil böngészők használata biztonsági okokból nem támogatott, melyek kommunikációja átmegy egy harmadik fél által üzemeltetett proxy szerveren (pl. Opera Mini).
Egyebekben az Ügyfél és a Társaság között létrejött szerződés, az adott általános szerződési feltételek, az Általános Üzletszabályzat és az üzletági üzletszabályzatok rendelkezései az irányadók.