Ügyfél által használt kommunikációs eszköz és használatának biztonsági követelményei

A távértékesítés folyamata során az Ügyfél kizárólag a saját (a szolgáltatónál is hozzá rendelt) telefonszámával kezdeményezhet elektronikus szerződéskötést.

Az Ügyfélazonosításhoz, az elektronikus jognyilatkozat megtételéhez (szerződés aláírásához), valamint a Bank mobilalkalmazási szolgáltatása (mBanking) igénybevételéhez az ügyfél által használt kommunikációs eszközök (különösen de nem kizárólagosan: okostelefon, számítógép (asztali/laptop), tablet/táblagép beleértve szoftver, hardver elemeket, és e-mail postafiókot (továbbiakban: Eszköz) biztonságos használatához, illetve az ügyfél személyes adatainak, banktitkainak megőrzéséhez elengedhetetlen ezeknek az eszközöknek a megfelelő karbantartása, megfelelő biztonságot különösen, de nem kizárólagosan az alábbi biztonsági követelmények folyamatos teljesítésével, amelyekért az Ügyfél kizárólagosan felel:

Általánosan az Eszköz:

- csak és kizárólag az ügyfél eszközön végzett sikeres azonosítását követően hozzáférhető, az azonosításhoz használt adatok rendszeresen cserélve vannak, nem könnyen kitalálhatóak (PIN kód -Okostelefon / Tablet- tekintetében), jelszó)
- elemei (operációs rendszer, firmware, böngésző, egyéb alkalmazások) rendszeresen frissítettek a gyártói ajánlásoknak megfelelően valamint szakszerűen beállítottak
- hálózati kapcsolatai biztonságosan beállítottak (megfelelő vezeték nélküli hálózati védelmi eljárások (pl titkosítás és azonosítás) használata, hálózati eszközök hozzáférésének korlátozás)
- kijelzője a folyamat során kizárólag az ügyfél számára látható
- A felhasználónév és jelszó mentése a böngészőben nem javasolt
- Javasolt olyan jelszó használata ami legalább 8 karakter hosszú, tartalmaz kis-. illetve nagybetűt, számot, speciális karaktert, nem tartalmaz értelmes szótári szót, javasolt, hogy dedikált jelszó kerüljön felhasználásra, az ügyfél kerülje más szolgáltatásnál használt jelszó újrafelhasználást, javasolt általánosságban biztonságos jelszótároló alkalmazása

Továbbá:

Okostelefon / Tablet eszköz tekintetében:

- az eszközön az operációs rendszer védelmi mechanizmusai, jogosultsági rendszere, egyéb alrendszerei nem kerültek módosításra (root - Android, jailbreak – iOS)
- Zárolt kijelzőn az SMS előnézet nem engedélyezett
- A PIN kód nem tartalmaz meg könnyen kitalálható adatot, pl. születési dátum, ismétlődő karaktereket pl. 111111

Asztali számítógép / laptop eszköz tekintetében:

- rendelkezik jogtiszta, naprakész kártékony kód védelemmel (vírusvédelem, anti-malware) – a vírusellenőrzés rendszeresen fut valamint hatóköre kiterjed a letöltött állományokra, az eszközhöz csatlakoztatott adathordozókra, korszerű védelmi megoldásokkal (pl tűzfal)

Továbbá az ügyfél biztosítja, hogy a távértékesítés folyamat során az általa az Ügyfélazonosításhoz illetőleg az elektronikus jognyilatkozat megtételéhez használt kommunikációs eszközökhöz kizárólagosan az ügyfél fér hozzá, harmadik fél hozzáférése kizárt.

Bank felelősségét kizáró rendelkezések

Az Eszköz nem megfelelő szintű biztonsági beállításaiból, nem megfelelő biztonsági szintjéből keletkező káresemények vonatkozásában a felelősséget a Bank teljes körűen kizárja.

A Bank nem felel azokért a károkért, amelyek az ügyfél berendezéseinek műszaki hibájából vagy abból adódnak, hogy az ügyfélnek ezen okból nem áll módjában megfelelő kapcsolatot létesíteni a Bankkal.

A Bank a bizonyítottan az adott azonosítóval (mobiltelefonszám) az online igénylési felületre bejelentkezett ügyfél által kezdeményezett és az ügyfél eszközére megküldött egyszer használatos jelszóval hitelesített igénylést a Bank úgy tekinti, hogy azt az igénylési adatlapon megadott személy kezdeményezte, és nem vizsgálja az azonosító és jelszó (mobiltelefon)használójának a használatra vonatkozó jogosultságát, illetve a használat körülményeit. A Bankot semmiféle felelősség nem terheli az azonosítóval kezdeményezett és az ahhoz rendelt jelszóval hitelesített, de jogosulatlan személytől származó igénylésből az ügyfelet vagy mást ért károkért.

A telefon illetve az Internet igénybevétele során a hálózat működésével összefüggésben a megfelelő gondosság mellett is előállhatnak olyan esetek, amikor az egymásnak küldött üzenetek illetéktelen harmadik személy(ek) számára megismerhetővé válnak. Erre tekintettel az Ügyfél tudomásul veszi, hogy a szolgáltatás igénybevételével és az annak útján történő rendelkezéssel kockázatokat vállal magára, és ennek a kockázatnak a mérlegelése után döntött a szolgáltatás igénybevételéről. Ennek kapcsán a Bankot nem terheli felelősség azért, ha az elektronikus kommunikáció során továbbított banktitoknak minősülő információ a Bank érdekkörén kívül eső ok(ok)ból jogosulatlan harmadik személy(ek) tudomására jut.

Budapest, 2020.10.15