Tájékoztató az elektronikus csatornán megadott meghatalmazotti hozzáférésekhez kapcsolódó visszaélések megelőzéséről

Tisztelt Ügyfelünk!

A pénzügyek rendezése mindinkább digitális útra terelődik, a visszaéléseknek pedig számos új formája jelent meg a digitális térben, így például a személyes hitelesítési és érzékeny fizetési adatok megszerzésén, majd ezek alapján fizetési megbízások jogosulatlan kezdeményezésén alapuló visszaélések, a megtévesztésen és pszichológiai manipuláción alapuló visszaélések – melyek során a fizető felet igyekeznek rábírni a fizetési megbízás kezdeményezésére, illetve a visszaélést elkövetők által kezdeményezett fizetési megbízások jóváhagyására –, valamint a fizető fél birtokában lévő készpénz-helyettesítő fizetési eszközhöz, például fizetési kártyához, mobilbankhoz vagy internetbankhoz történő közvetlen hozzáférésen alapuló visszaélések.

Az említett visszaélések járulékos kockázata, amikor az érintett fizető fél az Ön fizetési számlája feletti meghatalmazott felhasználó, hiszen így az ő elektronikus hozzáférésén, online felületein (pl. internetbank) keresztül a csalók az Ön fizetési számláihoz is hozzáférhetnek.

A bűnözők nem a pénzügyi intézményeket, illetve a biztonságos infrastruktúrát támadják, hanem elsősorban a (gyors változásokat olykor át nem látó) fogyasztók megtévesztése, érzelmi manipulálása révén érnek célt.

Javasoljuk ezért, hogy **amennyiben Ön meghatalmazást ad fizetési számlája feletti rendelkezésre, minden esetben hívja fel meghatalmazottjai figyelmét**, hogy**:**

- **a támadók elsődleges célja, hogy a jelszavaikat megszerezve hozzáférjenek a netbanki fiókhoz.**
- **semmilyen körülmények között ne adjanak meg bizalmas információkat, adatokat vagy azonosító és hitelesítő információkat e-mailben, SMS-ben vagy más úton érkező felkérésre!**
- **a jelszavaikat gondosan válasszák meg és kezeljék azokat körültekintően!** A számítógépes rendszerekbe a felhasználónevük és jelszavuk segítségével tudnak belépni. Amikor az adott rendszerhez (pl.: levelezésükhöz vagy privát banki felületükre stb.) hozzáférést nyernek, a naplózórendszer a felhasználónévhez rendelve rögzíti a tevékenységüket. Ha valaki megszerzi a felhasználónevüket és a hozzá tartozó jelszót, minden olyan adathoz hozzáférhet, amelyhez a felhasználók jogosultak. A rendszer szemszögéből ez olyan, mintha a felhasználó hajtaná végre az adott műveleteket, így amit a támadó tesz, a nevükben kerül rögzítésre a rendszer naplóállományaiban.
  A támadók kétféleképpen tudják feltörni a jelszavakat:
  - brute force (nyers erő) támadással: a lehetséges karakterek kombinációiból próbálják a jelszót összeállítani, ami rövid, egyszerű jelszavak esetén mindig célravezető;
  - „szótáralapú” támadással: értelmes szavakat, gyakran használt jelszavakat (pl.: név + születési dátum) próbálnak ki.
- **válasszanak erős jelszót az alábbiak szerint:**
  - Ne legyen rá jellemző, mert kevés információ birtokában is könnyen kitalálható (pl.: családtag neve + születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető);
  - Nem szerencsés, ha a jelszó csak egy szóból áll (például az „almafa” szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában);
  - Jó, ha a jelszó hosszú és többféle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a brute force technikával való feltörést;
  - A legjobb, ha néhány szóból álló jelmondatot választ, amelyben van kisbetű, nagybetű és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, brute force technikával feltörni pedig szinte lehetetlen.
- **ellenőrizzék rendszeresen bankszámlájukat, és a gyanús tevékenységekről tegyenek bejelentést!**

- **ügyeljenek a biztonságos telefonhasználatra!** Fel kell készülniük a csalárd banki hívásokra, hiszen a csalók bárki telefonját megcsörgethetik!
  Néhány tipp, hogyan kezeljék a csalárd hívásokat:
  - Ha valaki banki alkalmazottként vagy pénzügyi intézmény képviselőjeként mutatkozik be, kérjenek tőle további azonosító információkat, például a nevét, a bank nevét, a pozícióját, és hogy milyen ügyről van szó. Jegyezzék fel ezeket az információkat, majd ellenőrizzék a banknál vagy a pénzügyi intézménynél, hogy valóban hivatalos képviselőről van-e szó.
  - Tudniuk kell, hogy valós banki ügyintézői hívás esetén soha nem kérdeznek olyan bizalmas információkat, mint az online fiókunk hitelesítő adatai (felhasználónév, jelszó) vagy a kártyaadatok, biztonsági kódok, esetleg más személyes azonosító információk. Ha ilyen jellegű felszólítást kapnak, szakítsák meg a hívást, és hívják a Bankot az ismert/ellenőrzött telefonszámon, hogy mielőbb jelentsék az esetet.
  - Éljenek a keresztazonosítás lehetőségével! Valós banki ügyintézői hívás esetén a hívó fél ismeri a személyes adataikat. A keresztazonosítás során a feltett kérdésekre (például anyja születési neve) a válaszok egyik felét az intézmény ügyintézője adhatja meg, a válaszok másik felét pedig az ügyfélként a felhasználók magunk!
  - Soha ne adják meg online banki jelszavukat vagy az egyszer használható, második hitelesítési kódot! A bankok sosem kérik el ezeket az információkat!
  - Soha ne telepítsenek mások kérésére programot számítógépükre vagy telefonjukra! A csalók sokszor vírusvédelmi megoldásnak beállítva, álcázva próbálják rávenni áldozatukat arra, hogy visszaéléshez használható programot telepítsenek.
  - Ha beszélgetés közben a hívó fél felajánlja, hogy pénzük védelmében „átkapcsol egy másik bankhoz”, vagy a „bank biztonsági szolgálatához” továbbítaná a hívást „további biztonsági lépések” miatt, azonnal szakítsák meg a hívást! Ilyet valós banki ügyintéző sosem tesz.
  - Ha úgy érzik, hogy a hívás valóban fontos és hivatalos, és további intézkedéseket szeretnének tenni, ne használják a hívó által megadott elérhetőségeket. Inkább keressék meg a Bank hivatalos weboldalát, és az ott található elérhetőségeket használják, hogy további információkat szerezzenek.

Ha az Ön, vagy meghatalmazottja adatai csalók kezébe kerültek, javasoljuk, a lehető leghamarabb jelezze az esetet a Merkantil Banknak

- a **+36 1 268 6868** telefonszámon, vagy
- a 1138 Budapest, Föveny utca 4-6. szám alatti bankfiókunkban személyesen, vagy
- az informacio@merkantil.hu e-mail címen.

Amennyiben az Ön, vagy meghatalmazottja e-mail postaládájában Merkantil Direkt internetbank belépésre felszólító gyanús e-mail érkezik vagy adathalász SMS-t kap, **kérjük vegye fel a kapcsolatot kollégáinkkal** az informacio@merkantil.hu e-mail címen keresztül, hogy kivizsgálhassuk. A vizsgálat érdekében kérjük, hogy csatolmányként küldje el nekünk a gyanús levelet vagy SMS üzenetet is.
Ha a telefonhívás során felmerül Önben vagy meghatalmazottjában a gyanú, hogy illetéktelen személy akarja megszerezni a banki adatait és azonosítóit, **kérjük, azonnal szakítsa meg a beszélgetést**, továbbá **hívja fel** a Merkantil Bank Ügyfélszolgálatát **(+36 1 268 6868)** és jelezze Bankunknak a gyanúját.
Amennyiben az Ön vagy meghatalmazottja Merkantil Direkt internetbank belépési adatai illetéktelenek tudomására jutottak, lehetőségük van jelszavukat a hét bármely napján lecserélni a Merkantil Direkt felületén a bejelentkezés után a „Beállítások” menüpontban.

További információt a https://kiberpajzs.hu/ és a https://www.merkantil.hu/hu/Adathalaszat oldalakon talál.