

1. HISZÉKENYSÉG, KONTRA VÉDELMI FUNKCIÓK

Az elkövetők jóhiszeműségre és a tájékozatlanságra alapozva - ugyanakkor a körülmények által nem indokoltan - pszichológiai nyomás alá helyezik az ügyfelet egy-egy csalárd telefonhívás alkalmával.

az ügyfelet ráveszik, hogy a mobiltelefonra töltsön le távoli hozzáférést biztosító alkalmazást, melynek segítségével a csalók megismerhetik az SMS-ben kapott biztonsági kódot, és a banki alkalmazások felett át tudják venni az irányítást.

A PBT tapasztalatai szerint sok esetben még erre sem volt szükség, mert a hiszékeny ügyfelek a csalók kérésére az SMS-ben szereplő kódokat maguk adták ki, vagy a mobilalkalmazásban elvégzett hitelesítésekkel a tranzakciókat maguk hagyták jóvá.

Az ügyfelek az elkövetők által kért tranzakciót megelőzően látják annak minden adatát: a kedvezményezett nevét, a tranzakció összegét és devizanemét, mégsem fognak gyanút.

A csalók a bankkártya valamennyi adatának kiadása mellett a kód elárulására is ráveszik az ügyfeleket, ami állításuk szerint azért volt szükséges, mert a tranzakció ügyfél általi jóváhagyásával a tranzakciót zárolták, blokkolták vagy az adott összeget „biztonságos rendőrségi számlára” helyezték.

A kontrollszolgáltatással rendelkező ügyfelek a művelet után rögtön észlelték a számlaegyenlegük csökkenését.

Az ő kételyeiket azzal hátrították el, hogy a pénzt átmenetileg védelem alá helyezték, és majd a bank később visszavezeti azt a „biztonsági számláról”.

A csalók fő érve tehát az volt, hogy az ügyfelek pénzét védik, de valójában éppen elvették azt!

Mit lehet tenni a telefonos csalók ellen?

A bankok saját internetes felületükön, e-mailen, netbankon vagy a banki mobil alkalmazáson keresztül küldött push üzenetben folyamatosan tájékoztatják ügyfeleiket az aktuális adathalász kísérletekről, banki csalásokra használt módszerekről.

Ne sajnáljuk az időt a banktól kapott üzenetek átolvasására!

Ellenőrizzük, hogy az SMS-en vagy mobilalkalmazáson keresztül kapott üzenet tartalma, az abban szereplő tranzakció valóban megfelel a szándékunknak.

Legyünk körültekintők! Minden szempontból megéri.

Szólaljon meg a belső vészcsengője! Szakítsa meg a hívást, és tárcsázza a bankját, ha hasonló gyanús telefonhívással, sürgető hangnemben próbálják rávenni személyes ill. érzékeny banki adatainak, kódjainak megadására, vagy ismeretlen alkalmazás letöltésére.

2. KIS KÉRÉSEK, NAGY KÁROK

A csalók hihetetlen rafináltak és magabiztosak tudnak lenni.

Az MNB-nél működő Pénzügyi Békéltető Testület (PBT) elé került egyik ügyben a csaló elhitette az ügyféllel, hogy ő egy banki ügyintéző és éppen forró nyomon van!

Állítása szerint az igazi csaló egy másik banki alkalmazott, aki éppen „akcióban van” az ügyfél számláján, és ő küldi majd a bankkártya felfüggesztéséről az SMS-t és fel is hívja majd az ügyfelet. A csaló felhívta az ügyfél figyelmét, hogy ne dőljön majd be neki. A bank visszaélésszűrő rendszere valóban észlelte az elkövetők által angol fontban kezdeményezett kisösszegű műveletet, blokkolta a bankkártyát és telefonon felhívta az ügyfelet.

Az ügyfél azonban – a csalók javaslatára – a kis összegű tranzakciót saját maga által kezdeményezettnek ismerte el a bank igazi munkatársa felé. A történet vége milliós összegű kár lett, hiszen a bűnözők így már újabb, nagy összegű utalást is indíthattak.

A csalók által ajánlott megoldások visszatérő eleme a több megtévesztő megnevezéssel jelölt (pl. „vírusölő” vagy „hackertámadást elleni”) program telepítése az ügyfél online bankolásra használt mobiltelefonjára vagy számítógépére.

E programokat (mint az AnyDesk vagy a TeamViewer) annak ellenére telepítik a megtévesztett ügyfelek, hogy ténylegesen nem ismerik azokat, nem is ellenőrzik őket a letöltést megelőzően.

A csalók e programok segítségével a valóságban távoli és korlátlan hozzáférést kapnak az ügyfél online bankoláshoz használt eszközeihez.

A telepítését követően „csak” be kell léptetni az ügyfelet online banki felületére.

Annak érdekében, hogy az ügyfél ne lássa, milyen műveleteket végeznek ismeretlenek a mobiltelefonján, a telefon lefordítására és a rajta lévő kamerák eltakarására kérik meg.

Szintén visszatérő elem volt, hogy a csalók az általuk jelzett, valójában nem létező terhelések megakadályozása érdekében az ügyfeleket a korábbi alacsony összegre beállított bankkártyalimit lehető legmagasabb összegre történő megemelésére vették rá.

Ez a lépés azonban nem megakadályozta, hanem lehetővé tette, hogy minél nagyobb összegű visszaélést kövessenek el velük szemben.

Fontos, hogy legyünk tisztába azzal, hogy a bankok sohasem kérik programok, alkalmazások telepítését a pénzünk védelmében!

Nem kérik megadni a bankkártya valamennyi adatát, illetve hitelesítő kódokat, felhasználónevet, jelszavakat!!

Szólaljon meg a belső vészcsengője! Szakítsa meg a hívást, és tárcsázza a bankját, ha hasonló gyanús telefonhívással, sürgető hangnemben próbálják rávenni személyes ill. érzékeny banki adatainak megadására.

3 . LEGYEN GYANÚS A HÍVÁS, HA A SZÁMLAVEZETŐ BANKUNK MEGNEVEZÉSÉT KÉRIK

Telefonos adathalászat:

Trükkös adattolvajok akár banki telefonszámokat klónozva kezdeményeznek telefonos beszélgetést ügyfelekkel.

Ilyenkor emlékezzünk arra, hogyan azonosított minket bankunk a korábbi telefonhívások alkalmával.

Általában néhány személyes adatot kérnek el, illetve ellenőrző kérdéseket tesznek fel (pl. van-e megtakarítása a banknál).

A visszaélések során azonban számos esetben az ügyfelek beazonosítása elmarad, sok ügyfél ilyenkor mégis folytatja a beszélgetést a csalókkal.

Más esetekben történhet valamiféle azonosítás, amelyet követően az ügyfelek megnyugszanak, úgy érezhetik, valós banki alkalmazottal beszélnek, mivel olyan adatokat tudtak róluk, amelyeket csak a bank tudhatott.

Ilyen lehet a bankkártyaszámokkal történő azonosítás.

Valójában a csalók a kártya azon adatait ismerhetik, amelyhez az ügyfél távoli hozzáféréseken keresztül elért internet- vagy mobilbankjában juthattak hozzá (a rendszerekben a bankkártyaszám néhány adata látható), a hiányzó számokat pedig az ügyfelekkel diktáltatják be azonosításként.

A valóságban a bankok sohasem kérik el a bankkártya valamennyi adatát, illetve hitelesítő kódokat, felhasználónevet, jelszavakat - sem azonosításhoz, sem további műveletekhez.

Arra sem kérik az ügyfeleket, hogy a visszaélés megakadályozása érdekében „a sípszó elhangzása után” bediktálják nevüket, illetve bankkártyájuk valamennyi adatát.

Azt követően, hogy a csalók pszichológiai manipulációval elnyerték az ügyfél bizalmát, elindítják azokat a műveleteket, amelyeket – hivatkozásuk szerint – az ügyfél pénzének védelmében, de ténylegesen annak eltulajdonítására végeznek.

Szóljon meg a belső vészcsengője!

Szakítsa meg a hívást, és tárcsázza a bankját, ha hasonló gyanús telefonhívással, sürgető hangnemben próbálják rávenni személyes ill. érzékeny banki adatainak megadására.

4. ÚJ TRÜKKÖKKEL TÁMADNAK A BANKI CSALÓK

Egy álmos reggelen, munkába menet megcsörren a telefonunk. A kijelző szerint egy banki hívás. Egy határozott fellépésű, fiatal férfi vonal másik végén arról tájékoztat, hogy a bankszámlánkról gyanús tranzakciót hajtottak végre, és ha azt nem mi kezdeményeztük, segítenek a tranzakció megakadályozásában. Ha kiderül, hogy nem a számlavezető bankunk nevében telefonált, a hívó készségesen felajánlja, hogy „átkapcsol saját bankunkhoz” vagy jelzi a problémát felénk – persze, csak akkor, ha elmondjuk neki, pontosan melyik banknál vezetjük a számlánkat. A napunk további része azon múlik, milyen válaszokat adunk az ismeretlen személy kérdéseire, mit és hogyan teszünk. Legyünk tudatosak! Van arra mód, hogy ne legyünk a „vishing” (telefonos adathalászat) áldozatai.

Az első és a legfontosabb lépés, hogy meggyőződjünk róla, lehet-e valós egy ilyen tartalmú hívás.

A pénzünk elvesztése miatti pánik hajlamos kiiktatni a józan ítélőképességet.

Legjobb, amit tehetünk ekkor, ha hagyunk magunknak egy kis időt, hogy megértsük: miért is hívtak bennünket? Ha ezt megtesszük, akkor több esélyünk van arra, hogy észre vegyünk a gyanús jeleket.

Legyen óvatos! Szólaljon meg a belső vészcsengője!

Az ügyfelek többsége rendelkezik különböző kényelmi banki szolgáltatással, melyekkel a bankkártya- vagy számlaműveletekről (terhelésekről, jóváírásokról) SMS-ben vagy mobilalkalmazáson keresztül üzeneteket kapnak.

Ha nem érkezett ilyen üzenet, ennek ellenére a hívó fél konkrét visszaélésről tájékoztat minket, legyünk óvatosak!

Ellenőrizzük a hívó fél telefonszámát.

Sajnos, van arra mód, hogy a csalók egy adott telefonszámot klónozzanak, de a tapasztalatok alapján gyakran csak hasonlít a hívó fél száma a bank ügyfélszolgálatának telefonszámához (például a körzetszám után nem 7, hanem 8 számjegy található).

Figyeljünk arra is, hogy a bankszámlánkkal kapcsolatos jogtalan fizetési műveletekről csak a számlavezető bankunktól kaphatunk telefonhívást.

A bankok nem működtetnek közös ügyfélszolgálatot, s azok nem kapcsolnak át egymáshoz hívásokat.

Tekintsünk gyanúsnak minden olyan kérést, amely a számlavezető bankunk megnevezésére vagy érzékeny banki adatainkra irányul.

Ha bizonytalanok vagyunk, szakítsuk meg a hívást és hívjuk fel a bankunk ügyfélszolgálatát!

Olykor sürgető és adott esetben súlyos szankciókat kilátásba helyező, fenyegető hangnem jellemzi az ilyen hívásokat, de ne dőljünk be ezeknek! legyünk tisztában azzal, hogy a bankok alkalmazottai nem vezetnek a rendőrséggel együtt „forró nyomon”, ügyfelek azonnali közreműködését igénylő nyomozati cselekményeket.

Fontos, hogy ismerjük fel az árulkodó jeleket! A banki ügyintézők sosem sürgetnek, azonosításkor nem kérik el a bankkártya valamennyi adatát, illetve hitelesítő kódokat, felhasználónevet, jelszavakat!

Szólaljon meg a belső vészcsengője! Szakítsa meg a hívást, és tárcsázza a bankját, ha hasonló gyanús telefonhívással, sürgető hangnemben próbálják rávenni személyes ill. érzékeny banki adatainak megadására.

5. KIBERPAJZS

- MNB,
- Magyar Bankszövetség,
- NMHH,
- NBSZ-NKI,
- ORFK

közös oktatási és kommunikációs együttműködése a lakossági ügyfelek pénzügyi tudatosságának erősítése, a kiberkockázatok minél hatékonyabb kezelése érdekében, elsősorban a fogyasztók érzelmi manipulálásával, illetve megtévesztésével támadó, digitális pénzügyi bűnözők ellen.

Közös kibervédelmi edukációs és kommunikációs kampányról szóló együttműködési megállapodást írt alá:

A KiberPajzs projekt keretében az intézmények és a piaci szereplők átfogó oktatási programot indítanak az ügyfelek digitális pénzügyi tudatosságának fejlesztése érdekében.

A kiberbiztonsági kockázatok és az ellenük való védekezési lehetőségek bemutatására széleskörű, összehangolt kommunikációs kampány is kezdetét veszi.

A KiberPajzs projekt céljai között szerepel a kiberbiztonsági hatósági és piaci folyamatok elemzése, továbbfejlesztése.

Valamint hazai és nemzetközi szakmai tudásmegosztás és jógyakorlatok gyűjtése a minél erősebb és hatékonyabb pénzügyi kibervédelem megvalósítására.

A digitalizáció révén egyre hangsúlyosabbá válik az elektronikus pénzforgalom, ezzel párhuzamosan pedig – miközben a hazai pénzügyi rendszer európai összevetésben is rendkívül biztonságosnak számít – a rajta keresztül megfigyelhető sikeres visszaélések száma és aránya is növekszik.

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

Ezért vált mára alapvető fontosságúvá az „elsődleges védelmi vonalnak” számító ügyfelek pénzügyi tudatosságának erősítése, és felkészítésük a kiberkockázatok kezelésére.

A projekt kiemelten figyel a fiatalokra, a fokozottan kiszolgáltatott társadalmi csoportokra (így az idősekre), de a fogyasztók mellett megelőző jellegű üzeneteket fogalmaz meg a kis- és középvállalati, illetve az egyéb céges ügyfelek felé is.

A KiberPajzs program keretében az intézmények egységes arculatú, egyszerű üzenetekkel mutatják majd be a főbb csalási formákat:

- így az adathalászat különböző változatait,
- a hamis banki hívásokat vagy sms-eket,
- a meghamisított banki weboldalakat,
- a hamis tranzakciók jóváhagyási formáit,
- a csaló befektetési vagy egyéb online ajánlatokat,
- illetve a közösségi média segítségével történő személyes adat-lopásokat.