DR. TARPAI LAJOS TAMÁS*: Új trükkökkel támadnak a banki csalók

Egy álmos reggelen, munkába menet érkezik egy hívás az általunk ismerni vélt telefonszámról. Határozott fellépésű, fiatal férfi vonal másik végén arról tájékoztat egy bank nevében, 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 feléjük – 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. 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 észrevegyük a gyanús jeleket.

Legyen óvatos!

Az ügyfelek többsége rendelkezik különböző kényelmi banki szolgáltatásokkal, 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 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 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 sajátja az ilyen hívásoknak, de ne dőljünk be ezeknek! A bankok alkalmazottai nem vezetnek a rendőrséggel együtt „forró nyomon", ügyfelek azonnali közreműködését igénylő nyomozati cselekményeket.

Tekintsünk gyanúsnak minden olyan kérést, amely a számlavezető bankunk megnevezésére irányul

Trükkös adattolvajok

Ha valamiért mégis tovább folytatjuk a telefonos beszélgetést, emlékezzünk arra, hogy azonosított minket bankunk a korábbi telefonhívások során. 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 történt valamiféle azonosítás, amelyet követően az ügyfelek megnyugodtak, úgy érezték, 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 ismerték, amelyhez az ügyfél távoli hozzáférésen keresztül elért internet- vagy mobilbankjában juthattak hozzá (a rendszerekben a bankkártyaszám néhány adata látható), a hiányzó számokat pedig az ügyfelekkel diktáltatták 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 elnyerték az ügyfél bizalmát, elindítják azokat a műveleteket, amelyeket – hivatkozásuk szerint – az ügyfél pénzének védelmében, de ténylegesen annak eltulajdonítására végeznek.

A bankok sohasem kérik el a bankkártya valamennyi adatát, illetve hitelesítő kódokat, felhasználónevet, jelszavakat

Kis kérések, nagy károk

Az MNB-nél működő Pénzügyi Békéltető Testület (PBT) elé került egyik ügyben az elkövető elhitette az ügyféllel, hogy éppen forró nyomon van: állítása szerint az igazi csaló egy banki alkalmazott, aki éppen „akcióban van" az ügyfél számláján, és ő küldi majd a bankkártya felfüggesztéséről az SMS-t és hívja is az ügyfelet. Felhívták a figyelmét, hogy ne dőljön be neki. A bank visszaélésszűrő rendszere valóban észlelte az elkövetők által kezdeményezett, 0,72 GBP összegű műveletet, blokkolta a bankkártyát és telefonon kereste 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, nagyösszegű 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 az említett eszközökre, hogy ténylegesen nem ismerik azokat, nem is ellenőrzik őket a letöltést megelőzően.

A csalók e programok telepítésével 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, 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.

Hiszékenység, kontra védelmi funkciók

A különböző internetes biztonsági kódok, erős ügyfélhitelesítés világában felmerülhet, hogy miként valósulhattak meg e visszaélések. Nos úgy, hogy a mobiltelefonra letöltött távoli hozzáférést biztosító alkalmazás segítségével a csalók megismerhetik az SMS-ben kapott kódot, a banki alkalmazások felett az irányítást átvehetik. Sok esetben azonban erre sem volt szükség, mert az 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 látták annak minden adatát: a kedvezményezett nevét, a tranzakció összegét és devizanemét, mégsem fogtak gyanút. A csalók a bankkártya valamennyi adatának kiadása mellett a kód elárulására is rávették 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 hárították 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, s ezért kell a megtakarításokat egy biztonságos számlára utalni. Meséjük szerint minden bankban van az ügyfeleknek egy titkos alszámlájuk, amely ugyan nem az ügyfél nevére szól, mert csalók szerint arra nem szólhat. Továbbá, mivel az ilyen alszámlára maximum kétmillió forint utalása lehetséges, ezért a számlaegyenleg nagyságától függ az alszámlák száma.

A csalók által nem ismert, de az ügyfél által megnevezett számlaegyenleg ismeretében, a csalók útmutatásai szerint az ügyfelek rögzítették az egy vagy több alszámlára történő utalás adatait. Ez minden esetben az ügyfél bankján kívüli bankszámla volt, ismeretlen kedvezményezettel, a közleményben pedig „ajándékot" vagy egyéb megjegyzést kellett rögzíteni. Ezt követően az ügyfelek a PBT elé került esetekben át is utalták az összeget abban a hiszemben, hogy ezzel biztonságba helyezik a pénzüket Valójában lehet, hogy éppen elvesztették 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. Célszerű ezeket az üzeneteket átolvasni, tájékozódni. 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.

A visszaélések azért valósultak meg, mert az ügyfelek a csalók kérésére az SMS-ben szereplő kódokat is kiadták

** A szerző az MNB keretében működő Pénzügyi Békéltető Testület tagja*

„Szerkesztett formában megjelent az Origo.hu portálon 2022. április 27-én."