Dr. Tarpai Lajos Tamás*:

Sosem volt befektetésünk kifizetéséhez, nyomozáshoz csalnák ki banki adatainkat

Szomorú, de valós tény, hogy az online kibercsalók manipulációja révén sokszor olyan ügyfelek is áldozatul esnek a pénzügyi visszaéléseknek, akik életükben, munkájukban egyébként figyelmesen és körültekintően járnak el. Érdemes felkészülni a váratlan helyzetekre: például arra, hogy sosem volt befektetésünk kifizetéséhez vagy éppen hatósági nyomozáshoz kérnék el bizalmas banki azonosítóinkat.

A bankszámlákkal kapcsolatos visszaélések megakadályozása, a fogyasztók edukációja érdekében rendszeresek a visszaélésekkel, azok típusaival kapcsolatos tájékoztatások, különösen a Kiberpajzs program résztvevőitől. Ennek ellenére a visszaélések száma változatlanul nem csökken olyan mértékben, mint szeretnénk. A figyelemfelhívások kevésbé érintik azokat az emberi tényezőket, amelyek szintén befolyásolják azt, hogy valaki végül visszaélés áldozata lesz-e vagy sem. Kijelenthető, hogy bárki lehet visszaélés áldozata kortól, nemtől és képzettségtől függetlenül.

Telefonbetyárok, hamis hívások

A Pénzügyi Békéltető Testület elé kerülő, hamis befektetésekre hivatkozó visszaélések esetén az ügyfeleket telefonon keresték meg azzal, hogy több évvel ezelőtti befektetéseik immár nagyszerű hozamot értek el. Ezt most kifizetnének a részükre. A békéltetői eljárás során feltett kérdésre, hogy mi volt ez a korábbi befektetés, miből gondolták azt, hogy emiatt kereshetik őket telefonon, szinte sohasem született érdemi válasz.

„Az ügyfelek nem emlékeztek arra, mikor, hol és mennyit fektettek be és milyen termékbe. Mert nem is volt ilyen.”

Azt azonban elhitték, hogy az a befektetés, amelyekről évek óta nem tudnak semmit, kimagasló hozamot termelt. Az ügyfeleket ilyenkor olyan hatalmas összeg kifizetéséről tájékoztatják, amely sajnos elaltatja az óvatosságot.

A kecsegtető hozam reményében az érintett ügyfelek ezért követik a csalók minden utasítását. Még akkor is, ha azok rendkívül bonyolult és furcsa folyamatról rendelkeznek, mint például letölteni különböző programokat a telefonjukra, számítógépükre, hogy az ügyfelek netbankját összeköthessék e programokkal. Sajnos, az sem lesz gyanús, amikor azt az utasítást kapják: ha esetleg a bankjuktól telefonálnának az ezt követő gyanús tranzakciók miatt, akkor lehetőleg ne mondjanak semmit arról, amit éppen csinálnak.

Forró nyomon?

A hamis banki hívásos visszaélések során az ügyfeleknek több alkalommal azonnali „nyomozati cselekményekben” kellett részt venniük. Ennek során fizetési műveleteket kellett végrehajtaniuk annak érdekében, hogy az állítólagos bank és a rendőrség (valójában a bűnözők) forró nyomon követni tudja a pénz útját, majd azonnali beavatkozással el tudják fogni a csalókat akkor, amikor az ATM-ből éppen felveszik a lopott pénzt.

Az ügyfelek ilyenkor pontosan olyan fizetési műveleteket végeztek, olyan tartalmú SMS-eket kaptak, mint a korábbi saját maguk által végzett utalásaiknál. Maguk rögzítették be a kért utalást a netbanki felületen, a jóváhagyó kódot tartalmazó SMS ugyanúgy tartalmazta a forint átutalás tényét, a célszámla számát, a kedvezményezett nevét. A kód megadását, beírását követően látták a számlaegyenlegük csökkenését is, ahogy a korábbi átutalásaiknál. A korábbi tapasztalataik ellenére elhitték, hogy nekik kell ezeket a fizetési műveletek elvégezni és nekik kell több napon keresztül együttműködni az állítólagos nyomozókkal, valójában a kiberbűnözőkkel.

Az események során ugyanis volt egy-két momentum, amely miatt valósnak hatott a történet (pl. a hívó fél tudta a nevét és a számlaszámát). Emellett hiába volt számos gyanúra okot adó jel, sőt, hiába volt ismert ez a konkrét visszaéléstípus, az ügyfelek mégis attól tartottak, hogy ha nem működnek együtt, elveszítik a pénzüket.

Mindenki gyanús

Az egyik hamis banki hívással elkövetett visszaélés során, miután a csalók a távoli hozzáférést biztosító AnyDesk program telepítését sehogy sem tudták megoldani sem az ügyfél számítógépén, sem annak telefonján, a csalók egy másik megoldáshoz folyamodtak. Rábeszélték az ügyfelet, hogy menjen el egy közeli bankfiókba és ott adjon átutalásra megbízást, amelynek a kedvezményezettje egyébként ügyfél számára ismeretlen magánszemély volt.

„A csalók rávették arra is, hogy az utalás okáról a bankban ne beszéljen, mert lehet, hogy a bankfióki ügyintézők is érintettek a visszaélésben…”

Az utalást követően a kedvezményezett számlához való hozzáférést a gyanús körülmények miatt blokkolták. Ezt követően a számlavezető bankja felhívta az ügyfelét, tisztázni, hogy valóban szándékában állt a kedvezményezetti számlára történő utalás. A körülményeket tisztázó telefonbeszélgetést követően ismerte el az ügyfél, hogy valójában nem is akart utalni a számára ismeretlen személynek. Elmondta, hogy bár voltak kételyei, de félt attól, ha nem működik együtt, elveszti a pénzét.

Sok adatot kérnek az online csalók

A korábbi figyelemfelhívások ellenére 2025-ben is változatlanul sikeres az online termékértékesítéses visszaélés, ahol a csalók a vásárláshoz a bankéhoz megszólalásig hasonló álhonlapot küldenek a banki azonosítók megadására. Ennek oka lehet, hogy bár hiába voltak gyanúsak a körülmények (pl. miért kapott ilyen sok SMS-t az adott ügyfél, miért kellett ennyit kódot megadnia, limitet módosítania) a kedvező kondíciókkal hirdetett termék gyors megvételének lehetősége győzedelmeskedett az óvatosságon.

Előfordult olyan eset, amikor az ügyfél az online piactértől arról kapott értesítést, hogy az a bankfiók, ahonnan ő üzenetet kapott, adathalász tevékenységet folytat. Az ügyfél, habár bizonyos adatokat már megadott, nem értesítette a bankját a szükséges biztonsági intézkedések végrehajtása érdekében.

Egy másik esetben az ügyfélnek először gyanús volt, hogy ilyen sok adatot kérnek tőle. Ezért elővigyázatosságból a kevésbé használt és kis összeget tartalmazó bankszámlájához tartozó bankkártyaadatait adta meg a bűnözők által küldött hamis weboldalon. Nem sokkal később már nem volt

ennyire óvatos, ugyanezen a csaló oldalon a jelentősebb összeget tartalmazó számlájához köthető mobilalkalmazás regisztrációs kódját adta ki. Tette ezt annak ellenére, hogy a saját telefonján már rendelkezett ilyennel. A csalók az újonnan regisztrált mobilalkalmazással így már jelentősebb összeget tudtak eltulajdonítani…

Ami furcsa, nem véletlenül az

Sok megtévesztett ügyfél utólag arra hivatkozik, hogy az adathalászatkor nehéz napon volt túl, fáradt volt, teendői miatt nem tudott odafigyelni, vagy éppen gyorsan túl akart lenni a folyamaton. A helyzet azonban az, hogy a banki műveletek során mindig nagyon körültekintően kell eljárni.

„A banki tranzakciók olyanok, mint a gépjárművezetés: ugyanannyi figyelmet és óvatosságot igényelnek.”

A fáradtság, a kellő körültekintés hiánya, a megszokás a banki műveleteknél is problémát okozhat. Mivel a banki adathalász-kísérletek állandóvá váltak, az ügyfelek részéről is szükséges a folyamatos éberség, óvatosság, s a kibervédelmi tanácsok megfogadása.

Szükségünk van a józan ítélőképességünkre is, mivel a megtévesztési mintázatok állandóan változnak. Éppen ezért, ha valami új, eddig nem ismert fizetési módszerrel, kéréssel találkozunk, higgadtan gondoljuk végig: valóban szükséges ezt így, ebben a formában végigcsinálnunk? A hívó fél, az üzenet, a weboldal által kért adatok kapcsán pedig józanul – akár többször is - gondoljuk végig, hogy kérés teljesítése esetén vajon bárki más hozzáférhet-e a számlánkhoz? Lehet és kell is kételkedni. Az online világban a gyanakvás ugyanis nem hiba, hanem kiváló megelőző stratégia.

** A szerző az MNB-n belül működő Pénzügyi Békéltető Testület tagja*

„Szerkesztett formában megjelent 2025. október 17-én az Economx.hu oldalon.”