Tornai Annamária Natália*:

Banki kibercsalások útvesztője, avagy hogyan ne sétáljunk csapdába? – 2. rész

A klasszikus banki adathalász akciók mellett a bűnözők sokszor celebek, ismert cégnevek reklámjaival kínálnak hamis befektetési lehetőségeket. Gyakori az is, hogy adománygyűjtésre vagy ismert hatóságokra hivatkozva próbálják kicsalni az ügyféladatokat. A KiberPajzs együttműködés tájékoztató anyagai, segítsége révén előre felkészülhetünk a támadási kísérletekre. Ha már megtörtént a baj, érdemes haladéktalanul megkeresni bankunkat és feljelentést tenni a rendőrségen.

Egyre elterjedtebb a **hamis befektetési lehetőséget** kínáló csalástípus, de az is megtörténhet, hogy a ténylegesen, online megvásárolt befektetéseket (részvény, kötvény, kriptodeviza) lopják el a csalók. Ezeket gyakran – a tudtuk és beleegyezésük nélkül – közismert emberek, sportolók, modellek képeivel és ajánlásával visszaélve hirdetik, megbízható, ismert vállalkozás nevéhez nagyon hasonlító cégnévvel, kiemelkedő hozamot, biztonságos befektetési lehetőséget ígérnek vagy kedvező adózási feltételekkel kecsegtetnek.

Egy ilyen csapdába sétált bele az az ügyfél is, aki ismert celeb által reklámozott befektetési hirdetést talált az interneten és jelentkezett az ott megadott e-mail címen. Nemsokára telefonon kereste egy „befektetési tanácsadó”, aki olyan meggyőző volt, hogy az ügyfél maga utalt el egy kisebb összeget, melyhez a „tanácsadó” még technikai segítséget is nyújtott. Az ügyfél visszaigazolásul kapott egy linket, ahol úgy tűnt, nyomon tudja követni a befektetését.

Miután azt látta, hogy majdnem megduplázódott a pénze, még többet akart. Az újabb telefonhívás során ismét technikai segítségnyújtásnak álcázva irányították a csalók az ügyfelet, QR kódokat is küldtek neki, azokat kellett beolvasnia a mobiljával, így több átutalást is indított. Amikor azt látta, hogy jóváírások érkeznek a számlájára, gyanút fogott, de a „tanácsadó” azt állította (hamisan), hogy az MNB ellenőrzi a fedezetet és át is kapcsolta egy másik „ügyintézőhöz”, aki megnyugtatta, hogy biztonságban van a pénze. Valójában azonban az ügyfél meglévő befektetéseit váltották vissza, és az értékpapírszámlájáról érkeztek a folyószámlájára az összegek. Így végül nem lett új befektetése sem és a meglévő megtakarítását is elutalta a csalóknak.

Hogyan védekezhet? Ne olvassa be a gyanúsnak ítélt forrásból származó QR-kódokat! Ha már beolvasta és a céloldalon egy bejelentkezési űrlap jelenik meg, amely személyes vagy banki adatokat, jelszavakat kér, semmiképp ne adja meg ezeket, az oldalt pedig azonnal zárja be! Használja inkább a hivatalos weboldalt és legyen körültekintő, ne dőljön be a „túl szép ahhoz, hogy igaz legyen” ajánlatoknak, a gyors megtérülés és kiemelkedően magas hozam ígéretének!

Az MNB-hez számos olyan panasz is érkezett, mely szerint az ügyfelek jóhiszeműségét vagy hiszékenységét használták ki a csalók. Több ügyfél is elmondta, hogy a hívó nagyon megnyugtatóan és lassan beszélt, kedves és segítőkész volt, technikai segítséget is adott. Sok esetben viszont ennek épp az ellenkezőjét tapasztalták, a hívó hadart, sürgető volt a hangneme, a háttérben is nyüzsgés hallatszott, mintha egy telefonos ügyfélszolgálaton több ügyintézővel lenne egy légtérben és többeket át is kapcsoltak egy másik „ügyintézőhöz”.

Volt, hogy adományt gyűjtöttek, nyereményjátékot hirdettek, de visszaéltek hatóságok, a kormány, az államkincstár, a rendőrség és az MNB nevével, logójával vagy akár telefonszámával is. Az egyik ügyfél elhitte, hogy ha a kapott számsort, vagyis az „ellenőrző kódot” az összeg mezőbe, a „szinkronizálás” szót a megjegyzésbe beírja, akkor csak a számlaszáma valódiságát ellenőrzik, és

meg fogja kapni a nyereményét. Helyette azonban az „ellenőrző kód” összegével megterhelték a bankszámláját, hiszen valójában nem szinkronizációt, hanem önszántából átutalást indított megtévesztés következtében. Volt olyan eset is, ahol a károsult a csalók kérésére a hívás során lejátszott sípszó után az „automatának” adta meg a kért adatokat.

Számtalan módszerrel támadhatnak tehát a csalók, amelyek folyamatosan változnak. Nem csak az idősek, de minden korosztály vagy társadalmi csoport lehet célpont, és akár bármikor újra megkereshetik a szélhámosok vagy eladhatják az adatokat más bűnözőknek, annak az adatait is, aki korábban már csalás áldozata volt. Fontos tudni, hogy ha van online hozzáférése más személy, például családtag számlájához (állandó meghatalmazottként, számla feletti rendelkezőként vagy épp társtulajdonosként), akkor a netbankján/mobilbankján vagy akár a társkártyáján keresztül az ő pénzeszközeihez is hozzáférést engedhet a csalóknak. Az egyik áldozat internetbankján keresztül például a csalók a lánya számláján lévő összeget is megszerezték így, pedig csak a cipőjét akarta eladni.

Hogyan védekezhet? Győződjön meg a tartalom valódiságáról, alaposan fontolja meg a mellékletek letöltését, applikációk vagy szoftverek telepítését, a hivatkozásokra való kattintást! Csak a szolgáltatók hivatalos weboldalán vagy mobilapplikációjában fizesse ki a számláját, telefonon soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV/CVC-kódját, online banki jelszavát vagy hitelesítési kódját.

Igényeljen – az MNB ajánlása alapján rövidesen díjmentesen biztosítandó – biztonsági célt szolgáló azonnali tranzakciófigyelési (számla- és kártyafigyelési) szolgáltatást a visszaélések észlelése, későbbi visszaélések megelőzése érdekében! Állítson be számlájához és kártyájához napi és tranzakciós limiteket, online vásárlási limitet vagy korlátozást, továbbá bankkártyája földrajzi használhatóságának korlátozását, amennyiben van rá lehetőség, használjon egyszerhasználatos (digitális/virtuális/web) kártyát!

Ha mégis megtörténik a baj, tegyen feljelentést a rendőrségen és haladéktalanul jelentse a bankjánál a visszaélést! A kárenyhítés érdekében kérjen azonnali intézkedést, tiltassa le a kártyáját vagy a netbanki/mobilbanki hozzáférését is. Tegyen panaszt bankjánál!

A banknak jogszabályi kötelezettsége a bejelentések kezelése, és a vitatott fizetési művelet teljesítési körülményeinek megvizsgálása (például, hogy szükség esetén megtörtént-e az erős (kétfaktoros) ügyfél-hitelesítés, illetve a fizetési művelet megfelelő rögzítése). A bank köteles felelősséget vállalni, adott esetben a jóvá nem hagyott vagy hibásan teljesített megbízás összegét visszatéríteni, amennyiben nem az ügyfél megbízása szerint járt el.

A bizonyíthatóan az ügyfél által jóváhagyott, illetve az ő súlyos gondatlansága vagy csalárd magatartása miatti tranzakcióknál viszont mentesülhet is **a kárviselési felelőssége alól**. A bank a kivizsgálás eredményéről köteles tájékoztatni az ügyfelet és részletesen indokolnia kell, ha elutasítja a panaszt.

Ha a bank elutasította az összeg visszatérítését, esetleg nem is válaszolt a panaszra vagy ha a válasz nem érdemi vagy nem teljes körű, illetve a bank a panaszt nem a jogszabályban előírt módon kezelte, vizsgálta ki, az ügyfél fogyasztóvédelmi eljárást kezdeményezhet az MNB-nél. **Annak megítélése azonban, hogy a bank megalapozottan hivatkozott-e a kárviselési felelősség alól mentesítő valamely körülmény fennállására (pl. az ügyfél súlyosan gondatlan magatartására), bírói útra tartozik, így amennyiben az ügyfél kártérítési igényt kíván érvényesíteni a bankkal szemben, erre bíróság előtt, polgári perben van lehetősége.**

A kiberbiztonsági kockázatok megelőzésére, csökkentésére 10 állami intézmény, köztük az MNB és pénzpiac szereplői **KiberPajzs** néven közös kommunikációs és edukációs kampányt folytatnak, továbbá elemzik a folyamatokat, lehetséges intézkedéseket az elektronikus pénzügyi szolgáltatásokat igénybe vevő ügyfelek támogatására, védelmére.

KiberPajzs
Védelem a pénzügyekben

Az egyes csalástípusokról, ismertető jegyeikről, teendőkről a KiberPajzs oldalán további információkat talál (Ön felismerné az összes csalástípust? | KiberPajzs), emellett érdemes felkeresni az MNB Pénzügyi Navigátor weboldalának digitális biztonsággal kapcsolatos oldalát is, amelyen szintén hasznos információk találhatók a témában. Ugye megnézi a szöveg mögötti linket mielőtt kattint?

** A cikk szerzője, az MNB fogyasztóvédelmi munkatársa*

„Szerkesztett formában megjelent 2024. szeptember 25-én a VG.hu oldalon.”
