Dr. Lakó Anita*

Hihetetlen hozam pár kattintással? – A befektetési csalók trükkjei

Nem csak jövőbeni ígéretekkel, de a korábbi – gyakorta kriptovalutás – befektetéseinken elért állítólagos mesés hozamokkal is átverhetnek minket az adathalász bűnözők. Valójában semmit sem tudnak rólunk, de ha nem figyelünk, e sztorikkal kicsalhatják banki azonosítóinkat, majd elvehetik számlapénzüket. A pénzügyi békéltetőknél jelentkezett egyik károsult nevében még személyi hitelt is felvettek a csalók.

Kis befektetés, hatalmas hozam? Legyünk körültekintőek és tartsuk észben az örök szabályt: ha valami túl szép ahhoz, hogy igaz legyen, akkor nagy valószínűséggel nem is az. Sok ember rendelkezik manapság kriptovalutás befektetéssel, amely újabb lehetőséget biztosíthat a visszaélésekre.

Azt már tudjuk, hogy óvatosnak kell lenni, ha kihagyhatatlannak tűnő, kockázatmentes, gyors hozamot ígérő befektetési lehetőségeket kínálnak. Az alábbiakban bemutatott esetekben azonban az áldozatokat azzal keresték meg, hogy egy évekkel korábbi befektetésükkel értek el elképesztő hasznot, melyhez most könnyedén hozzá is juthatnak. Az ismeretlen telefonáló felvázolja egy már elfeledett befektetés eredményét és egy gyors, egyszerű ügyintézés ígéretével foszt meg minket számlánk akár teljes egyenlegétől. Ám adott esetben a kárunk még ennél is nagyobb lehet.

Kiemelés:

> ***„Vissza-visszatérően megjelennek azok a csalástípusok, ahol a bűnözők egy korábbi befektés hozamának jóváírásához kínálnak segítséget. Mint jó néhány adathalász támadás, ez a módszer is az érzelmi manipulációra támaszkodik."***

Az egyik, a Pénzügyi Békéltető Testületet (PBT) megkereső károsult kriptovalutát vásárolt online, nagyjából hatvanezer forintnak megfelelő összegben. Körülbelül egy évvel később telefonon arról értesítették, hogy immár hárommillió forintos eredményt sikerült elérnie. A hozam kifizetése érdekében e-mailben küldtek egy linket, melyre rákattintva látta a befektetéshez kapcsolódó teljes számlatörténetét, a kezdeti befektetéstől az egyenleg folyamatos alakulásáig. Az összeg dollárban volt feltüntetve, ezért a saját forint befektetési számlájára történő utaláshoz azt még át kellett váltani. Ennek érdekében e-mailben küldtek neki egy QR kódot, melyet mobilalkalmazáson keresztül kellett beolvasnia.

Miután a számlatörténetben láthatóvá vált, hogy az átváltás megtörtént, már csak a befektetési számláról a saját bankszámlájára kellett átvezetnie az összeget, ennek jóváhagyásához szintén QR kódot kapott. Ezt is beolvasta, majd észlelte, hogy hárommillió forintot utaltak el a számlájáról ismeretlen számla és személy részére. Azonnal hívta a bankját, ahol a vizsgálat során megállapítást nyert, hogy a beolvasott kódokkal a csalók által kezdeményezett internetbanki bejelentkezést és utalást hagyta jóvá.

Az említett történetnél is rémisztőbb esetekben a bűnözők amellett, hogy a teljes számlaegyenleget elutalják, még személyi kölcsön felvételében is „segédkeznek", és annak összegét is kicsalják az áldozatoktól. Az egyik ilyen ügyben – az előzőhöz hasonlóan – a károsult több éve fektetett be

kriptovalutába körülbelül ötvenezer forintot, majd meg is feledkezett róla. Hosszú idő után telefonon vették fel vele a kapcsolatot azzal, hogy a befektetése utáni, immár több millió forintra rúgó hozamot szeretnék utalni neki.

Az ismeretlen telefonáló személy tájékoztatása szerint ennek érdekében az összeg átváltása volt szükséges, melynek költségét személyi kölcsönből kellett finanszíroznia. Megnyugtatták, hogy ennek összegét a hozammal együtt vissza fogják utalni. A könnyebb együttműködés és segítségnyújtás érdekében javasolták egy távoli hozzáférést biztosító alkalmazás letöltését a számítógépére, melynek ő eleget is tett. Közben követte a telefonon kapott utasításokat, így belépett készülékén a netbanki felületére, bediktálta az SMS-ben kapott kódokat. Miután a személyi kölcsön összegét – egy sikeres limitemelést követően - tovább utalták, közölték, hogy ez sajnos még nem elég, újabb kölcsön felvételére lenne szükség. Ez már gyanússá vált az áldozatnak, így azonnal felvette a kapcsolatot a bankjával és akkor szembesült a ténnyel, hogy adathalász támadás áldozatává vált.

Sajnos több esetben előfordult, hogy a bank észlelte a számlához kapcsolódó gyanús tevékenységet, és erről üzenetben, illetve telefonon tájékoztatta is az ügyfelét, aki - a megtévesztés hatására - a tranzakció jogosságát elismerte és kérte az utalás engedélyezését. A károsultak szinte minden esetben elmondják, hogy a hívó fél nagyon precízen ismerteti az általuk megteendő, egymást követő lépéseket, így nem válik gyanússá a folyamat. A tapasztalatok szerint a visszaélő sokszor még annak lehetőségét is előre jelzi, hogy megkeresés fog érkezni a bank részéről, és annak okára is ad az adott helyzetben észszerűnek tűnő magyarázatot.

A PBT előtti sajnos sok hasonló, kibercsalás áldozatává vált ügyfél jelenik meg. A kérelmükre indult eljárásokban a bankok arra hivatkoztak, hogy az érintett károsult súlyosan gondatlanul megszegte a pénzforgalmi törvény rendelkezéseit, és hogy a visszaélés megakadályozható lett volna azáltal, ha az kellő gondossággal és körültekintéssel jár el.

A tapasztalat azt mutatja, hogy a sikeres visszaélésekhez hozzájárul az ügyfelek aktív közreműködése, így azok megakadályozásában is elengedhetetlen az ő részvételük. Kortól, nemtől és iskolai végzettségtől függetlenül bárki lehet visszaélés áldozata, így mindenkinek érdemes megfogadni az alábbiakat:

- elsőként mindig gondoljuk át nyugodtan, hogy pontosan miért vették fel velünk a kapcsolatot és mit, miért kérnek tőlünk;
- ne adjuk ki ismeretleneknek a bankszámlánkhoz kapcsolódó, hozzáférést biztosító adatokat;
- egyes programok/alkalmazások telepítése előtt tájékozódjunk, mire szolgálnak;
- a bankoláshoz is használt készülékünkhöz ne engedjünk hozzáférést ismeretlen személyeknek, a távoli hozzáférés ideje alatt ne lépjünk be a banki felületekre;
- a bankunktól kapott SMS vagy push üzenet szövegét minden esetben olvassuk el figyelmesen, értelmezzük, ellenőrizzük, hogy annak tartalma a szándékunknak megfelel-e;

- ha visszaélésnek csak egy csekély gyanúja is felmerül, azonnal szakítsuk meg a folyamatot és hívjuk a bankunk ügyfélszolgálatát az elektronikus szolgáltatások/bankkártya korlátozása érdekében;
- tudakozódjunk, van-e lehetőség a mobilalkalmazásban/internetbankban a visszaéléssel érintett elektronikus szolgáltatások, a bankkártya azonnali felfüggesztésére, ha igen, csalás gyanúja esetén éljünk ennek lehetőségével.

Az adathalászattal kapcsolatban a 10 hatóság által közösen működtetett www.kiberpajzs.hu honlap mutatja be egyszerűen, közérthetően a leggyakoribb bűnözői mintázatokat. Emellett a bankok is különböző tájékoztató anyagokat helyeznek el saját honlapjukon, egyéb internetes felületeken, figyelemfelhívásokat küldenek e-mailen, netbankon vagy mobilalkalmazáson keresztül. Néhány banknál a visszaélésekkel kapcsolatos tudásunk tesztelésére is van lehetőség, ahol a kérdések megtörtént eseteket dolgoznak fel, ezzel is elősegítve a helyzet felismerését. Célszerű ezeket rendszeresen figyelemmel kísérni és napra késznek lenni banki csalások módszereiről.

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

„Szerkesztett formában megjelent 2024. december 4-én a VG.hu oldalon.”