Pappné Márk Anita – dr. Seben-Pados Emese – dr. Szabó Nóra*: Továbbra is kibercsalásokról panaszkodnak az ügyfelek az MNB ügyfélszolgálatán

Az MNB a közelmúltban több fórumon is felhívta a figyelmet a kibercsalások, adathalász támadások veszélyeire. E cikkünkben a legelterjedtebb csalási módszereket, s a védekezés lehetőségeit mutatjuk be.

A kibercsalások között idén is az egyik legelterjedtebb módszer a csomagküldéshez kapcsolódik. Ha valaki meghirdetett már eladásra bármilyen terméket, nagy valószínűséggel találkozott adathalász megkereséssel. Jó esetben csak bosszantó, hogy valódi adásvétel helyett csalókat kell letiltani és jelenteni az adott portálon. Egyre többen figyelnek már ugyan a csalásra utaló jelekre, mégis sokan online adásvétel kapcsán elkövetett adathalászat miatt veszítik el megtakarításukat, munkabérüket, nyugdíjukat, vagy akár a családtámogatás összegét.

Ezen felül akár a biztonsági tartaléknak használt, a számlához tartozó folyószámla-hitelkeret összegét is lemeríthetik a csalók. Attól függően, hogy milyen adatokat csalnak ki tőlünk, akár személyi kölcsönt is igényelhetnek a nevünkben online módon. Sőt, ha valaki például internetbanki felületet használ meghatalmazottként, akkor még nagyobb a kockázat, hiszen csalás esetén veszélybe kerülhet mind a meghatalmazó, mind a meghatalmazott megtakarítása.

Sokszor előfordul, hogy az eladónak rossz előérzete van, de aztán mégis követi a csalók által adott utasításokat. Ennek a legyakoribb oka a sietség, az állítólagos vevő sürgetése, az eladó elfoglaltsága, a megelőlegezett bizalom egy hamis megkeresés kapcsán vagy akár az előzetes tájékozódás hiánya.

Mielőtt valamely platformot igénybe veszünk, tájékozódjunk annak használatáról, hogy lehetőség szerint ki tudjuk szűrni, ha valaki nem az adott platform tájékoztatójában írtak szerint jár el! Szükség esetén kérjünk tájékoztatást az adott platform üzemeltetőjétől annak hivatalos elérhetőségén! Akárcsak a bankok, az ismertebb adásvételi platformok, futárszolgálatok is jellemzően közzéteszneknek adathalászattal kapcsolatos figyelmeztetéseket. Megtakarításaink védelme érdekében ismerjük meg ezeket a tájékoztatókat is, mielőtt az adott platformot használni kezdjük, a csalók ugyanis sok esetben megfelelő tájékozódásunk hiányára építenek.

Amikor eladóként meghirdetünk valamely terméket, többnyire már elterveztük, hogy mire fogjuk költeni a pénzt. Amikor a hirdetésre jelentkezik valaki, örülünk, hogy az adásvétel is gyorsan végbemegy. Legyünk azonban óvatosak, és ne higgyünk el mindent: legyen például gyanús, ha a hirdetés megjelenése utáni percekben máris érdeklődnek a meghirdetett termék iránt. Persze előfordulhat ilyen is, de legyünk tisztában azzal, hogy az új hirdetés-megjelenéseket figyelhetik a csalók.

A hirdetésünkre gyakran valamely csevegőprogram igénybevételével jelentkeznek, ilyenkor az új csevegés indításakor jellemzően már eleve megjelennek egy esetleges csalásra figyelmeztető szolgáltatói üzenetek. Ezeket soha ne hagyjuk figyelmen kívül, mindig gondoljuk át, valós lehet-e az érdeklődés!

Sokféle történettel bírhatják rá a jellemzően eladni kívánó felhasználókat, hogy működjenek együtt. Ha ragaszkodik a vevő a futárszolgálat igénybevételéhez, akkor legyünk résen! Gyorsan ki lehet deríteni, hogy valódi érdeklődővel levelezünk-e, vagy csak a pénzünket akarják megszerezni.

Ilyenkor kérdezni kell, ne sajnáljuk rá azt a néhány plusz percet, mert a válasz árulkodik arról, hogy csalóval van-e dolgunk. A magyartalan megfogalmazás, a kérdéseinkre adott furcsa válaszok, a logikátlan adásvételi feltételekhez való ragaszkodás – például egy szekrénysor csomagküldő szolgálat automatájába helyezésének kérése – mind intő jelek lehetnek.

Ha a potenciális vevő által megrendelt futárszolgálaton keresztül zajlik a szállítás és a vevő általi fizetés, banki, bankkártya-adatainkat csak akkor adjuk meg, ha meggyőződtünk arról, hogy ténylegesen a futárszolgálat küldte az e-mailt, illetve SMS-t. Mindig ellenőrizzük a küldő tényleges e-mail címét, illetve a weboldal URL-adatait is! Segíthet a megelőzésben, illetve a károk mérséklésében, ha online adásvétel során virtuális kártyát használunk. Így egy esetleges visszaélés során nem a „főszámlánkon" lévő egyenleghez juthatnak hozzá illetéktelenek bankkártyánk adatain keresztül, hanem „csak" a virtuális kártyánkra általunk átvezetett összeghez.

Ha azt írja a vevő, hogy már átutalta a pénzt, akkor tegyük fel a kérdést, hogy pontosan hová is? Ha nem ismerjük az adásvétel megszokott módját, akkor ne hagyatkozzunk az ismeretlenek által küldött információra. Ha írásban kapjuk meg ezeket, intő jel, ha gépies, rossz ragozású a leírás.

A csalók először is addig ügyeskednek, amíg meg nem adjuk az e-mail címünket. Lehetséges, hogy ezután olyan linket küldenek, amelyre rákattintva valamelyik futárcég hamisított weboldalára kerülhetünk. Erről egy hamis banki oldal nyílhat meg, amely látszólag azonosnak tűnhet valódi bankunk honlapjával.

A csalók sokszor QR-kód beolvasását kérik az adathalász e-mailben, innen a kód szintén egy hamis banki oldalra vezethet. Találkozhatunk QR-kóddal az e-mailből kapott link útján megnyitott hamis banki oldalon is. Mivel a QR-kód annyit sem árul el, mint egy link – amelynél legalább látjuk, hova vezet a hivatkozás –, nagyon körültekintően kell eljárni ilyen esetben is! Ne olvassunk be olyan QR-kódot, amelynek eredete bizonytalan!

Az ilyen csalások további visszatérő fordulata a pénz fogadásához kapcsolódik. A vételárat azonban nevünk és bankszámlaszámunk ismeretében át tudják utalni részünkre. Nem szükséges QR-kód és ehhez egyéb adat megadása sem. A pénz jóváírásakor ma már SMS-t kaphatunk, illetve netbankunkba belépve láthatjuk egyenlegünk változását.

Mindezek mellett továbbra is sokszor előfordul, hogy bankunk „nevében" keresnek minket – általában – telefonon, amelynek során bankszámlánkat érintő csalásveszélyről tájékoztatnak. Ilyenkor általában sürgős ügyintézést, a számítógépünkre távoli elérést biztosító program (jellemzően: AnyDesk, Teamviewer) letöltését szorgalmazzák, hogy hozzáférjenek internetbankunkhoz, amelyen keresztül például jogtalan átutalásokat kezdeményeznek a csalók.

Előfordul ugyanakkor az is, hogy nemcsak a folyószámlánkon lévő pénzösszeg érintett a visszaélésben, hanem egyéb megtakarításaink, például értékpapírszámlánk, lekötött betéteink is. Hamis biztonságérzetet ad, hogy a megtakarításainkat lekötöttük, s azok elkülönítettek, hiszen azokhoz például internetbanki visszaélés során hozzáférhetnek illetéktelenek.

Az ismerősnek tűnő banki telefonszám se tévesszen meg minket, a csalók sokszor a hívószámokat „másolva" képesek elfedni, hogy honnan telefonálnak valójában. Ilyenkor érdemes a bankot a hivatalos telefonszámán hívni és ellenőrizni a hívás valódiságát.

Mivel a visszaélések nemcsak folyószámláinkat érinthetik, tájékozódjunk arról is, hogy megtakarításaink milyen módon válthatók vissza, vezethetők át bankszámlánkra. Ezzel kapcsolatban a bankkal kötött keretszerződéseink, valamint azok elválaszthatatlan részét képező általános szerződési feltételek (üzletszabályzatok, hirdetmények, stb.) adhatnak pontos tájékoztatást. Alaposan tanulmányozzuk át az internetbanki, mobilbanki felületeinket is, legyünk tisztában azzal, hogy ezen felületeken keresztül mi magunk, illetve egy esetleges visszaélés során mások milyen műveleteket tudnak végrehajtani. Legyünk tisztában például lekötött betétünk feltörésének, átutalási, vásárlási limitünk megváltoztatásának módjaival. Fizetési tranzakcióinkhoz kapcsolódóan célszerű limiteket beállítani – például az online térben való vásárlás limitösszegét –, de ugyanilyen fontos lehet, hogy ha tudjuk, hogy a közeljövőben nem kívánunk külföldön vásárolni, lehetőség szerint tiltsuk le akár a bankkártya külföldön történő használatát.

Ha meghatalmazottként járunk el valaki nevében, akár még az ő pénze is veszélybe kerülhet. Legyünk tisztában azzal, hogy a számláinkhoz (akár takarék-, értékpapírszámla stb.), kinek van még hozzáférése. Előfordulhat, hogy egy társkártya visszavonása nem jelenti a számlák kapcsán adott meghatalmazás visszavonását is, így a meghatalmazott továbbra is rendelkezhet számláink felett. Technikai okokból a meghatalmazott internetbanki felületén továbbra is feltűnhet a meghatalmazó bankszámlája. Így egy őt ért támadáskor meghatalmazóként a mi számlánk is érintett lehet. Épp az ilyen esetek elkerülésére fogalmazta meg elvárásait az MNB egyik vezetői körlevelében.

Kiskorúak bankszámláinál is nagyon fontos a tudatos bankolás, a digitális biztonság alapjainak megismertetése gyermekeinkkel. Fontos megtanítani őket arra, hogy az általuk használt eszközökre – például telefon, tablet, laptop – bejövő e-maileket, telefonhívásokat, SMS-eket körültekintően, illetve fenntartásokkal kezeljék. Az adathalász célú visszaélések, azok kísérletei ugyanis őket sem kímélik, bankszámláik ugyanúgy ki vannak téve a kibercsalás veszélyének, mint bármilyen egyéb bankszámla. Ez alól az sem kivétel, ha telefonszámukat, e-mail címüket csak a közeli barátaik ismerik, ugyanis ezen információk a legnagyobb elővigyázatosság ellenére is illetéktelenek birtokába kerülhetnek (például, ha valamely online közösségi platformon nyilvánosságra hozzák azokat).

Manapság ugyancsak gyakran fordul elő az is, hogy gyors hozamot ígérő, hamis befektetési lehetőségekkel keresnek meg minket. Ehhez elkérik bankkártyánk adatait is, amelyen keresztül a „nyereséget ki tudják fizetni” vagy a befektetés reményében először csak kisebb pénzösszeg átutalását kérik egy megjelölt bankszámlára. Ilyen esetben is legyünk gyanakvóak, több csatornán is ellenőrizzük a befektetési lehetőséget ajánló szolgáltatót, mindenekelőtt az MNB Piaci szereplők keresőjében.

Ha a szolgáltató nem szerepel az MNB keresőjében, érdemes más forrásból is tájékozódnunk, ilyen esetben az MNB Ügyfélszolgálatán, illetve a Pénzügyi Navigátor Tanácsadó Irodahálózatnál is szakértő segítséget kaphatunk. Nézzük át a szolgáltató hivatalos honlapját, a közösségi médiában megjelenő tartalmakat, egyéb, interneten található információkat is. Célszerű lehet a szolgáltató hivatalos elérhetőségén tájékozódni arról, hogy az adott befektetési lehetőséget tényleg az adott szolgáltató kínálja-e, ugyanis előfordulhat, hogy ismert szolgáltatók, személyek nevére hivatkozva próbálnak illetéktelenek pénzt szerezni, akár hasonló hangzású cégnévvel.

Olyan csalástípus is ismert, hogy nyereményjátékkal kecsegtetnek minket és a nyeremény „átvételéhez" kérik ismeretlen program telepítését, illetve banki adataink megadását. Ebben az esetben is az állítólagos nyereményjáték meghirdetőjének hivatalos elérhetőségein kérjünk felvilágosítást.

Ha felmerül bennünk a gyanú, hogy visszaéltek, visszaélhetnek banki adatainkkal, haladéktalanul keressük meg pénzügyi szolgáltatónkat, szükség esetén kérjük internetbankunk, bankkártyánk letiltását és tegyünk feljelentést a rendőrségen.

A kiberbűnözők sokszor az emberi jóhiszeműséget, hiszékenységet kihasználva csalják ki banki adatainkat és azokkal visszaélve okoznak kárt. Hogy ezt elkerüljük, tegyünk meg mindent, tájékozódjunk előzetesen és minél teljesebb körűen. Fogadjuk egészséges kételkedéssel a túl szépnek látszó ajánlatokat. Ne engedjünk a csalók pszichikai vagy sürgető nyomásgyakorlásának! Kérjünk időt a hallottak, olvasottak értékelésére, átgondolására.

A digitális biztonság erősítésére életre hívott KiberPajzs kezdeményezés honlapján megismerhetők az alapvető csalástípusok, sok érdekes és tanulságos eseten keresztül tájékozódhatunk a csalók aktuális módszereiről is. Az MNB vezetői körlevélben is megfogalmazta a bankok visszaélésekkel kapcsolatos tájékoztatásra vonatkozó elvárásait. Adathalászattal kapcsolatban hasznos információk olvashatóak továbbá a Nemzeti Kibervédelmi Intézet (NKI) honlapján is.

**A szerzők az MNB Ügyfélkapcsolati Információs Központjának munkatársai*

„Szerkesztett formában megjelent 2024. június 19-én a VG.hu oldalon."