EGYRE GYAKORIBB AZ ELADÓK ÁTVERÉSE AZ ONLINE PIACTEREKEN

Az egymás közötti adásvételt egyszerűen és ingyenesen lehetővé tévő online platformok, más néven online piacterek egyre több csalót vonzanak. Pár éve még a vevők megkárosítása volt a jellemző, manapság azonban már az eladók is a visszaélések céltáblájává válhatnak. Az ilyen esetekben az óvatlan eladót úgy verik át, hogy **a piactéren „értékesített" áruért járó ellenérték fogadásához vagy az áru kiszállításához valamilyen szokatlan, további teendőt várnak el**.

Nem mindenki használja csaló szándékkal az internetet, azonban fő az óvatosság és a biztonság, amellyel megakadályozhatjuk, hogy megkárosítsanak bennünket! Az online hirdetési platformokon 3-4 éve még az volt a csalási trend, hogy nem olyan minőségű áru érkezett a vevőhöz, mint ígérték, vagy egyáltalán meg sem érkezett a kívánt termék, amit a jóhiszemű vásárló előre kifizetett.

Egyre gyakoribb azonban, hogy a vevők mellett **az eladók is a csalók célpontjává válnak**. Az online fizetési lehetőségek elterjedésével további visszaélési módok jelentek meg, és a virtuális térben már **közvetlenül az ügyfelek adatai, bankkártyái és fizetési számlái, illetve bankszámlái is veszélybe kerülhetnek**. Nagyon fontos tehát, hogy a piacterek felhasználói megismerjék az online átverések tipikus trükkjeit, és megtudják, hogy mire figyeljenek biztonságuk érdekében.

Hogyan ismerjük fel az átveréseket?

Az eladó megkárosításának egyik leggyakoribb módja, hogy a vevő felhívja őt azzal, hogy kifizette a meghirdetett terméket. A „vásárló" kéri, hogy valamilyen távoli hozzáférést biztosító programot telepítsen (például AnyDesk vagy TeamViewer), az eladó a gépére vagy telefonjára annak érdekében, hogy **„biztosítva legyen az átutalás fogadása"**. Már ekkor **legyen éber, és szólaljon meg a belső vészcsengője**! Akinek nem elég az átutaláshoz a név és a számlaszám megadása, azzal a továbbiakban ne is álljon szóba!

Sajnos sok esetben a tájékozatlan eladó a kérésnek eleget tesz, majd végignézi, ahogyan belépnek az internetbanki fiókjába. A károsult gyakran még az úgynevezett erős vagy más néven több faktoros hitelesítésben is segédkezik (például megadja a csalóknak az SMS- ben kapott kódot), ami azt eredményezi, hogy a csalók kizárják őt a saját banki profiljából és kiürítik a bankszámláját.

Tanulság:

Pénzösszeg fogadásához a számlatulajdonos nevén és bankszámlaszámán (esetleg – kizárólag belföldi forint átutalások esetében - bankszámlaszám helyett használt másodlagos azonosítóján, például e-mail címén vagy mobiltelefonszám) kívül semmi egyébre nincs szükség. Akinek ez nem elég, azzal szakítsuk meg a kapcsolatot.

Soha ne töltsünk le ismeretlen programot vagy applikációt számítógépre, telefonra.

Sokszor előfordul, hogy **az eladó egy sms-t kap, amelyben tájékoztatják, hogy a termékét kifizették, de „fogadnia kell az összeget”** az üzenetben küldött link segítségével, vagy a termék kiszállításához ajánl a „vevő” csomagküldő szolgálatot (jogszerűen működő cégek nevével visszaélve, pl.: Foxpost, DHL, DPD, MPL) és a nevükre hivatkozással **küldenek adathalász linket tartalmazó üzenetet vagy e-mailt**. Amikor az eladó gyanútlanul rákattint, akkor egy, a csalók által készített hamis weboldalon találja magát, ahol meg kell adnia bankkártyaadatait (amivel ezután a csalók vissza tudnak élni, például vásárolhatnak vele) vagy **ki kell választania a számlavezető bankját, és arra kattintva megadni a saját banki belépési adatait**. Utóbbi esetben az eladó érzékeny banki belépési adatai kerülnek illetéktelen kezekbe. Mivel ez **a hamis oldal a valódi banki oldalnak továbbítja az adatokat, az óvatlan ügyfél (eladó) megkapja az egyszer használható bejelentkezési kódot (pl. SMS kódot), és azt is begépeli a hamis oldalon**. Így **a csalók bejutnak az ügyfél banki profiljába és a számlán lévő pénzhez is hozzáférnek**, azt azonnal elutalhatják, ellophatják. Ugyanakkor néha a csalás és a tényleges jogosulatlan átutalás között napok is eltelhetnek, ezért kiemelten fontos, hogy amint észleljük, hogy csalás áldozatai lettünk, akkor **azonnal, késlekedés nélkül jelentsük az esetet a bankunknak és tegyünk feljelentést**.

Tanulság:

Pénzösszeg fogadásához a számlatulajdonos nevén és bankszámlaszámán (esetleg ún. másodlagos azonosítóján) kívül semmi egyébre nincs szükség. Akinek ez nem elég, azzal szakítsuk meg a kapcsolatot!

Nem kell netbanki fiókunkba bejelentkezni vagy a kártyaadatainkat megadni ahhoz, hogy pénzt fogadjunk.

Soha ne kattintsunk sms-ben vagy emailben érkező ún. pénzfogadást megerősítő vagy fizetési linkekre!

A biztonságtudatosság és az óvatosság kiemelten fontos az online térben is!

Az alábbi kép szemlélteti hogyan néznek ki a hamis bankválasztó oldalak. Ezeket mindig hagyja figyelmen kívül!