A “Pig Butchering” típusú online csalás

NEMZETI KIBERVÉDELMI INTÉZET

Mi az a “pig butchering”?

A „pig butchering”, azaz „disznóvágásos” csalás egy összetett, több szakterület határán elhelyezkedő online bűncselekmény-típus, amely a pszichológiai manipuláció (social engineering) és a digitális infrastruktúra kihasználásán alapul. A csalók hosszú távú, fokozatosan kiépített bizalmi kapcsolat révén manipulálják az áldozatokat, céljuk pedig az, hogy jelentős pénzösszegeket csikarjanak ki tőlük valótlan befektetési lehetőségek ígéretével. A név metaforikusan utal arra a folyamatra, ahogyan az elkövetők „felhizlalják” az áldozatot – azaz bizalmat és érzelmi kötődést építenek ki –, majd „levágják”, amikor már a maximális pénzügyi kiaknázás megvalósult.

Az INTERPOL 2024 decemberében kiadott hivatalos közleményében arra hívta fel a figyelmet, hogy a köznyelvben és a médiában érdemes kerülni a „pig butchering” – magyarul „disznóvágásos csalás” – kifejezés használatát. Az elnevezés ugyanis sértő és embertelenítő lehet az áldozatok számára, akik emiatt gyakran szégyent éreznek, és sokkal ritkábban fordulnak segítségért vagy tesznek feljelentést. Ahogy a közlemény fogalmaz:

> *„A kifejezés azt a benyomást kelti, mintha az áldozatok tudatlanságból vagy önként sétáltak volna a vágóhídra. Ez a fajta megfogalmazás sokakat visszatart attól, hogy nyíltan beszéljenek a történtekről vagy jogi lépéseket tegyenek.”*

A támadás nem hirtelen történik: a kapcsolatfelvétel gyakran társkereső vagy közösségi oldalakon indul, mint például Tinder, WhatsApp, Facebook, Telegram vagy LinkedIn, hamis profilokkal, melyek mögött gyakran gépi tanulással generált chatbotok vagy emberi operátorok állnak. A csalók a pszichológiai manipuláció eszközeivel élnek: hosszú beszélgetések során személyes érdeklődést mutatnak, romantikus vagy mentor szerepet öltenek magukra, majd az érzelmi kapcsolat elmélyülésével áttérnek a pénzügyi ajánlatokra. A befektetési lehetőség jellemzően egy zárt, „csak belsősök számára” elérhető kriptovaluta-platform. Kisebb befizetések után a hamis platform pozitív egyenleget jelez, ez pedig megerősíti az áldozat bizalmát, így később egyre nagyobb összegeket ruház be – akár megtakarításait, kölcsönöket, vagy családi forrásokat mozgósítva.

A csalás lelki oldala legalább annyira fontos, mint a technikai. A csalók tudatosan olyan pszichológiai eszközöket vetnek be, amelyek befolyásolják az emberek viselkedését és döntéseit. Például, ha valaki sok törődést, figyelmet vagy „segítséget” kap, könnyen úgy érzi, ezt viszonoznia kell – akár bizalommal, akár pénzzel. Vagy ha már sok időt és pénzt fektetett valamibe, nehezen ismeri be, hogy hibázott – inkább tovább reménykedik abban, hogy mégis jól döntött. Az is megtévesztő lehet, ha a csaló azt mutatja, hogy mások is „sikerrel jártak” – például képernyőképeket, visszajelzéseket vagy nyereségeket mutat, amelyek mind hamisak. Emellett a csaló gyakran magabiztos, hozzáértő szerepben tűnik fel – például pénzügyi tanácsadónak vagy tapasztalt befektetőnek adja ki magát –, ami tovább növeli a hitelességét.

A cél az, hogy az áldozat érzelmileg kötődni kezdjen, és emiatt egyre kevésbé gondolkodjon kritikusan. Idővel kialakul egyfajta lojalitás, sőt akár függőség is, így az áldozat hajlamos elfogadni a csaló javaslatait – akkor is, ha már sejti, hogy valami nincs rendben. A digitális kommunikáció csak tovább nehezíti a helyzetet: a csaló arca rejtve marad, a bemutatott „bizonyítékok” – például egy hamis netbank vagy befektetési oldal – pedig nagyon is valódinak tűnnek.

Technikai szempontból ezek a csalások a klasszikus social engineering magasabb szintű, automatizált változatainak tekinthetők. A támadók gyakran élnek domain spoofinggal – vagyis olyan webcímeket hoznak létre, amelyek megtévesztően hasonlítanak ismert pénzügyi szolgáltatók oldalaira. Ezeket a hamis oldalaikat sok esetben érvényes SSL-tanúsítvánnyal látják el, így a böngésző zöld lakatot jelez, ami megtévesztő biztonságérzetet kelt a felhasználókban. Emellett gyakran használnak hamis kriptobefektetési alkalmazásokat és külön erre a célra létrehozott szervereket, amelyek professzionális kereskedési felületet szimulálnak. Az elkövetők gyakran automatizált marketingkampányokat futtatnak, deepfake-technológiákat alkalmaznak vagy közösségi médiás influenszereket klónoznak.

A detekció komoly kihívást jelent. A klasszikus védelmi rendszerek (tűzfalak, IDS/IPS, antivírus) nem alkalmasak az ilyen interperszonális, hosszú távú átverések azonosítására. Ugyanakkor a hagyományos védelmi eszközökön túl egyre nagyobb szerepet kapnak az új típusú megközelítések, például a felhasználói viselkedés elemzésére szolgáló módszerek (User Behavior Analytics – UBA), amelyek gyakran gépi tanulási algoritmusokat alkalmaznak az eltérő vagy gyanús mintázatok azonosítására. Emellett kiemelt jelentősége van a gyanús domainnevek fenyegetésalapú (threat intelligence) monitorozásának, valamint a csalásokhoz kapcsolódó szöveges mintázatok kiszűrésének természetes nyelvfeldolgozással (Natural Language Processing – NLP). Ezek az eszközök és eljárások lehetővé teszik a korai figyelmeztetések kiadását, és támogatják a megelőző biztonsági intézkedések bevezetését.

A pénzügyi szolgáltatók – különösen a kriptovaluta-tőzsdék – ebben kulcsszerepet töltenek be, mivel a tranzakciók elemzése, a pénzmozgások forrásainak ellenőrzése és a szabályalapú szűrés hatékonyan hozzájárulhat az ilyen típusú csalások visszaszorításához. A válaszintézkedések szintén strukturált megközelítést igényelnek. Az áldozatnak első lépésként minden kommunikációt le kell állítania, majd bizonyítékokat (chatlogok, képernyőmentések, webcímek) kell rögzítenie. Az esetet be kell jelenteni a megfelelő hazai (és nemzetközi) szerveknek, és amennyiben pénzintézet is érintett, a számlavezető bankkal is fel kell venni a kapcsolatot.

Társadalmi és gazdasági szinten e csalások kockázata messze túlmutat az egyéni károkon. Jelentős hatással vannak a digitális pénzügyi rendszerek iránti bizalomra, különösen a kriptovaluta-piac esetében. A „dark figure" – azaz a fel nem derített esetek száma – valószínűsíthetően rendkívül magas. A társadalom védelme érdekében multidiszciplináris együttműködés szükséges: a pszichológusok, információbiztonsági szakemberek, jogászok, pénzügyi elemzők és szabályozó szervek összehangolt fellépése elengedhetetlen.

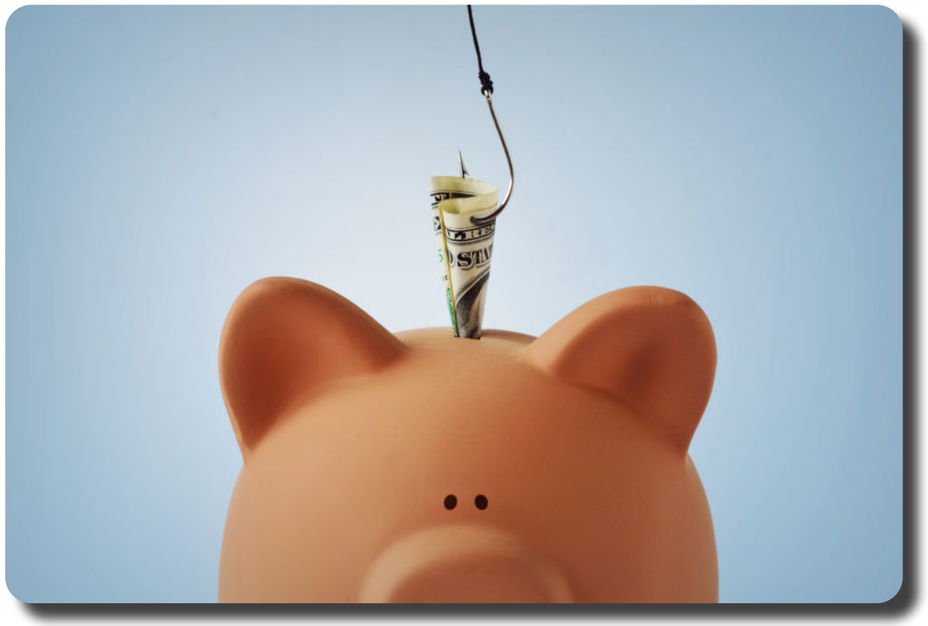
Miért veszélyesek ezek a támadások?

Gyakran beleolvad más ismert csalási típusokba. A lényeg, hogy a bizalom kiépítését más átverések szolgálatába állítja.

Csalás típusa	Leírás	Hogyan jelenik meg benne a „pig butchering"?
Nigériai csalás (419 scam)	Régi típusú átverés, amely hamis örökségekkel, pénzutalásokkal operál.	A régi „gyors pénz" helyett ma már hosszú levelezés, pszichológiai nyomás és „befektetés" is lehet része.
Romantikus csalás	Online szerelem, amelynek végén pénzt kérnek.	Hónapokig épített párkapcsolat után „közös jövőre" hivatkozva irányítják át a hamis befektetésre az áldozatot.
Kriptovaluta-átverés	Hamis kriptotőzsde, csalikampány.	A bizalomépítéssel sokkal több pénzt tudnak kiszedni az áldozatból, mint egy egyszerű hamis oldallal.

Csalás típusa	Leírás	Hogyan jelenik meg benne a „pig butchering"?
Ál-celeb kampányok	Elon Musk-féle „kriptós nyeremények".	Ha az ajánlat nem reklámként, hanem egy ismerős személy ajánlásaként jelenik meg, az egy hosszabb távú "pig butchering" típusú csalás része is lehet.
Állásajánlat, pénzmozgatás (money mule scam)	Online munkaígéret, ami végül pénzmosásba visz.	Tréninggel, „szakmai mentorálással" nyerik el a bizalmat, majd rávesznek befektetésre vagy pénz mozgatására.

A pig butchering tehát nem csupán egy csalástípus, hanem komplex társadalmi, technológiai és pszichológiai kihívás, amely rendszerszintű választ kíván. A probléma nem kezelhető csupán technológiai oldalról – a valódi védelem a tudatosság növelésén, a kockázatkezelés javításán, a detekciós rendszerek fejlesztésén és a nemzetközi együttműködés elmélyítésén múlik.



Megtörtént esetek

A rendőrségi források szerint több hazai eset is megerősíti, hogy a „pig butchering" típusú csalások nemcsak külföldön, hanem Magyarországon is jelentős kockázatot jelentenek.

Egy férfi egy népszerű online társkereső alkalmazáson keresztül került kapcsolatba az elkövetővel. A kezdetben barátságos és bizalmat keltő kommunikáció során a csaló fokozatosan terelte a beszélgetést befektetési irányba, és egy – látszólag biztonságos – kriptovaluta-platformot ajánlott. Az áldozattól először csak kisebb összegű befizetést kértek, amely azonban a kapcsolat mélyülésével és az elköteleződés fokozódásával arányosan emelkedett. A férfi végül közel 14 millió forintot veszített el. *(Forrás: police.hu)*

Egy másik esetben egy nő az interneten keresztül ismerkedett meg egy magát jómódú külföldi üzletembernek kiadó személlyel, aki a hitelesség alátámasztása érdekében még egy hamisított netbanki felületet is megosztott vele, amelyen több millió dolláros egyenleg volt látható. A csaló azt állította, hogy egy olajipari baleset miatt büntetőeljárás alá került, és csak akkor szabadulhat, ha a kártérítési összeget kifizeti. Az áldozat először 70 millió forintot utalt át, majd további 50 millió forintot egy másik bankszámlára, így összesen 120 millió forintos kárt szenvedett el. *(Forrás: police.hu)*

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025