Telefonos csalások

Bevezető*

A magántulajdon megjelenésétől kezdve a társadalom tagjai között mindig akadt olyan, aki a másik félrevezetésével, megtévesztésével, annak értékeit, vagyontárgyait megpróbálta eltulajdonítani, kicsalni. Ennek egyik módja a lopás, amikor az áldozat testi épsége megmarad, vagy a rablás, amikor vele szemben erőszakot követnek el. Mindkét esetben az a közös, hogy az elkövető nem akarja magát másnak kiadni, nem próbál megtéveszteni senkit.

A csalás azonban abban más a fentiektől, hogy ebben az esetben az elkövető az áldozatát megkísérli félrevezetni és ilyen módon igyekszik rávenni, hogy az önként adja át tulajdonát. Ennek véghezviteléhez azonban az áldozattal kommunikálni kell, úgy, hogy annak bizalmát elnyerje az elkövető.

Korábban elég volt mindössze magabiztosan hazudni, és ha ezt elég meggyőzően tette a csaló, akkor az áldozatát könnyűszerrel tudta befolyásolni. Minél nagyobb értéket akart az elkövető megszerezni, annál hihetőbben kellett tudni blöffölni, és annál grandiózusabb körítést kellett kitalálni a megtévesztéshez, hogy az áldozat fejében egy komplexebb és ezáltal meggyőzőbb kép alakuljon ki az elkövető hitelességét tekintve.

A csalásoknak rengeteg formája van, de most azzal a fajtájával szeretnék kicsit foglalkozni, amelyben a tettesnek megvan az az előnye, hogy az áldozata csak a hangját hallja, de képtelen azonosítani, hogy ki kommunikál vele.

Telefonos csalások

A telefonos csalások alapvető eleme az anonimitás. A csaló bárkinek kiadhatja magát, egy jóhiszemű emberben pedig fel sem merül, hogy éppen át akarják verni.

Mivel manapság sok esetben kommunikál velünk telefonon valamelyik szolgáltatónk, ezért gyakran ezek egyik munkatársának adják ki magukat az elkövetők. Ez önmagában azonban kevés lenne, mivel itt is fontos a hihető sztori a csalás véghezviteléhez, illetve fenn kell tartani az áldozat figyelmét. Ha a csaló valamilyen marketing szöveggel hívja fel a kiválasztott embert, az vélhetően hamar érdektelenné válik a számára, mivel egy átlagos ügyfél ezerszám kap hasonló ajánlatokat. Ráadásul itt a kendőzetlen rábeszélésről van szó, amit már joggal érezhet valaki kellemetlennek, tolakodónak.

Leghatásosabb, ha valamilyen vélt veszélyre hívja fel az elkövető az áldozata figyelmét, aki azt érezheti, hogy ha most nem fogadja el a telefonos munkatárs segítségét, akkor abból sokkal nagyobb baja történhet később. Ilyen eset például, amikor a csaló azt mondja, hogy az áldozat adatai eltűntek a rendszerből, ezért a hívás során azonosítania kell magát. Az egyik módszer, hogy megad egy telefonszámot, amire egy „kódot” tartalmazó SMS-t kell elküldenie az ügyfélnek, ezalapján kerülne újra aktiválásra az ügyfél a szolgáltatónál. A valóságban azonban az történik, hogy a csaló telefonjának egyenlegét tölti fel a hívott fél a megadott, általában 15.000 forint összegben. Azért csak ennyivel, mert ez a maximális összeg az egyenlegfeltöltés esetén.

Hasonló, de talán kevésbé szofisztikált módja a csalásnak, amikor telefonon keresztül kártya adatokat kérnek az ügyféltől. Ebben az esetben is elhangzik a csaló részéről valamilyen álinformáció, például, hogy adathalászat történt a banki rendszerben, ezért most minden ügyfelet telefonon próbálnak meg azonosítani, vagy azt mondják hogy gyanús tranzakciókra lettek figyelmesek az ügyfél számláját illetően, mert egy illetéktelen személy megpróbált egy jelentősebb összeget átutalni valamilyen

*Cikkünkben a fogalmakat elsősorban köznapi, nem pedig jogi értelmükben használjuk.

számlaszámra, és ezért most azonosítaniuk kell a tulajdonost. Igencsak elterjedt a köztudatban az a hivatalos tájékoztatás, hogy soha nem kér tőlünk kártyaadatot a számlavezető bankunk. A csaló ezért úgy igyekszik hitelesíteni az azonosítási folyamatot, hogy megpróbálja elhitetni az áldozattal, hogy az adatait egy gép rögzíti, amit egy sípszó után kell bemondani és ő azt nem fogja hallani.

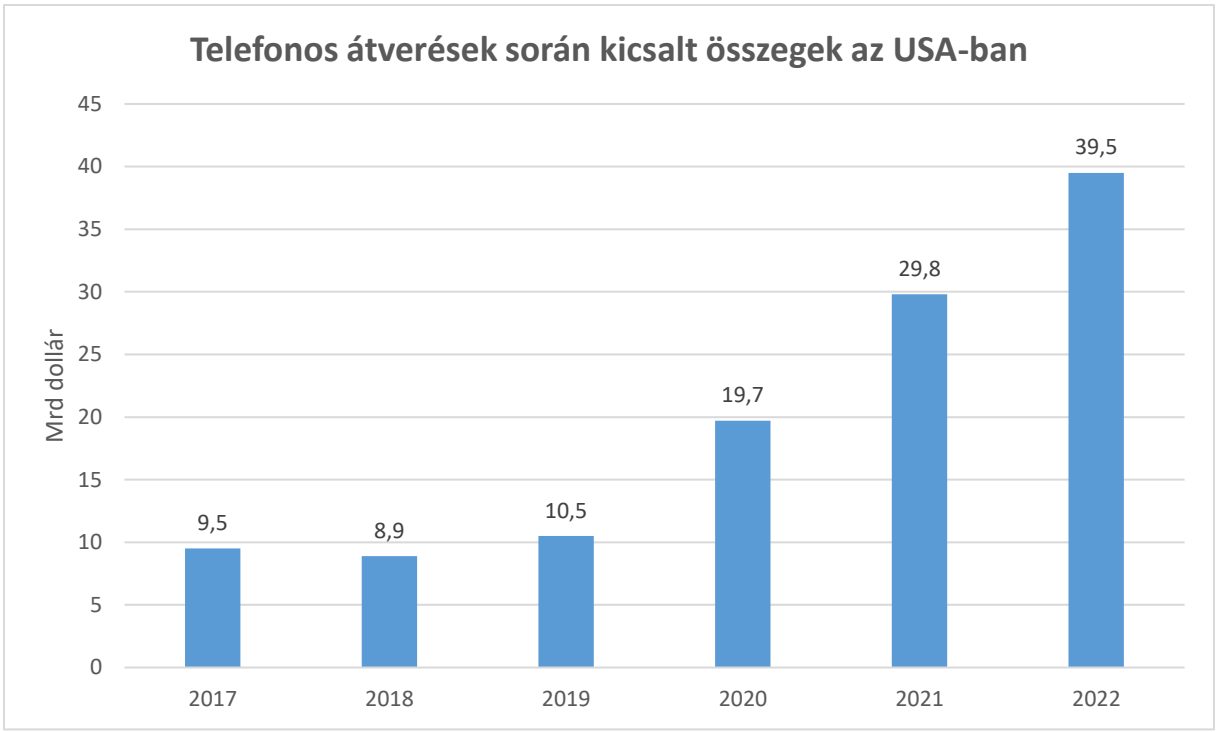
Banki ügyintézőnek kiadva magát azelkövető akár anélkül is meg tud szerezni bizalmas adatokat, hogy ezt különösképpen számításba venné az áldozat. Ilyen típusú csalás, amikor a tettes szintén valamilyen gyanús tranzakcióra, adathalászatra vagy kibertámadásra hivatkozva arra kér valakit, hogy töltsön le egy vírusírtó programot, majd az applikációban megjelenő adatokat bediktáltatja az áldozattal, hogy a vírust hatástalanítani tudja. A valóságban azonban egy olyan távoli hozzáférést biztosító kémprogramot telepít a kiszemelt telefonra, amivel hozzá tud férni a telefonon tárolt adatokhoz.

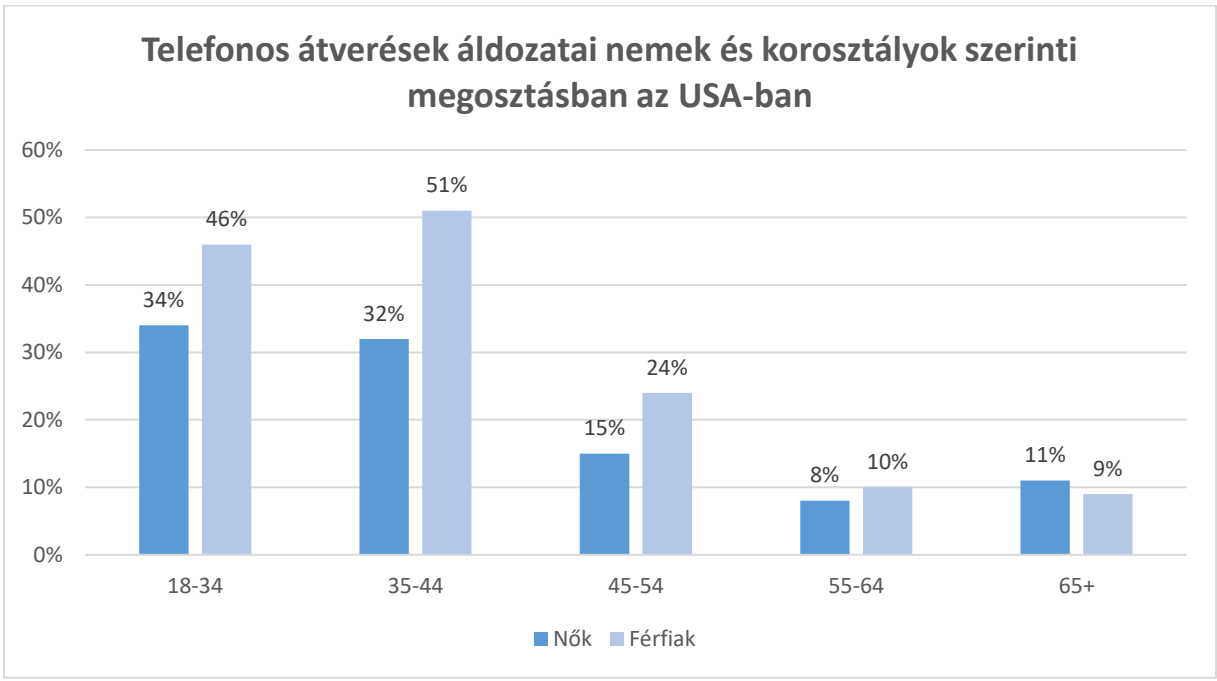
A fenti esetekben, amikor a szolgáltatónkként bemutatkozva keresnek bennünket telefonon, mindig érdemes figyelni, hogy az ügyintéző említi-e a nevünket, vagy tud-e bármilyen adattal szolgálni a szerződésünkkel kapcsolatban. Általában a csaló véletlenszerűen hív egy adott telefonszámot és nem tudja milyen adatok tartoznak hozzá, ezért ezt a helyzetet fenntartásokkal érdemes kezelni. Ha pedig tényleg adathalászat történt, és az adataink rossz kezekbe kerültek, ennek a helyzetnek is megvannak a hivatalos tájékoztatási formái, ami vélhetően nemegy telefonhívás lesz.

A csaló nem csak egy szolgáltató ügyintézőjének adhatja ki magát, hanem akár egy szerettünk ismerősének, arcátlanabb módon pedig akár a a hozzátartozónknak is. Ezekben az esetekben az elkövető az áldozatot felhívja, majd közli, hogy egyik családtagja (legtöbbször a gyermeke vagy unokája) nagy bajba keveredett és azonnal szüksége van készpénzre. Még kétség esetén is hamar felülírja a racionalitást annak a lehetősége, hogy egy szerettünk veszélyben lehet. A csaló ezért könnyen ráveszi az áldozatot, hogy szedjen össze minden nála lévő készpénzt, esetenként ékszereket is. Egy későbbi időpontban arcát eltakarva, vagy legalábbis a felismerést megnehezítő öltözékben (napszemüveg, baseball sapka, kapucnis felső) az áldozat címére megy, melyet telefonkönyvből vagy online tudakozóból tud meg legtöbbször. A police.hu által közölt információk szerint ez a fajta „unokázós” csalás még mindig nagy számban fordul elő az ország különböző pontjain.

A telefonos csalások nem csak magánszemélyeket, de nagy cégek munkavállalóit is célba veszik. Gazdasági társaságok esetében is egyre gyakoribbá válik, hogy egy felsővezető hangját használva és autoritására hivatkozva hívnak fel egy munkavállalót, hogy végezzen el egy tranzakciót, lehetőleg azonnal. Ebben az AI technológia is sokat tud segíteni az elkövetőknek, hiszen egy, a médiában gyakran szereplő vezető hangját könnyeben tudják ezekkel a programokkal szintetizálni. A dolgozó pedig még ha kételkedik is abban, hogy valóban azzal a személlyel beszél, akinek az kiadja magát, sokszor a félelem győz, amit a munkája esetleges elvesztése miatt érez, ezért inkább elvégzi a kért műveletet.

Néhány statisztikai adat az Egyesült Állomokból érdekes lehet. A 2022-es évben a telefonos csalások során kicsalt pénzek összege nagyságrendileg 39,5 milliárd dollár volt, ami jelentős növekedés a 2021-es 29,8 millió dollárhoz képest. Összesen 68,4 millió amerikai esett áldozatul az elmúlt évben. Ez azt jelenti, hogy átlagosan 577 dollárt csaltak ki egy-egy áldozattól, akik közül 55% férfi. A közhiedelemmel ellentétben a 18-44 év közötti korosztály fogékonyabb az ilyen típusú csalásokra. Az elkövetők legtöbbször az következő cégek nevében telefonálnak: Amazon, McAfee (Trellix), PayPal, Norton, Geek Squad.



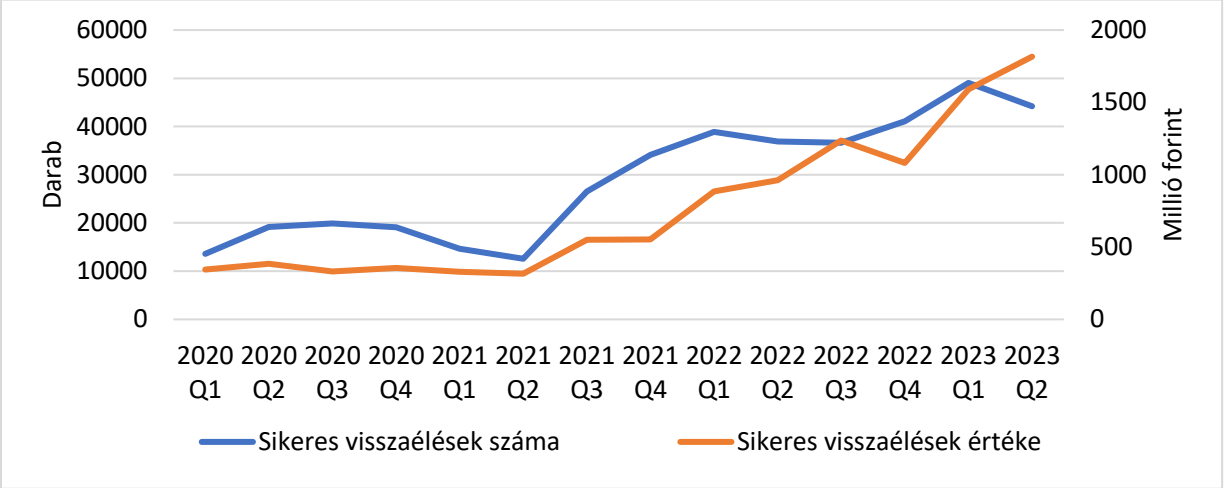


Forrás: Truecaller Insights/Harris Poll

Világviszonylatban aggodalmat keltőek a statisztikák:

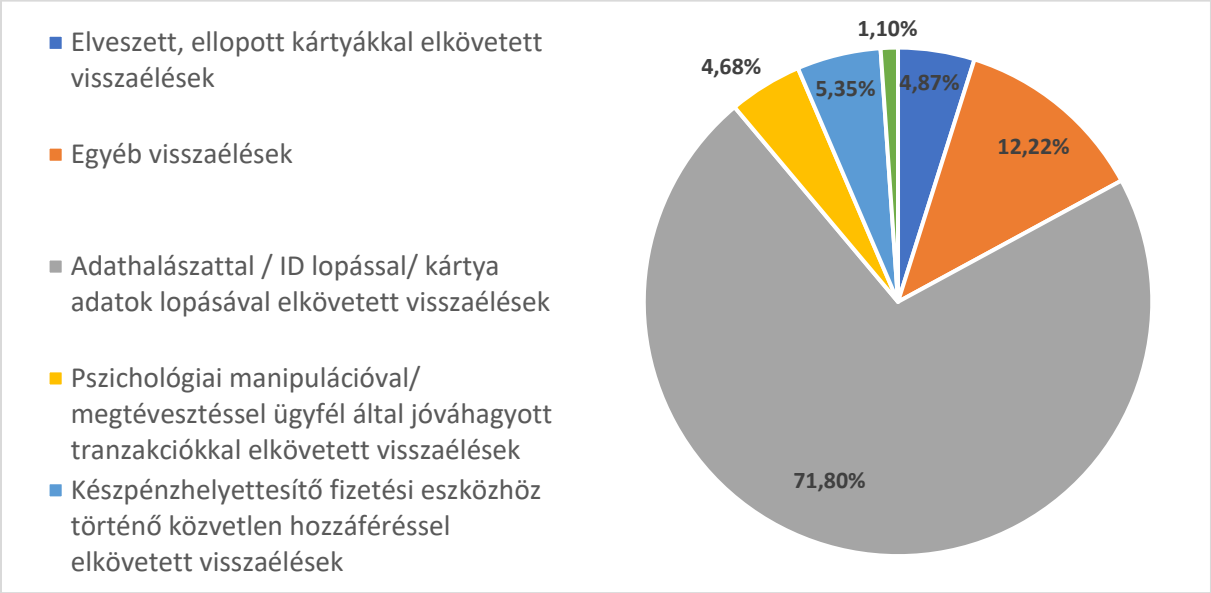
- A kibertámadások 98%-ában játszik szerepet a social engineering, vagyis a pszichológiai befolyásolás, mert majdnem minden esetben valamilyen manipulálás során kerülnek rossz kezekbe az adatok.
- Egy átlagos szervezet évente több mint 700 kibertámadásnak van kitéve.
- A social engineering átlagosan 130.000 dollár veszteséget okoz egy cégnek.

Magyar viszonylatban kevés a kifejezetten telefonos csalásokra vonatkozó adat. A Magyar Nemzeti Bank statisztikája szerint az elmúlt félévben (2023 januárjától júniusig) a kártyás visszaélések során kicsalt pénzek összege elérte a 1,8 millárd forintot, a csalások száma pedig meghaladta a 44 ezret. Az albbi ábrán látható, hogy az elektronikus fizetés folyamatos terjedésével a visszaélések száma szinte folyamatosan emelkedett.



Forrás: MNB

A visszaélési módszerek tekintetében az adathalászattal és az ehhez módszertanilag közel álló pszichológiai manipulációval elkövetett visszaélések aránya a legmagasabb itthon.



Forrás: MNB

A cégek csupán 56%-a biztosít kiberbiztonsági tréninget a dolgozóinak, pedig a szervezetek 86%-ában kattint rá legalább egy ember egy adathalász linkre. Az egyéb csaló módszerekkel együtt pedig ez a százalék még magasabb. Külön kockázatot jelent az AI technológia berobbanása, ami vélhetően a csalástípusok spektrumát is növelni fogja.

Összegzés

Cégek esetében a legfontosabb a munkavállalók és akár az ügyfelek tudatosságának folyamatos növelése, ezzel együtt az új csaló módszerek és a védekezési stratégiák megismerése és ismertetése. Ennek jó módszere lehet, ha szimulált támadásokkal hívják fel a dolgozók, valamint tájékoztató anyagokkal az ügyfelek figyelmét a veszélyekre. Belső ellenőrként, kockázatelemzésünk során érdemes végiggondolni, hogy vállalatunk munkavállalói és ügyfelei, partnerei hogyan és milyen mértékben lehetnek kitéve a telefonos támadások kockázatának, megfelelő védelmet nyújt-e a vállalati keretrendszer a telefonos csalások ellen. Ha arra jutunk, hogy nem, akkor érdemes – legalább néhány egyszerű, preventív – kontrol implementálásra javaslatot tenni.

Források:

telefonos átverések - YouTube

Ezek a leggyorsabban terjedő telefonos csalások Magyarországon – fotókkal (vg.hu)

Vigyázat, pénzmosásba keverhetik a banki csalók | 24.hu

Mutatjuk a telefonos csalók legújabb trükkjét – És azt is, hogyan védekezz ellene! | nlc

Egy bankos átverés története: ezekre vigyázz – Kiszámoló – egy blog a pénzügyekről (kiszamolo.hu)

Figyelem! Az unokázós csalók újra próbálkoznak! | A Magyar Rendőrség hivatalos honlapja (police.hu)

Vishing: hamis banki hívások (mnb.hu)

https://purplesec.us/resources/cyber-security-statistics/

https://www.zdnet.com/article/average-organization-targeted-by-over-700-social-engineering-attacks-each-year-report/

How phone scammers tricked Americans out of tens of billions of dollars in 2022 (cnbc.com)

35+ Phone Spam Statistics and Facts for 2017 - 2022 (comparitech.com)

Truecaller Insights 2022 U.S. Spam & Scam Report - Truecaller Blog

https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses

https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses

Milliárdokat lapátolnak le a magyarok bankszámláiról, gyorsan hízik a probléma - Portfolio.hu

Az MNB kezdeményezése a kiberbiztonságért | KiberPajzs

Többszörösére ugrott az internetes banki csalások száma, milliárdok úsznak el | Bank360

Az MNB ajánlással segíti a piaci szereplőket az adathalászat elleni harcban