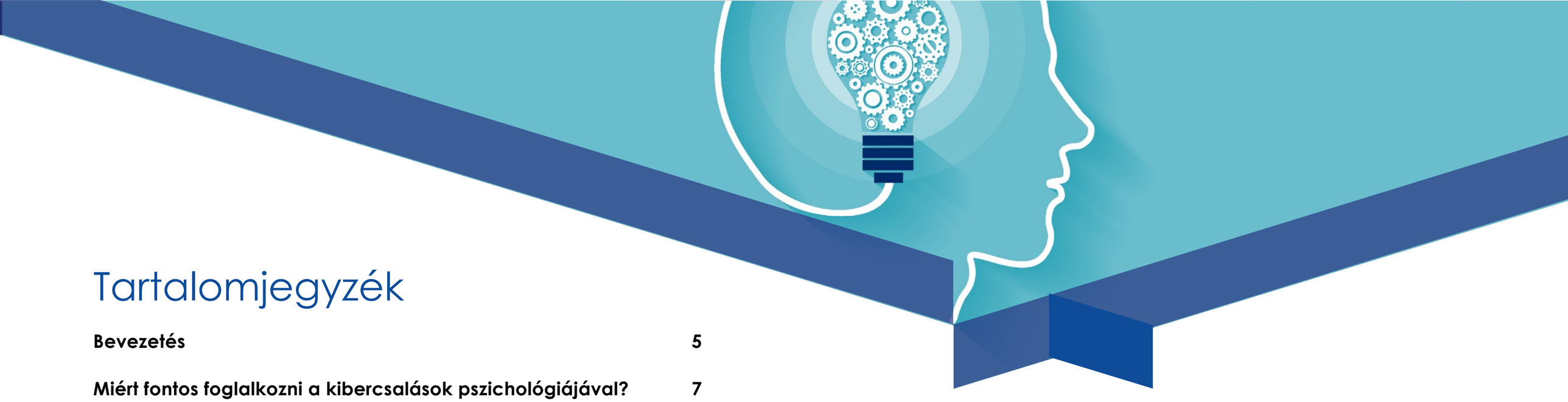
CTI Jelentés

A kibercsalások pszichológiája

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET



Tartalomjegyzék

Bevezetés **5**

Miért fontos foglalkozni a kibercsalások pszichológiájával? **7**

Főbb típusai **11**

- Pretexting 11
- Baiting 11
- Phishing (Adathalászat) 12
- Spear phishing (célzott adathalászat) 12
- Tailgating (Lopott belépés) 12
- Vishing (Hangalapú adathalászat) 13
- Smishing (SMS-alapú adathalászat) 13
- Impersonation (Személyazonosság-lopás) 13
- Romantikus csalás 14

A manipuláció eszközei **15**

- Sürgetés 15
- Félelem 15
- Autoritás 17
- Kapzsiság 17
- Bizalomépítés 18
- Pop-up hirdetések és hamis riasztások 20
- A “benne tartás” 21

Az áldozatok pszichológiája **22**

- Kinek a legnagyobb az esélye arra, hogy áldozattá válik? 22
- Az áldozattá válás utáni pszichológiai hatások 22

Megelőzés és védekezés **25**

- Tudatosság és oktatás 26
- Technológiai védekezés 27
- Jelszókezelés 27
- Óvatosság az információmegosztásban 28
- Hivatkozások és mellékletek ellenőrzése 29
- Vállalati felelősség 30
- Gyanakvás és figyelmesség 31
- Vészhelyzeti terv kidolgozása 32
- Hogyan lehet segíteni az áldozatoknak? 32

A jövő kihívásai **33**

- Natural Language Processing (NLP) 33
- Deepfake képgenerálás 34
- Voice Synthesis 35
- Machine Learning (ML) 36
- Érzelmi manipuláció 36
- Védekezés 37

Valós esettnulmányok **38**

- Target-adathalászat (2013) 38
- Twitter hack (2020) 39
- Sony Pictures hack (2014) 40
- Kevin Mitnick (1979) 41
- Deep Voice (2019) 42
- Banki csalás telefonon (2024) 43
- AnyDesk (2024) 43
- A híres zenész (2023) 44

Záró gondolatok **45**

Források **46**

Bevezetés

A kibercsalások olyan **szándékosan** megtévesztő cselekedetek, amelyek célja az áldozatok bizalmas adatainak megszerzése, anyagi eszközök eltulajdonítása vagy más személyes adat megszerzése online eszközök és platformok segítségével. Ezek magukban foglalhatják az **adathalászatot**, a **hamis weboldalak** létrehozását, illetve a **közösségi manipuláció** különböző formáit. Ezen csalások általában a **social engineering** (pszichológiai manipuláció) technikán alapulnak, amely során a csalók pszichológiai eszközökkel szereznek információt az áldozattól a viselkedésük és érzelmeik manipulációjával.

A gyakorlatban ez azt jelenti, hogy a támadó közvetlen kapcsolatba lép az áldozattal, és kihasználja annak segítőkészségét, félelmét vagy kapzsiságát. Például egy támadó egy technikai támogató munkatársnak adhatja ki magát, és így kérhet jelszót, bankszámla adatokat vagy más bizalmas információt.

„Mindenki azt mondja: "*Ó, ez velem soha nem történne meg*" - mondja Megan McCoy, a Kansasi Állami Egyetem személyes pénzügyi tervezéssel foglalkozó adjunktusa. „*De ez valójában egy jól ismert kognitív előítélet, amely sebezhetőbbé tesz minket*".

Van egy egyszerű és hatékony trükk, amelyre sok csaló támaszkodik: az **érzelmi manipuláció**. „*Félelemalapú taktikát használnak, hogy hassanak a primitív agyunkra, amely mindig készenlétben van*" - mondja Alex Melkumian, a Pénzügyi Pszichológiai Központ alapítója.

A Magyar Nemzeti Bank (MNB) adatai szerint 2023-ban **összesen 18 296 alkalommal** hajtottak végre sikeres banki csalást Magyarországon. Az ügyfeleknek ez **23 milliárd forintnál** is nagyobb kárt okozott. Ez a szám azt mutatja, hogy nagy mértékben nő a banki visszaélések száma, ugyanis **2022-ben még „csak" 9 milliárd** forintos kárt okoztak a csalók.

Az elektronikus pénzforgalomban bekövetkezett visszaélési kísérletek valamint sikeres visszaélések száma és értéke

Vonatkozási időszak	A negyedév során bekövetkezett sikertelen visszaélési kísérletek		A negyedév során bekövetkezett sikeres visszaélések	
	száma (darab)	értéke (Ft)	száma (darab)	értéke (Ft)
2023. I. név	3 048	1 285 214 559	4 169	3 278 332 201
2023. II. név	27 255	6 096 657 227	4 733	5 217 622 570
2023. III. név	18 280	6 815 792 739	5 679	9 208 925 701
2023. IV. név	13 937	4 810 507 390	3 737	5 795 701 130
2024. I. név	7 135	4 289 434 236	4 603	13 370 590 104
2024. II. név	5 878	4 543 256 206	4 509	5 979 383 302
2024. III. név	14 434	4 215 381 375	4 856	5 994 076 609

1. ábra
Az elektronikus pénzforgalomban bekövetkezett visszaélési kísérletek valamint sikeres visszaélések száma és értéke
Forrás: MNB Statisztika

Miért fontos foglalkozni a kibercsalások pszichológiájával?

A social engineering évtizedek óta állandó fenyegetés a kiberbiztonság területén. Kevin Mitnick, egy egykor híres hacker kijelentette, hogy könnyebb **manipulálni** az embereket, mint feltörni őket.

A kibercsalások elleni védekezés nem csupán technológiai kérdés; a támadások nagy része a pszichológiai manipuláció eszközeivel éri el célját. Az áldozatok viselkedésének és gondolkodásmódjának megértése kulcsfontosságú a hatékony megelőzés és a gyors reagálás érdekében. Az ilyen ismeretek hozzájárulhatnak a tudatosság növeléséhez, az oktatási programok kialakításához, valamint a személyes és vállalati szintű védekezés megerősítéséhez.

A social engineering csalások hatékonyan építenek az alapvető emberi érzelmekre és pszichológiai mechanizmusokra, különösen azokra, amelyek gyors és automatikus döntéshozatalt eredményeznek. Ezek a reakciók mélyen gyökereznek az evolúciós pszichológiában, hiszen a túlélés érdekében kialakult ösztönökre építenek.

A csalók gyakran alkalmaznak **sürgetést** vagy **fenyegetést**, amelyek a félelemalapú érzelmeket aktiválják, és a **"harcolj vagy menekülj"** reakciót idézik elő. Ezzel szemben más esetekben az emberek természetes hajlamát használják ki a bizalomra és a segítőkészségre. Ez a szociális kötődésekhez és a megerősítési torzításhoz kapcsolódik, mivel az emberek hajlamosak igazolni a már kialakított bizalmat, és nem kérdőjelezik meg a segítő szándékot.

A **kíváncsiság** és a **kapzsiság** szintén a gyakori kihasznált érzelmi reakciók közé tartozik, különösen a "túl szép, hogy igaz legyen" típusú nyereményjátékos csalások esetében. Ezek a jutalmazó rendszerre hatnak, dopamint szabadítva fel, ami motivációt és örömérzetet kelt. Ugyanakkor, ha valaki rájön, hogy átverték, gyakran szégyent és bűntudatot érez, amelyek gátolhatják abban, hogy segítséget kérjen. Ezek az önértékeléssel kapcsolatos érzelmek a **szociális énkép** sérüléséhez vezethetnek.

Végül, a csalók gyakran használják ki a társadalmi nyomást, hogy konformitásra ösztönözzenek (pl. "Mindenki más már megvette, ne maradj le!"). Ez a szociális összehasonlítás és a **csoportnyomás** pszichológiájához kapcsolódik, mivel az emberek hajlamosak követni a csoport normáit a társadalmi kapcsolatok fenntartása érdekében.

Összességében a social engineering csalások a mélyen gyökerező érzelmi és pszichológiai mechanizmusokat célozzák meg, amelyek gyors döntéshozatalra ösztönöznek, ezáltal hatékonyan manipulálva az áldozatokat.

A social engineering támadók gyakran arra törekszenek, hogy első benyomásra megbízhatónak, barátságosnak vagy hozzáértőnek tűnjenek. Ha az áldozat pozitív tulajdonságot társít a csalóhoz (például udvarias vagy segítőkész), akkor hajlamos lesz azt feltételezni, hogy más szempontból is megbízható, nem akar ártani, jogosan kér információt.

Ha a támadó vonzó megjelenést használ (például egy jól megválasztott profilképpel a közösségi médián vagy udvarias, megnyerő kommunikációval), akkor a célpont hajlamosabb lesz pozitív tulajdonságokat társítani hozzá, és kevésbé kritikus a kérésekkel vagy információkkal szemben.

A csalók olyan szakmák vagy társadalmi státuszok felhasználásával környékezik meg az áldozatot (például IT-támogató munkatárs vagy vezető beosztású személy), amelyhez az emberek természetüknél fogva megbízhatóságot és kompetenciát társítanak. A **holdudvar-hatás** miatt a célpont automatikusan feltételezi, hogy aki szakértőnek tűnik, az biztosan az is, így kevésbé lesz gyanakvó.

A **holdudvar-hatás** (angolul: halo effect) egy pszichológiai jelenség, amelyben egy személy vagy dolog egyetlen pozitív (vagy negatív) tulajdonsága alapján általánosan megítélést kap.
Más szóval, ha valakiről valamilyen jó tulajdonságot tudunk (például hogy vonzó, megbízható vagy gazdag), akkor hajlamosak vagyunk azt feltételezni, hogy más területeken is jól teljesít, még akkor is, ha erre nincs közvetlen bizonyíték. Ez a hatás gyakran megjelenik a marketingben is, amikor híresség̋eket használnak egy termék reklámozására. A híresség népszerűségét és vonzerejét átvisszük a termékre is, így annak megítélése is kedvezőbbé válik.

TUDTAD?

A fokozatos megközelítés segít abban, hogy az áldozat megszokja a kommunikációt a támadóval, és természetesnek érezze az információcserét. A támadó barátságosnak, segítőkésznek és megbízhatónak tűnhet, így az áldozat kevésbé lesz gyanakvó.

Az emberek hajlamosak következetesen viselkedni a korábbi döntéseikkel összhangban. Ha egyszer már segítettek a támadónak egy kisebb szívességgel, nagyobb valószínűséggel teljesítik a későbbi, nagyobb kéréseket is, hogy összhangban maradjanak a korábbi viselkedésükkel. A támadó először apró, ártatlannak tűnő információkat kér. Miután ezeket megkapja, a következő lépésben kicsivel több adatot kér, míg végül érzékeny információkat is megszerezhet.

Főbb típusai

01 PRETEXTING

Egy **kitalált történet** segítségével nyerik ki a csalók az információkat. Ennek során a támadó egy hamis előtörténetet (pretext-et) hoz létre annak érdekében, hogy elnyerje az áldozat bizalmát és megszerezzen olyan érzékeny információkat, mint például személyes vagy pénzügyi adatok, jelszavak vagy egyéb bizalmas információk. A támadó egy telefonhívás során egy banki alkalmazottnak adja ki magát, és azt állítja, hogy szüksége van bizonyos adatainkra ahhoz, hogy megerősítsen egy tranzakciót vagy megoldjon egy problémát. Az áldozat azt gondolja, hogy egy hivatalos személy keresi, és ennek megfelelően megadja az információkat.

02 BAITING

A támadók valamilyen **vonzó ajánlatot** használnak, például egy ingyenes szoftver letöltését, vagy ajándék fizikai adathordozót (pl. pendrive). Az áldozat önként tölti le a „nyereményét" vagy csatlakoztatja az ajándék vagy talált adathordozót, azonban valamilyen káros állománnyal fertőzi meg a saját eszközét, amely az elindítást követően a háttérben gyűjti az adatokat vagy valamilyen egyéb káros tevékenységet végez el.

03 PHISHING
(ADATHALÁSZAT)

Csalók **hamis e-maileket és weboldalakat** használnak, amelyek úgy néznek ki, mintha hivatalos szervezetektől származnának (pl. bankok, szolgáltatók). Célja jelszavak, bankkártyaadatok, vagy személyes információk megszerzése. Ezek általában nem személyre szabott, hanem tömeges támadások.

04 SPEAR PHISHING
(CÉLZOTT ADATHALÁSZAT)

A támadás sokkal inkább testreszabott, azaz az áldozatról gyűjtött **személyes információk felhasználásával** hoznak létre hitelesnek tűnő e-maileket. A spear phishing célzott és gyakran nagyobb értékű információk, például vállalati adatok vagy személyes pénzügyi információk megszerzésére irányul.

05 TAILGATING
(LOPOTT BELÉPÉS)

A támadó nem rendelkezik saját belépési jogosultsággal, de kihasználja a jogosult személy jóhiszeműségét vagy figyelmetlenségét. Egy illetéktelen személy **fizikailag követi** a jogosult személyt egy épületbe vagy akár szerverterembe, majd miközben az illető nyitja az ajtót, a támadó "megpróbál beosonni" mögötte. Az is előfordulhat, hogy egy támadó szándékosan kér segítséget egy jogosult személytől (*"Elfelejtettem a belépőkártyámat magammal hozni, be tudnál engedni?"*), hogy így elérje a belépést.

06 VISHING
(HANGALAPÚ ADATHALÁSZAT)

Telefonos csalások, amelyek során a csaló hivatalos szervezet munkatársának adja ki magát, és információkat kér. A **hívás gyakran olyan intézet nevében érkezik**, amelynél nincs szolgáltatása az áldozatnak. Amint ez kiderül, a csaló azonnal „intézkedik" és „átkapcsol" az érintett intézményhez. Banki ügyintézésnek álcázott csalás során arra is volt példa, hogy a kiadott adatokkal online személyi kölcsönt igényeltek.

07 SMISHING
(SMS-ALAPÚ ADATHALÁSZAT)

Hamis **SMS**-ek küldése, amelyek linkeket vagy utasításokat tartalmaznak, hogy az áldozat személyes adatokat adjon meg.

08 IMPERSONATION
(SZEMÉLYAZONOSSÁG-LOPÁS)

A támadó más személynek adja ki magát (pl. kolléga, barát, ügyfél), hogy bizalmas adatokat szerezzen vagy hozzáférést kapjon.

09 ROMANTIKUS CSALÁS

Érzelmi manipuláció vagy **romantikus kapcsolatok színlelése** érzékeny információk kicsikarása érdekében. Általában egy vonzó személy képét vagy szerepét használják arra, hogy az áldozatot megtévesszék, és így információkat, pénzt vagy más értékeket csaljanak ki tőle. A támadó kapcsolatba lép az áldozattal személyes üzeneteken vagy különböző chateken keresztül.

A beszélgetések eleinte ártatlanok, flörtölés vagy barátságos ismerkedés formájában zajlanak. Ahogy a kapcsolat elmélyül, a támadó egyre inkább személyes problémákról beszélhet, melynek során segítséget vagy pénzt kér. Azzal manipulálják az áldozatot, hogy meggyőzik őt a kapcsolatuk őszinteségéről, és hogy a pénz segíthet a szerelmük kiteljesülésében.

A manipuláció eszközei

SÜRGETÉS

A kiberbűnözők egyik leggyakoribb taktikája, hogy az áldozatban sürgősség érzetét keltik, ezzel **csökkentve a logikus gondolkodás képességét** és az információk kritikus értékelését.

2. ábra
Sürgető hangvételű üzenet

FÉLELEM

Az emberek hajlamosak gyors döntéseket hozni, amikor veszélyt éreznek. A csalók ezt használják ki olyan üzenetekkel, amelyek sürgetést és **fenyegetést tartalmaznak**, ezzel keltve félelmet az áldozatban.

RENDŐRSÉG POLICE

BÍRÓSÁGI IDÉZÉS
BÍRÓSÁGI VIZSGÁLAT ESETÉN
(AZ ELJÁRÁSI KÓDEX 45-1. CIKKE)

RENDŐRSÉG POLICE

A nevem Balogh János rendőr altábornagy, Magyarország rendőrfőkapitánya és országos rendőrfőkapitánya, az Europol Irodával együttműködve (az Igazságügyi Minisztérium megbízásából) az európai rendőrséggel (Interpol) együttműködve a büntetőeljárási törvénykönyv 45-1. és 316-7. cikkei alapján röviddel egy kibertámadás észlelése után, konkrétan a gyermekpornográfia és a kiberpornográfia weboldalával kapcsolatban, azért keressük meg Önt, hogy tájékoztassuk, hogy Ön ellen alkalmazandó bírósági eljárás folyik:

- **Pornográfiai weboldalak**
- **Gyermekpornográfia**
- **Kiberpornográfia**
- **Pedofília**
- **Exhibicionizmus**

Az igazságügyi eljárásról szóló törvény 47-3. szakaszának megfelelően válaszolnia kell, hogy az elkövetett bűncselekmény súlyának megfelelő szankciót állapítsunk meg. Ezt 48 órán belül kell megtenni.

Ezt követően kötelesek leszünk továbbítani a jelentést az ügyésznek és a kiberbűnözési szakértőnek a letartóztatási parancs kiadása érdekében.

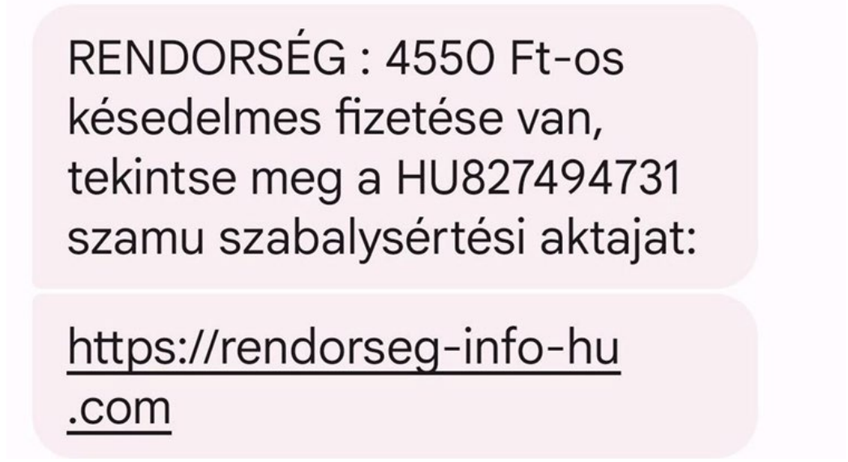
Ön felkerül a szexuális bűncselekmények elkövetőinek listájára, és a képe megjelenik a közösségi hálózatokon és a médiában, így a rokonai és a családja tudni fogja, hogy mit csinál az eszközön.

Balogh János altábornagy,
rendőrfőkapitány
www.police.hu

3. ábra
Félelmet keltő üzenet

AUTORITÁS

A kiberbűnözők gyakran hivatkoznak **hatóságokra** vagy tekintélyes szervezetekre (például bankokra, közüzemi vállalatokra, a rendőrségre vagy ismert cégekre), hogy meggyőzzék az áldozatot az üzenetük **hitelességé**ről. Az autoritás elfogadása egy természetes emberi hajlam, amely megkönnyíti a csalók dolgát.



RENDORSÉG : 4550 Ft-os késedelmes fizetése van, tekintse meg a HU827494731 szamu szabalysértési aktajat:

https://rendorseg-info-hu.com

4. ábra
A rendőrség nevével visszaélő üzenet

KAPZSISÁG

Az emberek vonzódnak a "gyors meggazdagodás" vagy az "egyedülálló lehetőségek" ígéretéhez. Az ilyen ajánlatok, például hamis lottónyeremények vagy befektetési lehetőségek sokakat csapdába ejthetnek.

Holnap 18 500 ft-t veszel fel, 3 nap múlva 70 000 ft-t, 7 nap múlva pedig akár 1 milliót –ezt az eredményt 72 ezer magyar már megerősítette

Üdv!

Graham Le Roux professzornak hívnak, és mindjárt bemutatok neked egy egyszerű módszert arra, hogy igen nagy pénzt kereshess. Megtanulod, hogyan tehetsz szert 20-30 ezer ft-ra egy nap alatt, és hogyan szerezhetsz 100 000 ft-t készpénzben 7 napon belül. Pár másodpercen belül **elmesélem ennek a módszernek néhány részletét**, amellyel - még ha csak fele annyi pénzre is teszel szert mint én, igazán nagy összeget zsebelhetsz be. Mindezt:

5. ábra
Gyors meggazdagodást ígérő üzenet

BIZALOMÉPÍTÉS

Gyakran használják a bizalomépítést, hogy az áldozat hajlandó legyen megosztani velük bizalmas információkat. Ez a módszer különösen hatékony célzott adathalászat (spear phishing) vagy közösségi platformon elkövetett támadások esetén. Néhány technika:

- **Személyre szabott kommunikáció**: Az áldozat korábban megosztott információi alapján hitelesnek tűnő üzeneteket küldenek. Például, ha tudják, hogy az áldozat nemrég vásárolt egy terméket, egy "ügyfélszolgálatos" felveheti vele a kapcsolatot azzal az ürüggyel, hogy a rendelésével gond van.

- **Megbízhatónak tűnő szereplők**: A támadók olyan pozíciókat vesznek fel, amelyek természetesen bizalmat keltenek, mint például banki ügyintéző, IT-támogatási munkatárs vagy rendőr.

- **Hosszú távú manipuláció**: Néhány esetben a támadók akár hetekig vagy hónapokig építik a kapcsolatot, például egy közösségi média barátságon keresztül, hogy elnyerjék az áldozat bizalmát. Ilyenek lehetnek a partner kereső oldalakon elkövetett csalások.

- **Szívességi normák kihasználása**: Az emberek hajlamosak viszonozni a szívességet, még akkor is, ha az nem valós. Például egy "ingyenes ajándék" vagy "egyedi ajánlat" felajánlása az áldozatot arra késztetheti, hogy cserébe adatokat szolgáltasson.

- **Közösségi értékelés**: Az emberek gyakran követik mások példáját, különösen akkor, ha bizonytalanok. A csalók hamis visszajelzéseket vagy értékeléseket használhatnak, hogy meggyőzzék az áldozatot az ajánlatuk megbízhatóságáról.

POP-UP HIRDETÉSEK ÉS HAMIS RIASZTÁSOK

A kiberbűnözők gyakran használnak felugró ablakokat, hogy megtévesszék az áldozatot és rávegyék, hogy kártékony szoftvert töltsön le vagy személyes adatokat adjon meg. A felugró ablakok azt állítják, hogy az áldozat eszközét "vírus fertőzte meg", és **azonnal** le kell töltenie egy "biztonsági szoftvert" (ami valójában malware). Egy másik metódusban a pop-up azt állítja, hogy az áldozat valamilyen **díjat nyert**, és az adatai megadásával vagy egy alkalmazás letöltésével igényelheti a nyereményt. A hamis figyelmeztetések olyan üzeneteket is tartalmazhatnak, mint például: *"Bejelentkezést észleltünk egy új eszközről. Kattintson ide a fiókja ellenőrzéséhez."* Ezek a felugró ablakok gyakran **pontosan úgy néznek ki**, mint egy jól ismert antivírus szoftver vagy operációs rendszer értesítése.

6. ábra
Néhány csaló pop-up értesítés
Forrás: Malwarebytes

A "BENNE TARTÁS"

Ez egy olyan manipulációs technika, amely során a csaló célja az, hogy az áldozata **minél hosszabb ideig** maradjon aktív a csaló által irányított rendszerben, hogy az idő múlásával egyre nagyobb összegeket tudjon kicsalni belőle.

A csaló először egy **vonzó ajánlattal** csábítja el az áldozatát, ígéretes hozamokkal, kedvező ajánlatokkal és kezdeti nyereményekkel. Ahogy az áldozat többet és többet fektet be, a csaló igyekszik fenntartani a hitet a rendszer működésében. Ennek során hamis statisztikákat, győzelmi értesítéseket küld, vagy azzal hitegeti az áldozatot, hogy a következő lépés már biztos nyereséget hoz. Ezzel próbálja **fenntartani a felhasználó érdeklődését és bizalmát**.

Ha az áldozat gyanakodni kezd, a csaló gyorsan reagál. Megnyugtató magyarázatokat ad, új bizonyítékokat kreál, vagy érzelmi zsarolást alkalmaz. Az áldozat egyre inkább a csaló által nyújtott „jutalmakra" (pl. elismerés, hamis remény, szerelmi ígéretek, anyagi lehetőségek) támaszkodik, és már **nem tud vagy nem mer kiszállni**. Az áldozat végül rájön, hogy valójában sosem volt valódi nyereménye, és az egész rendszer csak egy trükk volt, hogy elcsalják a pénzét.

Az áldozatok pszichológiája

Kinek a legnagyobb az esélye arra, hogy áldozattá válik?

A **bizalom**, a **naivitás** és a **tapasztalatlanság** gyakran támogatja a manipuláció sikerét. Azok, akik hajlamosak az emocionálisabb döntésekre, könnyebben válnak áldozattá. **Szorongás** vagy **stressz** alatt álló személyek gyakran kevésbé figyelmesek. Az **idősebb generációk** gyakran nem rendelkeznek megfelelő szintű ismeretekkel, ezért nem mindig tudják felismerni a gyanús linkeket, átveréseket, vagy a hamis e-maileket. Sokszor nem tudják, hogyan kell megvédeniük személyes adataikat, vagy hogyan tehetik biztonságossá a digitális fiókjaikat.

Az olyan **tinik** és **fiatal felnőttek** is eshetnek csapdába, akik túlzottan megbíznak a technológiai platformokban, és kevésbé figyelnek a potenciális veszélyekre. A csalók kihasználhatják a fiatalok **naivitását** és hamis **trendi** alkalmazásokat, linkeket küldhetnek.

Az áldozattá válás utáni pszichológiai hatások

Amikor az áldozat ráébred, hogy social engineering csalás áldozata lett, gyakran jelentős utólagos **érzelmi sérüléseket** él át. Ezek az érzelmi reakciók összetettek lehetnek, és hosszú távú pszichológiai hatásokat is okozhatnak.

Szégyen és bűntudat

Az áldozatok gyakran saját **magukat hibáztatják**, ami megnehezítheti a helyzet feldolgozását és a segítségkérést, hiszen úgy érezhetik, hogy naivitásuk vagy figyelmetlenségük vezetett a csalás sikeréhez. Ez a belső küzdelem fokozhatja az elszigeteltséget és a bizalmatlanságot, különösen, ha attól tartanak, hogy **mások elítélik** vagy **kigúnyolják** őket a történtek miatt. Az ilyen érzelmi teher akadályozhatja őket abban, hogy jelentést tegyenek a hatóságoknál, vagy megosszák tapasztalataikat, pedig ezek a lépések kulcsfontosságúak lehetnek a csalók elleni fellépésben és a további károkozások megelőzésében.

Az áldozatok úgy érzik, hogy hibásak a történtekért, mert nem voltak elég elővigyázatosak, vagy nem követték a biztonsági protokollokat. A bűntudat különösen erős lehet, ha a csalás következményeként mások is károsultak, például munkahelyi adatlopás esetén. Ez lelki teherhez és önvádhoz vezethet.

Stressz és PTSD

Az élmény utáni trauma gyakran tartósan befolyásolja az áldozatok mentális egészségét, akik **állandó aggodalommal** élhetnek az miatt, hogy egy újabb csalás áldozatává válnak. Ez az állandó szorongás megnyilvánulhat **alvászavarokban**, **koncentrációs nehézségekben** vagy **túlzott éberségben**, amely kimerítővé teheti a mindennapi életüket.

Az ismétlődő emlékek vagy rémálmok formájában megjelenő trauma (PTSD) miatt egyes áldozatok **kerülik** azokat a tevékenységeket, helyzeteket vagy technológiai eszközöket, amelyek a csalásra emlékeztethetik őket. Ez a fokozott bizalmatlanság akár a személyes és szakmai kapcsolataikat is negatívan befolyásolhatja, tovább erősítve az elszigeteltség érzését.

Ha a stressz és a PTSD feldolgozatlan marad, hosszú távú mentális és fizikai egészségkárosodást okozhat, ezért kiemelten fontos a probléma felismerése és a szakmai segítség igénybevétele.

Bizalomvesztés

Az áldozatok elveszítik bizalmukat nemcsak az online rendszerekben, hanem sokszor **embertársaikban is**, különösen, ha a csalás személyes manipuláción alapult. Ez a bizalomvesztés súlyosan érintheti az áldozatok kapcsolatait, hiszen nehezebben nyílnak meg mások előtt, és állandóan **gyanakodva** vizsgálják az emberek szándékait. Az online vásárlások, banki tranzakciók vagy akár az egyszerű e-mailek kezelése is **stresszforrássá** válhat, mivel az áldozatok attól félnek, hogy ismét megtévesztik őket. Ez a fajta bizalmatlanság hosszú távon megnehezítheti a modern technológiák használatát és a társadalmi kapcsolatok ápolását, ami **elszigetelődéshez és akár depresszióhoz is** vezethet. Az áldozatok sokszor úgy érezhetik, hogy nem számíthatnak másokra, ami alááshatja a közösségi támogató hálózatok hatékonyságát, pedig ezek elengedhetetlenek lennének a trauma feldolgozásában és a bizalom újraépítésében.

Szétesett önkép és önbizalomvesztés

A social engineering csalás áldozatai gyakran megkérdőjelezik a saját **ítélőképességüket**, **intelligenciájukat** vagy **szakmai hozzáértésüket**. Ez hosszú távú **önbizalomhiányhoz vezethet**, amely kihathat a karrierre, a kapcsolatokra és az önértékelésre is. Ha az áldozat jelentős anyagi veszteséget szenvedett el, vagy ha a csalás komoly hatással volt az életére (például személyazonosság-lopás), depressziós tünetek is kialakulhatnak. A depresszió hosszú távú mentális egészségügyi problémákhoz vezethet, és kezelés nélkül súlyosbodhat.

Megelőzés és védekezés

Az adathalászat megelőzésére fontos a **tájékozottság** és az **elővigyázatosság**. Az ismert csalástípusok mellett bármikor újak jelenhetnek meg. Tájékozódjunk a szolgáltatók honlapján, valamint a csalások visszaszorítása érdekében létrehozott KiberPajzs honlapon. Ha mégis megtörtént a baj, haladéktalanul vegyük fel **bankunkkal** a kapcsolatot és tegyünk **rendőrségi** feljelentést. A rendőrség foglalhatja le azt a bankszámlát, amire a pénzünket átutalták, a bankunknak nincs ilyen jogosítványa.

Tudatosság és oktatás

- A kibercsalások kiszűrése érdekében elengedhetetlen, hogy **megértsük** ezen csalások természetét és ismertetőjeleit, például a gyanús e-maileket, a sürgető üzeneteket és a túl szépnek tűnő ajánlatokat.
- Amennyiben lehetőségünk van rá, szorgalmazzuk **oktatási kampányok** indítását az iskolákban, munkahelyeken és közösségi fórumokon.
- Egy vállalat életében elengedhetetlen a rendszeres **tréningek** szervezése, ahol valós példákon keresztül mutathatjuk be a téma fontosságát és komolyságát.
- A **támogató környezet** megteremtése elengedhetetlen ahhoz, hogy az áldozatok bizalommal tudjanak felénk fordulni. Így megoszthatjuk egymással a tapasztalatokat, másokat figyelmeztethetünk a veszélyekre és új, specifikus megelőzési módszereket hozhatunk létre az esetlegesen újonnan megjelent trendek megismerésével.
- Az érzelmi manipuláció elleni védekezés érdekében fontos a **kritikus gondolkodás** erősítése, amely segít az embereknek megkérdőjelezni a kapott információk hitelességét.

Technológia és védekezés

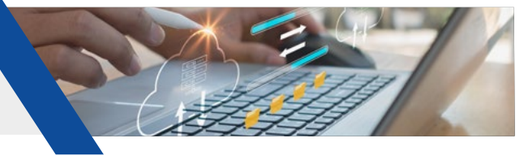
- Ajánlott vírusirtók és tűzfalak **telepítése** az eszközeinkre, amelyek segítenek kiszűrni a kártékony tartalmakat.
- Antiphishing-eszközök **alkalmazása** is javasolt, amelyek figyelmeztetnek a gyanús weboldalakra vagy linkekre.

Jelszókezelés

- Javasoljuk a **hosszú jelmondatok** használatát, melyek egyszerűen megjegyezhetőek, és számos esetben biztonságosabbak mint a bonyolult, különleges karaktereket tartalmazó jelszavak.
- Célszerű eltérő szolgáltatásokhoz eltérő jelszavak **alkalmazása**.
- Amennyiben van rá lehetőségünk, **engedélyezzük a** kétfaktoros azonosítást (2FA), amely jelentősen megnöveli a biztonságot!

Javasoljuk jelszószéf alkalmazások használatát az adatok biztonságos tárolása érdekében. A témában készült podcastunk itt hallgatható meg, a témában írt jelentésünket pedig ide kattinva olvashatja el.

Óvatosság az információmegosztásban



- Lehetőleg senkivel se osszuk meg személyes vagy pénzügyi adatainkat!
- A közösségi médiában elérhető **személyes adatainkat** minimalizáljuk, ne teregessük ki az egész életünket! Ez olyan, mintha nyitva hagynánk a házunk bejárati ajtaját és bárki szabadon járhatna-kelhetne az életünkben.
- Amikor adatokat osztunk meg az online térben, fontos, hogy alaposan mérlegeljük: ki kéri, miért kéri és hogyan fogják azokat felhasználni. A **keresztkérdések** segítenek tisztázni a helyzetet, és biztosítani, hogy adataink biztonságban maradjanak. Ha bármilyen kétség merül fel, jobb, ha nem osztjuk meg az információkat.

Miért kérdezik tőlem?

Ha nem vagyunk biztosak abban, hogy miért van szükség az információra, kérdezzük meg az illetőt, miért van szükségük az adatra.

Megbízható forrás?

Bizonyosodjunk meg róla, hogy az információkérés egy olyan személytől származik, akiben megbízunk, és akinek valóban szüksége van az adatra.

Hogyan fogják felhasználni?

Kérdezzük meg, hogyan fogják használni az adatainkat! A válasznak egyértelműnek és konkrétnak kell lennie. Ha nem vagyunk biztosak a célokban, akkor ne osszuk meg az adatokat!

Van alternatíva?

Ha nem akarunk adatokat megosztani, kérdezzük meg, hogy van-e más módja annak, hogy ugyanazt a szolgáltatást vagy információt megkapjuk!

Hátrányos következmények?

Ha a kérés nem kötelező, érdemes érdeklődni, hogy milyen hatása van annak, ha nem osztjuk meg az adatokat. Ha nem muszáj, ne osszuk meg az adatainkat!

Hivatkozások és mellékletek ellenőrzése

- **Soha** ne kattintsunk gyanús linkekre vagy töltsünk le mellékleteket ismeretlen forrásból!
- Keressük meg magunktól és használjuk az **adott weboldal** hivatalos elérését a kapott linkek helyett.

Vállalati felelősség

- A vállalatoknak rendszeres képzéseket kell tartaniuk a kiberbiztonságról, úgymint **adathalászat** (phishing), **social engineering, jelszókezelés**. Ezeknek az oktatásoknak nemcsak az alapvető fenyegetésekről kell szólniuk, hanem arról is, hogyan lehet megelőzni őket.

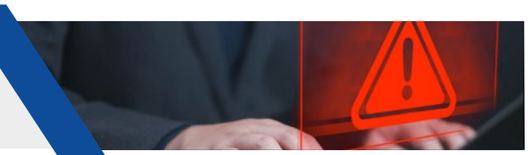
  Javasoljuk a **rendszeres kiberbiztonsági gyakorlatok**at, amelyek segíthetnek a munkatársaknak felismerni a gyanús jeleket a valós környezetben, mielőtt valódi kockázatot jelentene. Javasolt rendszeresen frissíteni a vállalati biztonsági irányelveket, és tudatosítaniuk kell a dolgozókban a kiberfenyegetések fontosságát. Ezek lehetnek belső kommunikációs kampányok, hírlevelek vagy plakátok a munkahelyeken.

- A vállalatoknak érdemes magasan képzett kiberbiztonsági szakembereket alkalmazniuk, akik folyamatosan figyelik a rendszereket, értékelik a kockázatokat, és javaslatokat tesznek a **legjobb védelmi intézkedések**re. Rendszeresen el kell végezni a belső biztonsági auditokat, hogy biztosítsák, hogy minden alkalmazott betartja a biztonsági irányelveket és szabályzatokat. Fontos a külső szakértők bevonása is a rendszeres auditok elvégzésére, hogy objektív és független szemmel értékeljék a vállalat biztonsági helyzetét. A belső szakemberek együttműködése a külső tanácsadókkal erősítheti a biztonságot.

- Az MFA elengedhetetlen minden fontos rendszerhez való **hozzáféréshez**, legyen szó e-mail fiókról, vállalati rendszerekről vagy banki alkalmazásokról. Ezzel a módszerrel az adatok védelme még akkor is biztosítható, ha valaki megszerzi a jelszavakat.

- A szoftverek, operációs rendszerek és alkalmazások naprakészen tartása **kulcsfontosságú** a biztonság megőrzésében. A biztonsági rések gyors lezárása segít megakadályozni, hogy támadók kihasználják azokat.

Gyanakvás és figyelmesség



- Ha bárki, indokolatlanul kér személyes, vagy pénzügyi adatot, kezeljük a megkeresést óvatosan! Ha nem vagyunk biztosak a kérés legitimitásában, inkább **ne adjunk ki információkat** telefonon vagy e-mailben!

- Ismeretlen forrásból származó megkeresések esetén mindig ellenőrizzük a hitelességet! Ha szükséges, mi magunk keressük fel az adott szervezetet és ellenőrizzük a megkeresés valódiságát!

Vészhelyzeti terv kidolgozása

Legyen kész forgatókönyvünk arra az esetre, ha kibertámadás áldozatává válnánk, például gyors bankszámlazárolás, szakértői segítség kérése, a bankintézet és rendőrség értesítése.

Hogyan lehet segíteni az áldozatoknak?

Hallgassuk meg ítélkezés nélkül, és biztosítsuk arról, hogy **nem ő a hibás**. Bátorítsuk arra, hogy beszéljen a családdal, barátokkal vagy támogató csoportokkal. Szükség esetén pszichológus vagy tanácsadó bevonása segíthet feldolgozni a traumát és helyreállítani az önbizalmat.

Léteznek szervezetek, amelyek segíthetnek az áldozat traumáját feldolgozni. Ezek a szervezetek a lelki segítségnyújtáson túl pénzügyi segélyben is részesíthetik a rászorulókat (pl.: Van segítség).

A jövő kihívásai

A social engineering már régóta kedvelt taktika a kiberbűnözők körében, mivel hatékonysága révén az **emberi sebezhetőséget** használja ki, nem pedig a technikai sebezhetőségeket. A **mesterséges intelligencia** integrálásával ezek a támadások egyre kifinomultabbá, személyre szabottabbá válnak és egyre nehezebb felderíteni őket. Számos MI technológia közvetlenül alkalmazható a social engineering támadások hatásának fokozásában.

Az olyan fejlett technológiák, mint a **Natural Language Processing (NLP)**, **deepfake képgenerálás**, **voice synthesis**, és a **machine learning** új lehetőségeket teremtenek a csalók számára, miközben a védekezést is egyre nagyobb kihívássá teszik.

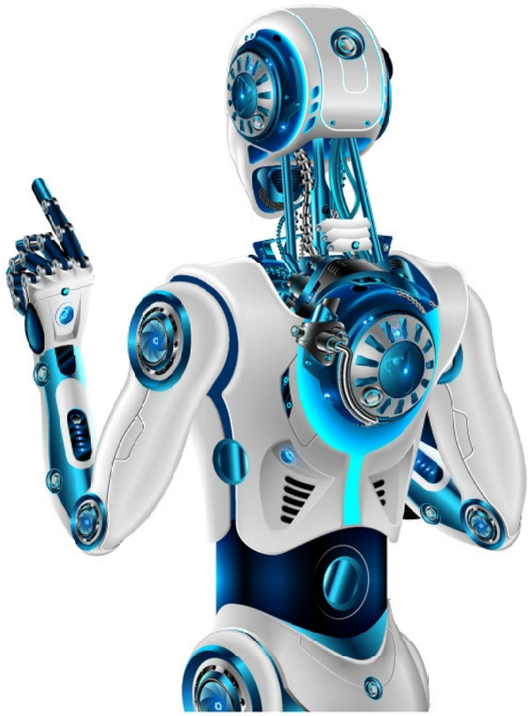
Natural Language Processing: a valósághű interakciók

A modern Natural Language Processing (NLP) rendszerek képesek valósághű és **hibátlan kommunikációra**. A korábbi phishing e-mailek gyakran amatőr megfogalmazásúak voltak, tele nyelvtani hibákkal. Az NLP segítségével a támadók olyan üzeneteket hozhatnak létre, amelyek tökéletesen utánozzák egy adott személy vagy szervezet stílusát, így nehezebbé válik a csalás felismerése. Az NLP lehetővé teszi, hogy a támadók személyre szabott üzeneteket készítsenek, amelyek az áldozat érdeklődési körére, online viselkedésére és korábbi kommunikációira épülnek. Ez fokozza az üzenetek hitelességét és a sikerességi arányt.

Az NLP-alapú chatbotok képesek **dinamikusan** reagálni az áldozat kérdéseire, így hosszabb interakciók során is meggyőzőek maradnak. Például egy hamis ügyfélszolgálati chatbot képes hitelesen utánozni egy bank ügyfélszolgálatát és jelszavakat vagy PIN-kódokat kérni az ügyféltől.

Deepfake képgenerálás:
a vizualizált bizalomépítés

A deepfake technológiák lehetővé teszik meggyőző **személyek** vagy **videók létrehozását**. A támadók olyan képeket vagy videókat készíthetnek, amelyekben például egy vezérigazgató arra kéri az alkalmazottakat, hogy sürgősen utaljanak át pénzt egy adott számlára. Hitelesített dokumentumok manipulálása révén, hamis igazolványok, aláírt szerződések vagy pecsétek segítségével a támadók növelhetik az áldozatok bizalmát a csalás hitelességével kapcsolatban.



Voice Synthesis:
a hitelesített hangutánzás

A voice synthesis technológia lehetőséget ad arra, hogy a támadók **valósághű hangokat** szimuláljanak. Egyre elterjedtebb az, hogy a támadók az áldozat által ismert személyek (pl. vezetők, ügyfelek, rokonok) hangját utánozzák, és telefonon kérnek adatokat vagy adnak utasításokat. Voice synthesis és NLP kombinációjával az áldozatok interaktív telefonos beszélgetésekben találhatják magukat, ahol a támadók meggyőzően imitálják a valódi személyeket vagy szervezeteket.

Az Amerikai Egyesült Államokban már előfordult, hogy egy interneten talált hangminta – videó, hangklip – segítségével hamisították meg a családtag hangját. A „rokon" telefonon elmondta, hogy bajba került és pénzre van szüksége, de még mielőtt kérdezni tudtak volna, egy „rendőr" vette át a telefont. Ezekben a helyzetekben is fontos, hogy őrizzük meg a hidegvérünket, gondoljuk át a helyzetet és inkább hívjuk fel a bajba került rokont.

Machine Learning (ML): a gépi tanulás

Lehetővé teszi tömeges támadások személyre szabását. A Machine Learning (ML) algoritmusok az áldozatok online viselkedésének, közösségi média aktivitásának és egyéb digitális lábnyomainak **elemzésével célzott phishing kampányokat** generálhatnak. Az ML modellek képesek a korábbi phishing támadásokból tanulni, optimalizálni a módszereket és növelni a hatékonyságot. Az ML segítségével a támadók olyan e-maileket és üzeneteket készíthetnek, amelyek képesek megkerülni az AI-alapú spam- és phishing-szűrőket. Például egy támadás során az ML algoritmus az áldozat közösségi média tevékenysége alapján személyre szabott adathalász e-mailt hoz létre, amely az áldozat érdeklődési köreit és aktuális tevékenységeit használja ki.

Érzelmi manipuláció: a social engineering

Az AI algoritmusok képesek elemezni az embereket a profiljuk alapján, hogy olyan személyreszabott üzeneteket hozzanak létre, amelyek magas hatásfokkal váltanak ki olyan érzelmi reakciókat, mint például félelem vagy izgatottság, így elhomályosítva az áldozatok ítélőképességét. A mesterséges intelligencia által vezérelt botok nagyszabású social engineering kampányokban vehetnek részt a közösségi platformokon, automatizálva a bizalom kiépítésének és az egyének manipulálásának folyamatát.

Védekezés

Az AI és az ML használata nemcsak a támadás , hanem a védekezés **kulcsfontosságú eszköze is lehet.** Az anomáliák és gyanús tevékenységek felismerése lehetővé teszi a phishing támadások időben történő blokkolását.

A gépi tanulási algoritmusok képesek **hatalmas mennyiségű adatot gyorsan** feldolgozni és azonosítani azokat a mintákat, amelyek eltérnek a normális viselkedéstől. Meg tudja tanulni, hogy mi a „normális" aktivitás egy felhasználó esetében, majd figyelmeztetéseket generálhat, ha valami gyanús történik. Ha egy felhasználó egy szokatlan eszközről vagy helyről jelentkezik be, vagy a gépelési szokásai jelentősen megváltoznak, az AI jelezheti, hogy a fiók esetleg kompromittálódott.

Ezek az algoritmusok **fel tudják ismerni a hamis weboldalak** jeleit, amelyek hasonlóak a valódi, hivatalos oldalakhoz, de bizonyos részletekben eltérnek (pl. URL, dizájn, titkosítás hiánya). A gépi tanulás algoritmusai az ilyen weboldalak esetében, a detektálást követően figyelmeztetéseket generálhatnak.

Képesek az adathalász **e-mailek automatikus felismerésére is**. A szöveges tartalom, a feladó címének analízisére, a linkek és mellékletek vizsgálatára alapozva képesek azonosítani a gyanús e-maileket és figyelmeztetni a felhasználókat.

A gépi tanulási algoritmusok elemezhetik a felhasználók pénzügyi adatait, a pénzügyi tranzakciókat, hogy gyorsan **észleljék a szokatlan tevékenységeket**, például hamis vásárlásokat, pénzkivonásokat, vagy olyan helyekről történő tranzakciókat, amelyek nem illenek a felhasználó szokásos mintáiba.

Valós esettanulmányok

Néhány hírhedt kibercsalás, amely pszichológiai manipulációval ért célt:

Target-adathalászat (2013)

2013 decemberében az egyik legnagyobb amerikai kiskereskedelmi vállalat, a Target Corporation, az Egyesült Államok történetének egyik legnagyobb adatvédelmi incidensét élte meg. Közel 40 millió vásárló hitelkártyaszámát lopták el POS rendszerek adataihoz való hozzáférés révén.

A kezdő célpont nem a Target volt, hanem az egyik beszállítója. A Fazio Mechanicalnak csaknem 2 hónappal a betörés előtt egy adathalász e-mailt küldtek. A Fazio Mechanical a Malwarebytes Anti-Malware ingyenes verzióját használta. A használt rosszindulatú szoftver a Citadel volt, amely egy jelszólopó botprogram, amelyet valószínűleg az e-mailben található PDF vagy Microsoft dokumentumba ágyaztak be, majd telepítettek az áldozat számítógépére. A kártevő képes volt megszerezni az online eladói portál bejelentkezési adatait, majd innen jutottak be a Target hálózatába.

Független források szerint az ellopott hitelkártyaszámokból eredő károk **250 millió és 2,2 milliárd dollár** közé tehető. A Target ellen több, mint 80 pert indítottak. Az adatvédelmi incidens teljes költsége 202 millió dollár volt.

Twitter hack (2020)

A támadók olyan Twitter-alkalmazottakat kerestek a LinkedIn-en, akik valószínűleg **adminisztrátori jogosultságokkal** rendelkeztek. Ezután az állásközvetítők számára elérhetővé tett fizetős eszközökön keresztül megszerezték ezeknek az alkalmazottaknak a mobiltelefonszámait és egyéb privát elérhetőségi adatait. A támadók felvették a kapcsolatot az alkalmazottakkal, akiknek többsége a COVID-19 járvány miatt távmunkában dolgozott, és a LinkedIn-ről és más nyilvános forrásokból származó információk felhasználásával a Twitter munkatársainak adták ki magukat. Arra utasították az áldozatokat, hogy jelentkezzenek be egy hamis belső Twitter VPN-be. Az elkövetők hozzáférést szereztek a Twitter adminisztrációs eszközeihez, így maguk módosíthatták a fiókokat, és azokon egy bitcoin csalást népszerűsítettek. A csaló tweetek azt állították, hogy a feladó egy COVID-19 segélyakció részeként visszafizeti bármely felhasználónak az adott tárcákra küldött bitcoinok értékének kétszeresét. A fiókok között olyan ismert személyek is akadtak, mint Barack Obama, Joe Biden, Bill Gates, Jeff Bezos, MrBeast, Michael Bloomberg, Warren Buffett, Floyd Mayweather Jr, Kim Kardashian és Kanye West, valamint olyan cégek, mint az Apple, az Uber és a Cash App.

Sony Pictures hack (2014)

A 2014-es Sony Pictures hack egy jelentős kibertámadás volt, amely során a **Lazarus** (Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Diamond Sleet) nevű hackercsoport behatolt a Sony Pictures Entertainment számítógépes hálózatába. A támadás során a csoport **több mint 100 terrabájtnyi adatot tulajdonított el**. Ezt követően törölték a Sony rendszereinek jelentős részét, így azok működésképtelenné váltak. Az ellopott adatok között voltak alkalmazotti e-mailek, személyes információk, pénzügyi adatok, valamint még meg nem jelent filmek másolatai. A hackerek követelték a "The Interview" című film bemutatásának leállítását, amely egy vígjáték volt Kim Dzsongun észak-koreai vezető meggyilkolásáról. A fenyegetések hatására több nagy mozihálózat lemondta a film vetítését, és a Sony végül úgy döntött, hogy korlátozott számú moziban és digitális platformokon elérhetővé teszi a filmet.

Az Egyesült Államok kormánya a támadásért Észak-Koreát tette felelőssé, bár egyes szakértők megkérdőjelezték ezt az állítást. A támadás jelentős anyagi és reputációs károkat okozott a Sony számára, és rávilágított a vállalati kibervédelem fontosságára. A hackerek spear phishing e-maileket küldtek a Sony alkalmazottainak, amelyek látszólag megbízható forrásból származtak, például Apple ID-ellenőrzéseket imitáltak. Ezek az e-mailek hamis linkeket tartalmaztak, amelyekre kattintva a felhasználók megadták a bejelentkezési adataikat a támadóknak.

A megszerzett hitelesítő adatok segítségével a támadók beléptek a Sony hálózatába, majd további jogosultságokat szereztek. A behatolás után a támadók kártevő szoftvereket telepítettek, amelyek lehetővé tették számukra az adatok gyűjtését és továbbítását. Ezen kártevők között volt egy "Brambul" nevű féreg, amely brute force támadásokkal terjedt a hálózaton, valamint egy SMB Worm Tool, amely különböző komponenseket tartalmazott, mint backdoor és proxy eszközök.

Kevin Mitnick (1979)

Kevin Mitnick sikeresen megszerezte a Digital Equipment Corporation (DEC) VMS **operációs rendszerének forráskódját.** Mitnick felhívott több DEC alkalmazottat, és hivatalos személynek adta ki magát. Meggyőzően eljátszotta, hogy a cég egyik belső dolgozója, akinek sürgős hozzáférésre van szüksége egy adott rendszerhez. Ezt olyan részletes információk segítségével érte el, amelyeket korábban nyilvános adatokból vagy más alkalmazottak félrevezetésével gyűjtött össze. A telefonhívások során megszerezte a céges dolgozók belépési adatait, például felhasználóneveket és jelszavakat. Miután megszerezte az információkat, távolról belépett a DEC rendszerébe, és lemásolta a VMS forráskódját, amiért az 1988-as perben elítélték, és 12 hónap börtönbüntetésre, valamint három év felügyeletre ítélték. A felügyeleti időszak vége felé Mitnick behatolt a Pacific Bell hangposta rendszereibe is, ami miatt újabb letartóztatási parancsot adtak ki ellene. Ezt követően több mint két évig szökésben volt, mielőtt 1995-ben letartóztatták.

Deep Voice (2019)

Egy brit energetikai vállalat vezérigazgatóját deepfake technológia alkalmazásával tévesztették meg. A csalók mesterséges intelligencia segítségével leutánozták a cég német anyavállalat vezetőjének hangját, és telefonhívás során sürgős pénzátutalásra utasították a vezérigazgatót. A megtévesztő hívás annyira meggyőző volt, hogy a vezérigazgató **220 ezer eurót utalt át** egy magyarországi bankszámlára, abban a hitben, hogy főnöke kérését teljesíti.

A vezérigazgató felismerte főnöke hangjában a finom német akcentust, ráadásul a hang a férfi „dallamát" hordozta. Később kiderült, hogy a hívás mögött csalók álltak, akik kihasználták a deepfake technológia fejlődését, amely lehetővé tette számukra a valósághű hangutánzást. A csalók háromszor hívták fel a céget. Először az átutalás kezdeményezése miatt, másodszor hamisan azt állították, hogy már visszatérítették, harmadszor pedig utólagos kifizetést kérve. Ekkor az áldozat szkeptikus lett. Látta, hogy az állítólagos visszatérítés nem történt meg, és észrevette, hogy a hívás egy osztrák telefonszámról érkezett.

Bár a legnagyobb átverések külföldön történtek, Magyarországon is jelentős károkat okoznak a social engineering módszerrel elkövetett csalások. Elég csak a még mindig előforduló, banki ügyintézőnek álcázott csalásra gondolni, amelyről intézetünk korábban több tájékoztatót adott ki. Erről a Kiberpajzzsal együttműködve egy telefonhívást is publikáltunk.

Banki csalás telefonon (2024)

Egy magát banki szakembernek kiadó nő vert át egy magyar férfit. A hívás során arról tájékoztatta, hogy a számláján nagy értékű gyanús tranzakciót észleltek. Az áldozat közölte, hogy nem ő kezdeményezte, mire az ügyintéző utasításokat adott, hogy elkerüljék a további károkat. Utasította, hogy menjen be egy közeli bankfiókba, és ott adjon le egy átutalási megbízást a telefonon lediktált számlára. A csaló felhívta áldozata figyelmét, hogy ne mondjon semmit a banki ügyintézőnek, mivel lehetséges, hogy ő is benne van a támadásban. A férfi végrehajtotta a kért átutalási megbízást. **Több mint 4 millió forint**ja került a csalók számlájára.

AnyDesk (2024)

Közel 5 millió forintot utaltak el annak a tapolcai lakosnak a bankszámlájáról, akit egy magát banki ügyintézőnek kiadó nő hívott fel azzal, hogy a számláján 200 000 forint értékben gyanús tranzakciót észleltek. A férfit rávették az AnyDesk nevű alkalmazás telepítésére. Ezután az elkövető a megszerzett csatlakozó kóddal teljes hozzáférést szerzett áldozata telefonjához, és azon keresztül a bankszámlájára is be tudott lépni a webes felületen. Az AnyDesk alkalmazással elkövetett csalásokról korábban intézetünk is adott ki tájékoztatót.

A híres zenész (2023)

A Pécsi Tudományegyetem és a Vas Vármegyei Markusovszky Lajos Egyetemi Oktatókórház közölt egy esetet, amelyben egy 70 éves magyar nő online ismerkedett meg egy híres zenész képeit felhasználó csalóval. A beszélgetéseik egyre bizalmasabbá váltak, számos személyes információt is megosztottak egymással. Egyre több kedves üzenetet kapott tőle, melyekben a „zenész" dicsérte, hogy milyen különleges és vonzó személyisége van. Egy alkalommal telefonon is beszéltek, amikor a művész szerelmet vallott. Később különböző okokra hivatkozva (például jótékonysági célok, telefonszámla kifizetése) jelentősebb pénzösszegek átutalását kérte.Kezdetben belátta, hogy ez meghaladja anyagi lehetőségeit. Ekkor rendőrségi feljelentést is tett, ennek következtében több álprofilt megszüntetett a csaló, de később egy újabb profilon folytatta a kommunikációt áldozatával. Ettől megromlott a kapcsolata a férjével, **súlyos lelki válságba került, ami öngyilkossági kísérlethez vezetett**.

Ezek az esetek jól mutatják, hogy a pszichológiai manipuláció hogyan használható fel hatékonyan a kiberbűnözésben, mekkora károkat képes okozni, és miért kulcsfontosságú ennek megértése a védekezésben.

Záró gondolatok

A kibercsalások pszichológiájának megértése napjainkban elengedhetetlen, hiszen az online tér egyre szervesebb részévé válik az életünknek. Mindennapi tevékenységeink – legyen szó banki ügyintézésről, online vásárlásról vagy közösségi média használatról – folyamatosan kiberbűnözők célpontjává tesznek ki minket. Az ilyen támadások nem csupán anyagi károkat okozhatnak nekünk, hanem jelentős pszichológiai terhet is róhat ránk, ezért alapvető fontosságú, hogy megértsük a támadók módszereit, és hatékony eszközöket fejlesszünk ki ezek ellen.

A társadalmi manipuláció és az emberi pszichológia kihasználása a kibercsalások egyik legnagyobb ereje. Az emberek természetes bizalmára, segítőkészségére, illetve félelmeire alapozó technikák sajnálatos módon jó hatékonysággal működnek, ha az áldozatok nincsenek felkészülve ezek felismerésére. Az **oktatás** és a **figyelemfelhívás** ezért kulcsfontosságú. A kibertámadásokkal szembeni tudatosság növelése révén megelőzhetjük, hogy a támadók érzelmi manipulációval kihasználják gyengeségeinket.

Ezen túlmenően, a társadalom egésze számára fontos, hogy az áldozatok ne legyenek megbélyegezve, hiszen **bárki válhat célponttá**. Az áldozathibáztatás elkerülése segíthet abban, hogy az érintettek könnyebben forduljanak segítségért, és a tapasztalatok megosztásával másokat is megóvjanak a hasonló helyzetektől. Az empátia és támogatás kulcsszerepet játszik az áldozatok pszichológiai felépülésében.

A jövőben a technológiai fejlesztések mellett még nagyobb hangsúlyt kell fektetnünk az emberi tényezőre. Mivel a kiberbűnözés **folyamatosan fejlődik**, a védekezésnek is **lépést kell** ezzel tartania. Az emberek oktatása és a pszichológiai aspektusok megértése nemcsak a megelőzést szolgálja, hanem hozzájárul egy tudatosabb, biztonságosabb online közösség kialakításához is.

A kibercsalások pszichológiájának tanulmányozása végső soron nemcsak a bűnözők elleni harcot segíti, hanem egy olyan digitális kultúra megteremtését is, ahol a felhasználók biztonságban érezhetik magukat, és tudatosan, felelősségteljesen használhatják az online világ eszközeit. A megelőzés, a védekezés és a folyamatos tanulás hármasa a kulcs ahhoz, hogy csökkentsük a kibercsalások áldozatainak számát, és megerősítsük az emberek ellenálló képességét a digitális térben.

Források

- **Chaintech (2024).** *1979 DEC Breach: kevin Mitnick's First Cyber Intrusion.* https://www.chaintech.network/blog/1979-dec-breach-kevin-mitnicks-first-cyber-intrusion/ (Letöltve: 2025. január 06.)
- **Columbia Business School (2025).** *Using natural language processing to analyse text data in behavioural science.* https://business.columbia.edu/sites/default/files-efs/citation_file_upload/s44159-024-00392-z.pdf (Letöltve: 2025. január 05.)
- **Cornell Univesity (2024).** *Chibuike Samuel Eze, Lior Shamir - Analysis and prevention of AI-based phishing email attacks.* https://arxiv.org/abs/2405.05435 (Letöltve: 2024. december 17.)
- **Forbes (2019).** *A Voice Deepfake Was Used To Scam A CEO Out Of $243,000.* https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/ (Letöltve: 2025. február 12.)
- **Medium (2022).** *Complete Case Study — Target Data Breach.* https://medium.com/thedeephub/complete-case-study-target-data-breach-2-ba4bb365a82e (Letöltve: 2025. január 08.)
- **Diósi Szabolcs (2024).** *Mesterséges intelligencia, szintetikus valóság - Az MI és GenMI rendszerekkel kapcsolatos globális kihívások és európai szabályozási stratégiák.* https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/diosi-szabolcs/diosi-szabolcs-muhelyvita-ertekezes.pdf (Letöltve: 2025. január 07.)
- **Osváth Péter, Vörös Viktor, Simon Júlia, Hamvas Edina, Tényi Tamás, Nasri Alotti (2023).** *Az online romantikus csalások veszélyei – tanulságok egy mentális zavarral élő idős áldozat esete kapcsán.* Orvosi Hetilap, 165(5) 192-200. pp. https://akjournals.com/view/journals/650/165/5/article-p192.xml (Letöltve: 2024. december 18.)
- **Rendőrség (2024).** *Banki ügyintézőnek adta ki magát, közel 5 millió forintot csalt ki.* https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/banki-ugyintezonek-adta-ki-magat-kozel-5 (Letölve: 2024. december 17.)

- **Rendőrség (2024)**. *Bement a bankba, és több mint 4 milliót elutaltatott a csalóknak.* https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/bement-a-bankba-es-tobb-mint-4-milliot (Letöltve: 2024. december 17.)
- **SecureOps (2021).** *The Hack on Sony Group Pictures Entertainment.* https://www.secureops.com/wp-content/uploads/2021/06/Sony-Breach-Analysis-v4.pdf (Letöltve: 2025. január 03.)
- **Time (2024).** *The Psychological Trick Scammers Rely on and How to Protect Yourself.* https://time.com/6802061/scammers-financial-fraud-emotions/ (Letöltve: 2025. január 07.)
- **Unite.AI (2024).** *Empathetic AI: Transforming Mental Healthcare and Beyond with Emotional Intelligence.* https://www.unite.ai/empathetic-ai-transforming-mental-healthcare-and-beyond-with-emotional-intelligence/ (Letöltve: 2025. január 06.)
- **X Blog (2020)**. *An update on our security security incident.* https://blog.x.com/en_us/topics/company/2020/an-update-on-our-security-incident (Letöltve: 2024. december 04.)

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025