



Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Hogyan használják ki a kiberbűnözők érzelmeinket

Egy drága üzenet

Emma épphogy végzett a bevásárlással, karjain táskák csüngöttek, amikor telefonja megcsörrent a lányától kapott SMS miatt.

"Anyá, elvesztettem a telefonomat! Az egyik barátomról írok. Kellene pénz egy újra. Tudnál nekem küldeni 800 dollárt minél hamarabb? - Később majd elmagyarázom!"

A szíve majdnem megállt egy pillanatra. A lánya, Angie egy távoli egyetemen tanult, Emma pedig tudta, hogy a telefon rendkívül fontos számára az iskola meg a munka miatt, és a kapcsolatot is csak azzal tudták tartani. Nyugtalanította a gondolat, hogy lánya telefon nélkül maradt. Gyorsan válaszolt,

"Jól vagy? Mi történt?"

Hamarosan meg is érkezett a válasz.

"Jól vagyok, de most nem tudok beszélni. Kölcsönkértem egy barátom telefonját. El tudnád küldeni a pénzt most? Minél hamarabb kéne egy másik telő. Este felhívlak. Szeretlek!"

Emma egy pillanatig hezitált. Érezte, hogy valami furcsa, de az aggodalma erősebb volt kételyeinél. Megnyitotta a banki alkalmazását, és átutalta a 800 dollárt az SMS-ben megadott telefonszámra. Eszébe sem jutott megkérdőjelezni, miért nem közvetlenül a lánya számlájára megy az összeg – talán Angie nem fér hozzá a telefonja nélkül.

Később este felhívta Angiet a saját számán, reménykedve abban hogy megkönnyebbülve veszi majd fel. Ehelyett átlagos hangon válaszolt.

"Szia anyá! Mizujs?"

Emma lefagyott.

"Megkaptad a pénzt?"

Angie zavarodottnak hangzott.

"Milyen pénzt?"

Emma gyomra görcsbe rándult. Ismét megnyitotta üzeneteit, és elolvasta őket friss szemekkel. A sürgősséget sugalló hangnem, a részletek hiánya, a kitartás az azonnali pénzküldés mellett - hirtelen mind azt kiáltotta **csalás**. Egy csaló a lányának adta ki magát, tudva, hogy egy pánikba esett anyuka nem fog megállni gondolkodni.

Sajnos Emma nincs egyedül. Mindennapos dolog, hogy a kiberbűnözők érzelmeiket manipulálják annak érdekében, hogy az embereket drága hibák elkövetésére ösztönözzék. Itt van öt érzelmi trigger, amiket gyakran kihasználják - és az is, hogy hogyan vehetjük észre őket mielőtt túl késő.

1. Sürgősség - "Cselekedj Most, vagy Elvesztesz Valamit"

A csalók gyakran mesterséges időnyomást helyeznek ránk, annak érdekében, hogy a nagy sietség miatt hibát kövessünk el.

Hogyan működik:

"A bankfiókját feltörték! Igazolja személyazonosságát két órán belül, különben zároljuk a számláját."

- "A vásárlását rögzítettük." (amikor valójában nem is vásároltunk semmit)
- "A jelszava hamarosan lejár! Frissítse azonnal itt."

Hogyan vegyük észre:

- Vegyük fel a kapcsolatot a céggel a hivatalos elérhetőségein, például egy megbízható telefonszámon vagy a cég saját mobilalkalmazásán keresztül.
- Keressük a homályos részleteket az üzenetben - a valódi cégek részleteket közölnek, nem fenyegetnek.

2. Félelem - "Valami rossz fog történni"

A kiberbűnözők a félelmet használják pánikkeltésre, hogy az áldozatok gondolkodás nélkül cselekedjenek.

Hogyan működik:

- "Ez a kormány. Önnek adóhátraléka van, fizesse ki azonnal, különben letartóztatjuk."
- "Egy vírust észleltünk eszközén! Hívja fel ezt a telefonszámot támogatásért."
- "Ha nem fizeti ki a váltságdíjat, a privát fotóit közzétesszük."

Hogyan vegyük észre:

- A kormányzati szervek nem fenyegetőznek SMS-ben, sem e-mailben.
- A tech cégek nem keresnek fel, hogy megjavítsák a számítógépünket.

3. Kíváncsiság - "Ezt nem fogod elhinni!"

A csalók a kíváncsiságot sokkoló vagy csábító üzenetekkel használják ki.

Hogyan működik:

- "Ezen a videón te vagy? 🤪" (kártékony linkkel csatolva)
- "Rendkívüli hírek! Hatalmas celeb botrány - kattints ide, hogy láthasd!"
- "Az egyik barátod megjelölt téged egy örült postban!"

Hogyan vegyük észre:

- Legyünk skeptikusak a szenzációhajász üzenetekkel szemben.
- Ellenőrizzük a feladó hitelességét, mielőtt bármire rákattintanánk.

4. Bizalom és Tekintély - "Ez olyasvalaki, akit ismerünk"

A kiberbűnözők megbízható személyeknek adják ki magukat - például bankoknak, a főnökünknek vagy akár a szeretteinknek.

Hogyan működik:

- "Szia Anya, én vagyok! Elvesztettem a telefonomat. Tudnál küldeni egy kis pénzt?"
- "Szia, a főnököd vagyok. Arra szeretnék megkérni, hogy vegyél pár ajándékutalványt egy irodai eseményhez."
- „Gyanús tevékenységet észleltünk a fiókjában. Kattintson ide, hogy biztosítsa!"

Hogyan vegyük észre:

- Hozzunk létre egy titkos jelszót a családtagjainkkal, hogy meggyőződhesünk egymás személyazonosságáról.
- Keressünk homályos részleteket - a csalók a legtöbbször nem tudják a nevünket, sem a címünket.
- Legyünk óvatosak a szokatlan kérésekkel szemben - különösen ha pénzről vagy érzékeny információról van szó.

5. Kíváncsiság és Kapzsiság - "Ön nyert valami elképesztőt!"

A "túl szép, hogy igaz legyen" típusú csalások az emberek jutalom vagy figyelem iránti vágyát használják ki.

Hogyan működik:

- "Gratulálunk! Ön nyert egy ingyen iPhone-t - vegye át most!"
- "Csodálatos embernek tűnsz, mesélj még magadról."
- „Ön kiválasztásra került egy exkluzív befektetési lehetőségre."

Hogyan vegyük észre:

- Ha előtte nem jelentkezünk, akkor nem is nyertünk. A valódi cégek nem kérnek díjat a nyeremények átvételéhez.
- Legyünk óvatosak az olyan idegenekkel, akik valamilyen túl szép dolgot erőltetnek ahhoz, hogy igaz legyen, vagy akik túl gyorsan vallják be romantikus érzelmeiket irántunk.
- Legyünk szkeptikusak azokkal az exkluzív ajánlatokkal szemben, amikre véletlenszerűen lettünk kiválasztva.

Legközelebb ha sürgős üzenetet vagy hívást kapunk, álljunk meg egy pillanatra, gondolkodjunk és győződjünk meg a dolgok biztonságosságáról mielőtt cselekszünk. Ne hagyjuk, hogy az érzelmeink a gyengeségeinké váljanak!

Vendégszerkesztő

Teresa Gehrke a [PopCykol](#) nevű online biztonsági és tudatosító cég alapítója. Több mint 10 évnyi iparágon belüli tapasztalattal rendelkezik, tanácsadóként dolgozott műszaki íróként, UX tervezőként és projektmenedzserként. A WiCyS Colorado igazgatósági tagja. Teresa egy díjnyertes zenész. [Linktree](#)



Források

Hízelgés és üres pénztárca: romantikával átitatott befektetési csalások: <https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/>

Fantomhangok: Védekezés a hangklónozásos támadások ellen: <https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/>

SMS-támadások: Egy smishing történet: <https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/>

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)

OUCH! A SANS Security Awareness által közzétett és a [Creative Commons BY-NC-ND 4.0 licence](#) alatt terjesztett kiadvány. Ezt a hírlevelet szabadon megoszthatja vagy terjesztheti egészen addig, amíg nem adja el vagy nem módosítja. Szerkesztőbizottság: Phil Hoffman, Leslie Ridout, Princess Young.