OUCH! 2025. február

SANS SECURITY AWARENESS

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Hízelgés és üres pénztárca: romantikával átitatott befektetési csalások

Lisa emlékezetes története

Lisa, a barátságos és sikeres menedzsment szakértő élete teli volt izgalommal a zsúfolt munkájának köszönhetően. Viszont ahogy a munkája egyre nyomasztóbbá vált, egyre inkább elszigetelve érezte magát, és a közösségi médiához fordult, hogy új embereket ismerhessen meg. Így ismerte meg "Ryan"-t online, egy férfit, akit hamar a bizalmába fogadott mint barát és társ – bár mindössze virtuálisan, hiszen a férfi a világ másik felén élt. Törődőnek tűnt, és Lisahoz hasonlóan érdekelte az utazás, a főzés, és végül: a befektetések.

Néhány hónap alatt kapcsolatuk egyre inkább megerősödött, Ryan azt ajánlotta Lisanak, hogy fektessen be abba a kriptopiacba, amibe ő is, hiszen az gyorsan növekedett. Megbízhatónak tűnt, így a nő eleinte kisebb összegekkel kezdte a befektetéseit. Ahogy látta, hogy az összeg nő, és Ryan is tovább biztatta, egyre több pénzt kezdett befektetni a piacba a következő hónapokban. Hat hónapnyi kapcsolat után végre megpróbálta kivenni a pénzét, a platform azonban „befagyasztotta" a számláját, Ryan pedig eltűnt. Lisa ekkor jött rá, hogy több mint 175,000 dollárt veszített egy romantikus és befektetési csalás keretein belül, amelyet "Pig Butchering"-nek neveznek. Az anyagi kártól csak az érezelmi árulás volt fájdalmasabb.

Mi az a Pig Butchering?

A "Pig Butchering" egy olyan bonyolult átverés, amely egyszerre ötvözi a romantikus és a befektetési csalásokat is. Néhány kiszámítható lépést követ, bár a részletek változhatnak:

1. **Kezdeti kapcsolatfelvétel**: A csaló gyakran üzenetküldő alkalmazásokon vagy a közösségi médián keresztül lép kapcsolatba az áldozattal hétköznapi üzeneteket, bókokat küldve neki, vagy valódi érdeklődést mutatva az élete iránt.
2. **Kapcsolat kiépítése**: Idővel, a csaló bizalmat épít ki. Személyes történeteket osztanak meg egymással, egyszerű, mindennapi beszélgetésekbe bocsátkoznak, és gyakran romantikus kapcsolatot építenek ki hogy megerősítsék a kötődést.
3. **Befektetési lehetőségek bemutatása**: A bizalom megteremtése után a csaló megemlít egy „biztonságos és jövedelmező" befektetést, gyakran kriptovalutákban. Azt állíthatják, hogy bennfentes tudással vagy kotábbi sikerrel rendelkeznek ezzel a befektetéssel kapcsolatban, gyakran hamis befektetési eredményeket mutatnak hihetetlen pénzügyi megtérüléssel.
4. **Kisebb befektetések ösztönzése**: A csaló arra ösztönzi az áldozatot, hogy próbálkozzon egy kisebb befektetéssel. Eleinte az áldozat a hamis "profitokat" és visszatérítéseket látja, amelyeket a csaló arra használ, hogy kiépítse megbízhatóságát. A kapcsolat elején a csaló még akár azt is megengedheti az áldozatnak, hogy kisebb összegeket kivegyen a befektéteskből, ezzel is építve a legitimitás látszatát.
5. **Tét növelése**: Ahogy az áldozat „nyereséget" lát, a csaló a sürgősség érzetével sietteti, hogy még többet fektessen be - „Cselekedj most, vagy lemaradsz!"
6. **Kapcsolat megszakítása**: Amikor a csaló úgy gondolja, hogy az áldozattól minden pénzt elvett, „befagyasztja" a számlát, vagy egyszerűen eltűnik. A platform elérhetetlenné válik, így az áldozatnak nem marad semmije.

Mik a legfőbb jelei a Pig Butchering csalások felismerésének?

1. **Túl szép hogy igaz legyen**: Óvakodjunk azoktól, akik garantált nyereséget vagy kockázatmentességet ígérnek. A legitim befektetésekben mindig van valamennyi kockázat, így a gyors, folyamatos nyereség gyakran into jel lehet.
2. **Váratlan kapcsolatfelvétel**: Legyünk óvatosak, amikor idegenek lépnek velünk kapcsolatba tisztázott ok nélkül. Kaptál valaha egy random “Hi” / "Szia" / köszönő üzenetet egy teljesen idegen embertől, és gondolkodtál, hogy mi lehet ez? Ez egy csalás kezdete. Lehetőség szerint semmilyen módon ne válaszoljunk rá, és amennyiben lehet, tiltsuk a küldő profilját.
3. **Kapcsolat hamar anyagiassá válik**: Ha valaki, akit online ismertünk meg elkezd befektetésekről vagy pénzügyekről beszélni, vegyük jelzés értékűnek. A csalók kapcsolataikat pénzügyekkel vegyítik, így manipulálva a bizalmat.
4. **Nyomás a befektetés felgyorsítására**: A csalók gyakran sürgetés érzetével veszik rá az áldozatokat hogy nagyobb összegeket és gyorsan fektessenek be. Azt állíthatják, hogy a lehetőség “ablaka csukódik”, vagy azt, hogy ez a lehetőség csak limitált ideig elérhető.
5. **Hamis befektetési platformok**: Sok rosszindulatú szereplő használ hamis, de legitim kinézetű befektetési weboldalakat vagy applikációkat, amelyek fabrikált számokat mutatnak. Óvakodjunk minden olyan platformtól, amely széleskörűen nem elismert vagy ajánlott megbízható tanácsadók által.
6. **Nehézségek a pénzfelvételben**: Az utolsó piros zászló az, amikor megpróbálunk pénzt felvenni, és késedelemmel, kifogásokkal vagy további költségekkel szembesülünk. Bármely megbízható befektetési portál engedi, hogy hozzáférjünk pénzünkhöz bármiféle akadály nélkül.

Hogyan védhetjük meg magunkat

Ezen csalások mögött képzett manipulátorok állnak. Mi magunk vagyunk a legnagyobb védelmünk.

- **Legyünk elővigyázatosak**: Amikor idegenek kezdeményeznek kapcsolatot velünk, legyünk nagyon gyanakvóak. Továbbá, minél jobbnak tűnik az üzlet, és minél inkább erősödik a befektetés iránti nyomás, annál valószínűbb, hogy csalásról van szó.
- **Alaposan ellenőrizzük a platformokat**: Ragaszkodjunk a jól ismert befektetési platformokhoz, és kerüljünk el minden olyan platformot, amelynek nem egyértelmű a tulajdonosi háttere vagy nincs szabályozási információja.
- **Védjük személyes adatainkat**: Ne osszunk meg túl sokat a pénzügyeinkről sem a magánéletünkről online, különösen olyan emberekkel ne, akikkel személyesen soha nem találkoztunk.

Vendégszerkesztő

Karen Nemani az AWS Canadian Professional Services kereskedelmi biztonsági vezetője és a WiCyS ontáriói leányvállalatának elnöke. Szenvedélyesen törekszik a kiberbiztonsági kultúra megváltoztatására, hogy olyan befogadó munkaerőt hozzon létre, ahol a különböző gondolkodásmódok, készségek és perspektívák virágozhatnak. https://www.linkedin.com/in/karenbnemani/

Források

Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you
Ne hagyjuk, hogy a kiberbűnözők lenyúlják a megtakarításainkat: Zároljuk a pénzügyi számláinkat!: https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/
Óvd a szívedet (és a pénztárcádat) a romantikus csalásoktól!:https://www.sans.org/newsletters/ouch/guard-your-heart-wallet-against-romance-scams/

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

Az 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: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.