ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

Már nem csak magánszemélyeket támadnak a csalók.

Az egyik főként cégeket érintő csalási módszer, amikor elkövető cégeket keres fel és valamilyen valós ügyfél, beszállító, partner vagy hitelező képviselőjeként azonosítja magát. A megkeresés érkezhet telefonon, levélben, vagy e-mailben. A hamis email cím megtévesztésig hasonlít az eredetire.
A csaló azt kéri, hogy a jövőbeli számláinál módosítsák valamelyik banki adatot, például a kedvezményezett bankszámlaszámát vagy másodlagos számlaazonosítóját. Az így megadott bankszámla felett a csaló rendelkezik és ha a cég alkalmazottja bedől a trükknek és a megadott számlára utal, megtörténik bűncselekmény, hiszen az összeget valójában a csalónak utalta el.

- Amennyiben ilyen e-mailt kapnak, mindenképpen vegyék fel személyesen a kapcsolatot a másik féllel, hogy ellenőrizzék, valóban ők küldték azt!
- Ellenőrizzenek minden, állítólagosan a beszállítótól vagy hitelezőtől érkező kérelmet – főleg akkor, ha azt kérik, hogy a jövőbeli számláknál módosítsák valamelyik banki adatot!
- Jelöljenek ki egy megbízott kapcsolattartót azoknak a vállalatoknak az esetében, amelyek számára rendszeresen indítanak kifizetéseket!
- Vezessenek be egy biztonságos rendszert adott összeghatár feletti kifizetések esetében, amelynek kifejezetten a helyes bankszámlaszám és kedvezményezett ellenőrzése a célja! Ez lehet például egy megbeszélés az érintett vállalattal.
- A számla kifizetésekor egy ellenőrzött e-mail-címre küldjenek tájékoztatást a kedvezményezettnek! A biztonság szavatolása érdekében szerepeltessék a fogadó bank nevét és a bankszámlaszám utolsó nyolc számjegyét, illetve a másodlagos számlaazonosítójának jellemző részletét (pl. az adóazonosító utolsó négy karakterét)!
- Korlátozzák azokat az adatokat, amelyeket megosztanak az alkalmazottakról a közösségi médiában!
- Az alkalmazott minden esetben jelentse a vezetőnek a csalási kísérleteket!

Egy másik módszerrel általában a kifizetési jogkörrel rendelkező alkalmazottakat támadják az elkövetők, és hamis számla kifizetésére, vagy jóvá nem hagyott átutalás indítására próbálják rávenni. Arra építenek, hogy a dolgozók igyekeznek gyorsan teljesíteni azokat a feladatokat, amelyek közvetlenül a felső vezetéstől érkeznek. A csalók általában részletes információkkal rendelkeznek a szervezetről, és a hívás (vagy e-mail) rendkívül meggyőzőnek látszik. Ez a fajta megkeresés kéretlen telefonhívás (vagy e-mail) formájában érkezik, látszatra a megfelelő felsővezetőtől, aki rendszerint a téma bizalmas kezelését kéri, de sürgeti az ügyintézést. A kérés ugyanakkor szokatlan, a belső előírásoknak ellentmondó is lehet.

- Az alkalmazottak kezeljék óvatosan, fenntartással a „vezetőtől” érkező szokatlan megkereséseket!
- Tartsák be szigorúan a kifizetésekre és a beszerzésre vonatkozó biztonsági eljárásokat! Ne hagyjanak ki eljárási lépéseket, és ne engedjenek a nyomásgyakorlásnak!

Tolna Vármegyei Rendőr-főkapitányság
Bűnmegelőzési Alosztály
7100 Szekszárd, Mészáros L. u. 19-21.
bunmegelozes.tolnavmrfk@tolna.police.hu

- Mindig gondosan ellenőrizzék a hívásokban, e-mailekben érkező kéréseket a bizalmas információk, pénzátutalások esetében! A csalók gyakran adják ki magukat pl. az épp külföldön tartózkodó cégvezetőnek, vagy használnak a valódihoz nagyon hasonló e-mail-címeket, amelyek csak egy karakterben térnek el az eredetitől.
- Ne az e-mailre válaszolva próbáljanak meggyőződni annak valódiságáról, hanem inkább telefonáljanak vagy más csatornán ellenőrizzék a feladatot! Ha van rá mód, hívják fel a felsővezetőt vagy annak asszisztensét, titkárságát!
- Amennyiben kétségeik vannak egy átutalási utasítással kapcsolatban, mindig kérdezzék meg egy kompetens munkatársukat, még akkor is, ha a feladat diszkrét kezelésére kérték!
- Soha ne nyissanak meg e-mailben kapott gyanús hivatkozásokat vagy mellékleteket! Különös körültekintéssel járjanak el, ha vállalati számítógépeken nyitják meg személyes e-mail-fiókjukat!
- Korlátozottan terjesszék az információkat, és kezeljék óvatosan a közösségi médiát! Ne tegyenek közzé semmilyen, a munkával vagy a munkahellyel kapcsolatos tartalmat, információt! Ne osszanak meg a vállalati hierarchiára, biztonságra és eljárásokra vonatkozó információkat!
- Minden esetben értesítsék a vezetőt, ha gyanús e-mailt vagy telefonhívást kapnak!

Ajánlom szíves figyelmükbe a kiberpajzs.hu weboldalt, ahol a hatóságok folyamatosan tájékoztatást adnak az online térben elkövetett vagyon elleni bűncselekmények trendjeiről, valamint azok megelőzésének lehetőségeiről.

Ha bajba kerül, forduljon a rendőrséghez, vagy hívja a 112-es segélyhívó számot!

Tolna Vármegyei Rendőr-főkapitányság
Bűnmegelőzési Alosztály
7100 Szekszárd, Mészáros L. u. 19-21.
bunmegelozes.tolnavmrfk@tolna.police.hu