RENDŐRSÉGI FELHÍVÁS

ÜZLETI CSALÁSOK A KIBERTÉRBEN

Az interneten történő ügyintézés, kommunikáció elterjedését a bűnözők is igyekeznek kihasználni. A gazdálkodó szervezeteket az alábbi két csalási forma érinti leggyakrabban. A módszerek ismeretében könnyebben felismerhetők és kivédhetők az ilyen kísérletek. A Rendőrség most ehhez nyújt segítséget. Legyen Ön is körültekintő, hogy ne váljon áldozattá!

SZÁMLACSALÁS

Az elkövetők úgy tesznek, mintha cége üzleti partnerei (pl. beszállítók) lennének. A csalók arról tájékoztatják, hogy a kapcsolattartási adatok vagy a fizetési adatok (pl. kedvezményezett banki adatai) megváltoztak. Az üzenet többféleképpen érkezhet: telefonon, levélben, e-mailben, stb. A feladó e-mail címe nagyon hasonlíthat üzleti partner e-mail címére vagy akár a levelezési rendszer feltörése esetén érkezhet az üzleti partner igazi e-mail címéről is. Az új e-mailt címet, telefonszámot vagy bankszámlát pedig a csalók felügyelik.

MIT TEHET MINT CÉG?

• Tájékoztassa alkalmazottait a csalók által használt módszerekről!
• Minden esetben ellenőriztesse a beszállítókkal vagy szerződésekkel kapcsolatos adatok (kapcsolattartási adatok, fizetési mód, bankszámla számok) módosítására vonatkozó igényeket!
• Figyelmeztesse az alkalmazottait, hogy mindig győződjenek a fizetési kérelem jogosságáról, és ellenőrizzék, nincs-e valamilyen szabálytalanság a számlán!
• Minimalizálja a szállítókkal és szerződésekkel kapcsolatos nyilvános adatokat a cége honlapján vagy közösségi médiában!

MIT TEHET MINT ALKALMAZOTT?

• Alaposan ellenőrizze az üzleti partnerektől érkező kéréseket, különösen, ha a kapcsolattartási adatokban, fizetési módokban, bankszámlájuk megváltoztatásáról tájékoztatnak! Fokozattan ellenőrizze a feladó e-mail címét, ne csak a megjelenített nevet!
• Ne használja a levélben/faxon/e-mailben érkezett kérésekben szereplő kapcsolattartási adatokat! Alkalmazza a korábbi levelezésekben szereplőket!
• Legyen személyes kapcsolata a céghez, amelynek rendszeresen utal!
• Bizonyos összeg feletti kifizetés esetére dolgozzon ki egy eljárást a bankszámla és a kedvezményezett ellenőrzésére! (pl. egyeztessen személyesen vagy videóhívásban a cégnél lévő kapcsolattartójával)!
• A közösségi médiában a lehető legkevesebb információt osszon meg munkáltatójáról, ne osszon meg adatokat üzletei partnereikről, szerződésekről!

További információkért látogasson el honlapounkra és Facebook oldalunkra:
http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag
https://www.facebook.com/internettudatosan

VEZETŐ NEVÉBEN ELKÖVETETT CSALÁS

Az elkövetők a cég pénzügyi ügyintézőjét valamilyen megtévesztéssel hamis számla kifizetésére vagy a cég számlájáról történő átutalásra veszik rá.

A csalók jól ismerik a céget, így magukat annak magasszintű vezetőjének kiadva, felhívják az alkalmazottat vagy e-mailt küldenek neki. Azonnali átutalás kérnek, gyakran használják a „titoktartás", „a cég bízik önben kifejezéseket". Kihasználhatják a vezető távollétét és az e-mailben arra hivatkoznak, hogy nem elérhető. Sürgős ok miatt kérik az utalást: adóügyek, vállalatfelvásárlás. A kérés elutasítása esetén fenyegetést alkalmaznak az ügy fontosságára és sürgősségére tekintettel.

A feladó e-mail címe nagyon hasonlíthat cégvezető e-mail címére vagy akár a levelezési rendszer feltörése esetén érkezhet az igazi e-mail címről is.

ÁRULKODÓ JELEK

- Közvetlenül olyan vezető lép kapcsolatba az ügyintézővel, akivel eddig nem volt kapcsolata.
- Teljes titoktartás kérése. Nyomásgyakorlás és sürgetés alkalmazása.
- Fenyegetés vagy szokatlan jutalom ígérete.
- A belső eljárásoktól vagy a gyakorlattól való eltérésre vonatkozó kérés.

MIT TEHET MINT CÉG?

- Ismerje meg és tájékoztassa alkalmazottait a csalók által használt módszerekről!
- Figyelmeztesse alkalmazottait, hogy legyenek elővigyázatosak a fizetési kérelmekkel!
- Vezessen be belső protokollokat a kifizetésekkel kapcsolatban!
- Ellenőriztesse az e-mailben vagy telefonon érkezett fizetési kérések jogosságát!
- Vizsgálja felül a cég weboldalán szereplő információkat, minimalizálja azokat a legszükségesebbre, legyen óvatos a közösségi médiában
- Gondoskodjon informatikai rendszerei (pl. elektronikus levelezés) biztonságáról!
- Ha csalást észlel, mindig értesítse a rendőrséget, akkor is, ha nem érte kár!

MIT TEHET MINT ALKALMAZOTT?

- Szigorúan tartsa be a fizetéssel kapcsolatos biztonsági szabályokat!
- Fokozattan ellenőrizze a feladó e-mail címét, ne csak megjelenített nevet!
- Ha kétsége merül fel egy fizetési kéréssel kapcsolatban, mindig egyeztessen felettesével vagy egy hozzáértő kollégájával!
- Soha ne nyisson meg gyanús linkeket vagy mellékleteket, amelyek e-mailen érkeznek!
- Legyen különösen figyelmes, ha a saját e-mail fiókjába lép be a céges számítógépen!
- Minimalizálja a munkájával és munkahelyével kapcsolatos információk megosztását a közösségi oldalakon!
- Ne osszon meg információt a cég szervezeti felépítésével, biztonságával és eljárási rendjével kapcsolatban!
- Ha gyanús e-mailt vagy telefonhívást kap, mindig jelezze a vezetőjének, illetve a biztonságért felelős részlegnek!

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN
Országos Rendőr-főkapitányság

További információkért látogasson el honlapounkra és Facebook oldalunkra:
http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag
https://www.facebook.com/internettudatosan