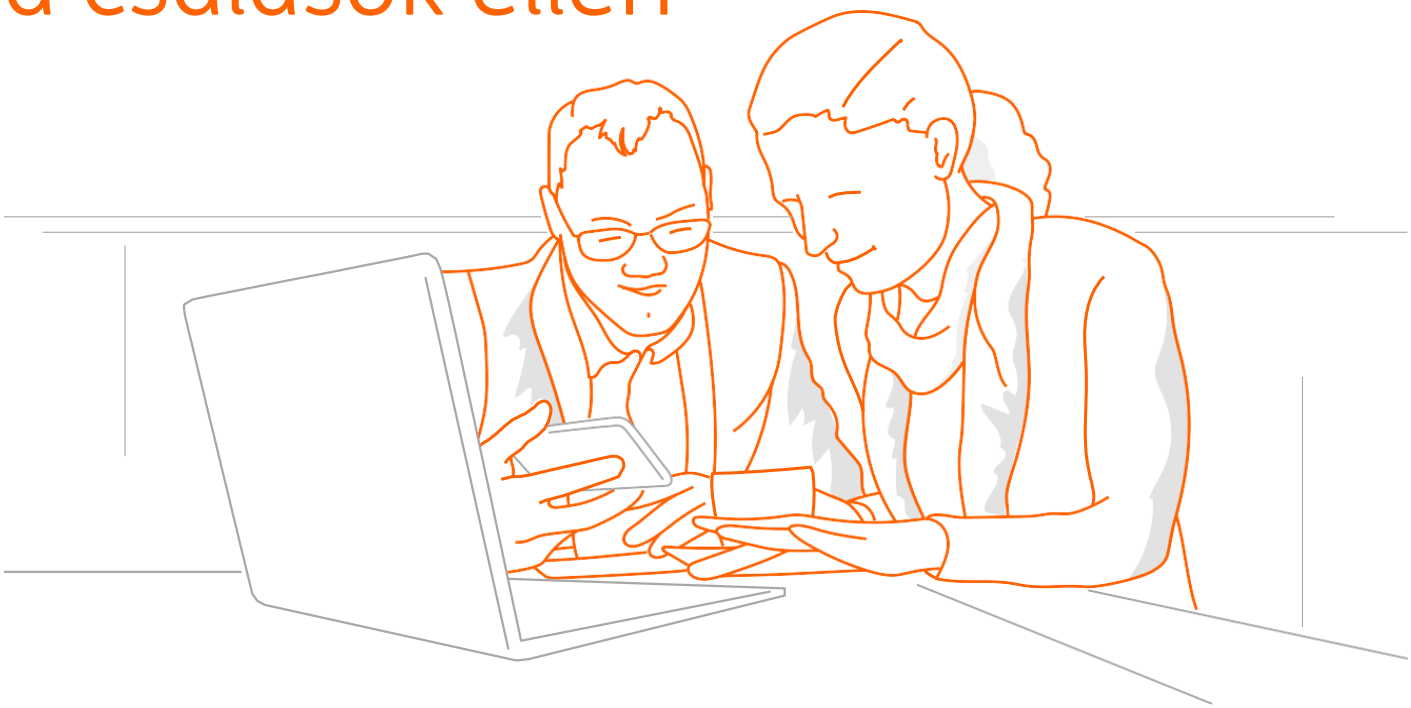
Óvja vállalkozását a csalások ellen



Vállalati csalás – Vezető tisztviselők nevével való visszaélés

Ez a brosúra a leggyakoribb csalástípusokat ismerteti, amelyek kihathatnak Önre és munkaadójára. Tanácsot ad továbbá abban, hogyan óvhatja meg magát. A csalók okosak, rendszerezettek és a „pszichológiai manipuláció” mesterei. Megtévesztést alkalmaznak, hogy intézkedések végrehajtására vagy a kiberbűncselekményekhez használt bizalmas vagy személyes információk megosztására ösztönözzék az embereket. Világszerte naponta történnek csalások, és több milliós veszteséget eredményeznek. Legyen óvatos.

Hogyan kell használni ezt a dokumentumot?

Terjessze a vállalatán belül, hogy felhívja a munkavállalói figyelmét, különösen azokét, akik jogosultak a vállalat számláihoz való hozzáférésre, vagy akik létrehozhatnak és/vagy jóváhagyhatnak fizetési utasításokat. A csalók gyakran azokat a munkavállalókat célozzák, akik rendelkeznek ilyen jogokkal.
Bár nincs teljes körű védelem a kiberbűnözés ellen, a tudatosság segíthet a „figyelmeztető jelzések” felismerésében.
Ismertesse és alkalmazza a brosúrában található ajánlásokat, hogy csökkentse a csalás kockázatát!

Fontos információ!

Amennyiben csalás történt, minden esetben haladéktalanul értesítse az ING kapcsolattartóját. Bár az elvégzett tranzakciók véglegesek, meg lehet próbálni visszanyerni vagy zárolni az összeget, mielőtt az végleg eltűnik a kedvezményezett számlájáról. A gyorsaság elengedhetetlen, mivel minden perccel egyre csökken az esély, hogy a tranzakciót vissza lehessen fordítani.

Ha az ING kapcsolattartója nem elérhető, kérjük, hívja

az ING Wholesale Banking csalásokkal foglalkozó részlegét a +36 1 235 8700-as számon

Munkaidő után vagy korábban történt
csalás esetén, kérjük, írjon a communications.hu@ingbank.com címre.

Mit jelent a vezető tisztviselők nevével való visszaélés?

A pszichológiai manipuláció során arra ösztönzik az embereket, hogy bizalmas vagy érzékeny információkat osszanak meg. A csaló felső vezetőnek vagy a felső vezetés nevében eljáró harmadik félnek tünteti fel magát, hogy a munkavállalókat fizetési tranzakciók végrehajtására vagy bizalmas információk megosztására ösztönözze.

Mi történik?

1. A csalók e-mailen vagy telefonon kapcsolatba lépnek a vállalatával, auditorként, mérlegképes könyvelőként vagy akár vizsgálatot végző kormányzati tisztviselőként lépnek fel. Ezzel információt gyűjtenek a számítógépén található belső fizetési eljárásokról, valamint azokról a személyekről, akik jogosultak ezek végzésére. Ezenkívül a közösségi oldalakon (LinkedIn, Facebook...) található információk segíthetnek a csalóknak abban, hogy azonosítsák a fizetési eljárásokban részt vevő alkalmazottakat vagy azokat, akik épp szabadságon vannak, annak érdekében, hogy a „bőrükbe bújjanak".
2. Vezérigazgatóként, pénzügyi igazgatóként vagy egyéb felső vezetőként feltüntetve magukat kapcsolatba lépnek a vállalat azon munkavállalóival, akik jogosultak nagyösszegű kifizetések teljesítésére, és egy külföldi versenytárs lehetséges felvásárlására irányuló döntésre vagy nagyobb tranzakciót igénylő eseményre hivatkoznak.
   Általában ezekben a forgatókönyvekben a csaló azt mondja, hogy a tranzakciót sürgősen és a lehető legnagyobb titokban kell végrehajtani.
3. A csalók külső tanácsadókra is hivatkozhatnak (akiknek ellopták a személyazonosságát), hogy a művelet még hitelesebbnek tűnjön. Ezt követően a „tanácsadó" kapcsolatba lép a kiszemelt munkavállalóval, hogy jóváhagyja a tranzakciót, és megerősíti a teljesítendő kifizetés titkos és sürgős jellegét. Ha a munkavállaló hezitál, a csalók számos trükköt bevetnek, például megemlítik a vállalat felső vezetőinek nevét, bókolnak vagy akár fenyegetnek.

Az ilyen csalások fajtái

Számos típus létezik, a csalók például tettethetik magukat ügyvédnek, közjegyzőnek, rendőrnek, ügyfélszolgálati munkatársnak stb.

Milyen óvintézkedéseket kell tenni?

- Mindig legyen óvatos, ha pénzösszegek sürgős és titkos átutalását kérik.
- Sürgős kérés esetén mindig hívja vissza azt a személyt, aki a kérést intézte, ismert, korábban ellenőrzött telefonszámon.
- Válassza szét a feladatköröket, alkalmazzon például kettős aláírással történő jóváhagyást, ahol legalább két embernek alá kell írnia a kifizetést. Ezenkívül győződjön meg róla, hogy az aláírást megfelelően teljesítette, a vállalat protokollját betartva, és ne írjon alá semmit bizalmi alapon.
- Ne engedélyezze a hitelesítési eszközök (pl. kártyák és PIN-kódok) megosztását.
- Kérje meg a munkavállalókat, hogy a közösségi oldalakon ne részletezzék, milyen szerepet töltenek be a szervezetnél.

Jogi nyilatkozat

Ez a brosúra kizárólag tájékoztatási célokat szolgál annak érdekében, hogy ismertesse az Ön számára a leggyakoribb csalási típusokat, és javaslatokat tegyen a velük szembeni védelemre. Ez a tájékoztatás nem biztosítja, hogy a vállalata az ajánlások betartásával védelmet élvez vagy fog élvezni a jelen brosúrában ismertetett bármely csalástípussal szemben. Semmilyen jog nem származik abból, ha a jelen ajánlások betartásával alkalmazza a megadott óvintézkedéseket. Az ING nem vállal felelősséget azzal kapcsolatban, hogy Ön betartja az ajánlásokat vagy azok eredményeként intézkedéseket hoz. Erre a jogi nyilatkozatra a holland jog irányadó.