Óvja vállalkozását a csalások ellen

Vállalati csalás – e-Bankinggal kapcsolatos csalás

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.

Mi az az e-Bankinggal kapcsolatos csalás?

Az e-Bankinggal kapcsolatos csalások magukban foglalják az adathalászatot és a rosszindulatú szoftverek vírusait. Ezek kihathatnak a vállalatára vagy a magánéletére. Bárhogy is, a kiberbűnözők meg fogják próbálni ellopni a pénzt azzal, hogy megszerzik az azonosító kódokat és elektronikus aláírásokat az áldozatuktól. Ezekkel a kódokkal átutalják az összeget a saját számlájukra, és kiürítik az Ön bankszámláit.

Mi történik?

1. Vélhetőleg kap egy e-mailt a bankjától, amelyben az alábbiak valamelyike áll: a bank biztonsági ellenőrzést végez, a számláját zárolják, vagy a bank módosítja néhány szolgáltatását. A cél az, hogy Ön rákattintson arra a hivatkozásra, amely az online bankfelületre hasonlító, hamis azonosító oldalra irányítja Önt.
2. Ezen az oldalon Ön megadja a belépési kódjait, amelyeket a bűnözők könnyen megszerezhetnek. A kódjaival hozzáférhetnek az Ön online banki felületéhez, és tranzakciókat végezhetnek az Ön nevében.

Az e-Bankinggal kapcsolatos csalások típusai

- Hívást kap a csalótól, aki banki munkavállalónak adja ki magát. Arra kéri Önt, hogy végezzen el valamilyen biztonsági ellenőrzést vagy „frissítést”, ami azt jelenti, hogy meg kell adnia neki a kódjait az okoskártyájával vagy leolvasójával. A csaló ezeket arra fogja használni, hogy belépjen az Ön személyes e-Banking profiljába, és aláírja az Ön nevében a tranzakciókat.
- Az Ön számítógépe rosszindulatú szoftverrel fertőzött. Az ilyen vírusok jellemzően a mellékletek, a rosszindulatú e-mailekben található hivatkozások megnyitásából vagy a sérült oldalak felkereséséből erednek, és jellemzően a webes böngészőjének vagy operációs rendszerének sérülékenységeit használják ki.

A rosszindulatú szoftver típusától függően számos forgatókönyv létezik, amelyet a csalók alkalmaznak a felhasználó megtámadásához. Végezetül ezek mind ahhoz vezetnek, hogy a rosszindulatú szoftver csalárd kifizetéseket hoz létre és hajt végre az Ön nevében.

Milyen óvintézkedéseket kell tenni?

- Biztosítson biztonságos munkakörnyezetet azzal, hogy megosztja és alkalmazza a biztonságos e-Bankingról szóló tájékoztatást, amelyet az ING az ingbank.hu címen tett elérhetővé
- Tartsa titokban PIN-kódját és a létrehozott biztonsági kódokat. Soha ne ossza meg ezeket a titkos kódokat senkivel, aki arra kéri Önt pl. telefonon, e-mailben, SMS-ben, WhatsApp üzenetben vagy személyesen. Az ING munkavállalói soha nem fogják elkérni az Ön kódjait.
- Soha ne generáljon biztonsági kódot, ha nem Ön lép be vagy használja az online banki felületet.
- Mindig ellenőrizze a részleteket, pl. az összeget és a kedvezményezett számlaszámát minden kifizetésnél, amelyet alá akar írni.
- Mindig zárja be megfelelően a webes böngészőben az aktív munkamenetet a „Kijelentkezés” gombra kattintva. Soha ne hagyja a számítógépét felügyelet nélkül, ha a munkamenet aktív: Zárja be a munkamenetet és zárolja a számítógépét.

Az online fizetési eszközök megfelelő kezelése

Egyes vállalati viselkedésminták megkönnyíthetik a csalók tevékenységét, és növelhetik a csalásoknak való kitettség mértékét:

- A kettős aláírás nem megfelelő kezelése: A kettős aláírás olyan eszköz, amely segít feltárni és megelőzni a csalást. Az a személy, aki a második aláírást végzi, és még egyszer ellenőrzi a tranzakciót, nem lehet érintett magában a tranzakcióban, és így könnyebben feltárhatja a csalást. Soha ne bízza mindkét aláírást ugyanarra a személyre, és ellenőrizze, mit ír alá. Mindig győződjön meg róla, hogy az első és második aláíró különböző PC-ket használ, mivel ez növeli a rosszindulatú szoftver által létrehozott csalárd kifizetések feltárásának esélyét.
- Megosztott hozzáférés: Ne használjon megosztott hozzáférésű eszközöket. Ez növelni fogja a biztonságot a vállalata és az adott személy számára, aki csak a jogosultságoknak megfelelően fog tudni eljárni.

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.