

VEZETŐI/ÜZLETI E-MAIL CÍMMEL ELKÖVETETT CSALÁS

Vezetői vagy üzleti e-mail címmel elkövetett csalás az, ha egy cég pénzügyi ügyintézőjét valamilyen trükk alkalmazásával hamis számla kifizetésére vagy a cég számlájáról történő pénzáttalásra veszik rá.

HOGYAN TÖRTÉNIK?

A csalók a cég magasszintű vezetőjeként telefonon felhívják az alkalmazottat, vagy e-mailt küldenek neki (pl. CEO vagy CFO).



Gyakran nemzetközi utalásokat kérnek, Európán kívülre.



Elég jól ismerik a céget.



Az ügyintéző elutalja a pénzt a csalók által kezelt bankszámlára.



Azonnali pénzáttalást kérnek.



Az ügyintézésre vonatkozó instrukciókat később tudatják vele, vagy egy harmadik személy küldi e-mailen.



Gyakran használják a 'Titoktartás', 'A cég bízik Önben', 'Jelenleg nem vagyok elérhető' kifejezéseket.



Arra kérik az ügyintézőt, hogy térjen el a megszokott ügyintézésről.



Érzékeny témára hivatkoznak (pl. adóellenőrzés, egyesülés és vállalatfelvásárlás).

MIK AZ ÁRULKODÓ JELEK?

- Kéretlen e-mail/ telefonhívás.
- Nyomás és sürgetés érzése.
- Közvetlenül egy vezető lép Önnel kapcsolatba, akivel eddig nem került kapcsolatba.
- A megszokott belső eljárásoktól történő eltérésre vonatkozó kérések.
- Teljes titoktartást kér.
- Fenyegetés vagy szokatlan kedvesség/jutalom ígérete.

MIT TEHET?

MINT CÉG

Legyen tisztában a veszélyekkel és győződjön meg arról, hogy ezeket az alkalmazottak is ismerik!

Figyelmeztesse az alkalmazottakat, hogy legyenek elővigyázatosak a fizetési kérésekkel!

Vezessen be belső protokollokat a kifizetésekkel kapcsolatban!

Vezessen be egy eljárást arra, hogyan ellenőrizzék az e-mailben érkezett fizetési kérés jogosságát!

Alakítson ki jelentési rendet a csalások kezelése érdekében!

Vizsgálja felül a cég weboldalán szereplő információkat, ha szükséges, korlátozza ezeket az információkat, és legyen óvatos a közösségi média oldalakon!

Feljessze és frissítse a technikai biztonságot!



Mindig értesítse a rendőrséget, ha csalást észlel, akkor is, ha nem dőlt be a csaló üzenetnek!

MINT ALKALMAZOTT

Szigorúan tartsa be a fizetéssel és a beszerzéssel kapcsolatos biztonsági szabályokat! Semmit ne hagyjon figyelmen kívül!

Mindig figyelmesen ellenőrizze az e-mail címeket, amikor bizalmas információkat kezel vagy pénzt utal!

Ha kétsége merül fel egy fizetési kéréssel kapcsolatban, egyeztessen egy hozzáértő kollégával!

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!

Minél kevesebb információt osszon meg 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 az informatikai részlegnek!