

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).

Elég jól ismerik a céget.

Azonnali pénzáttalást kérnek.

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

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

Gyakran nemzetközi utalásokat kérnek, Európán kívülre.

Az ügyintéző elutalja a pénzt a csalók által kezelt bankszámlára.

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

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

MIK AZ ÁRULKODÓ JELEK?

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

BEFEKTETÉSI CSALÁS

A befektetési csalást tartalmazó üzenetek általában jól jövedelmező befektetési lehetőségeket ajánlanak, például részvények, kriptovaluták, ritka fémek, tengerentúli földvásárlás és alternatív energiák.

MIK AZ ÁRULKODÓ JELEK?

➤ Gyors megtérülést ígérnek, és hogy biztonságban lesz a pénze.

➤ Az ajánlat csak rövid ideig elérhető.

➤ Több kéretlen telefonhívás érkezik.

➤ Az ajánlat csak Önnek szól, és arra kérik, ne ossza meg másokkal.



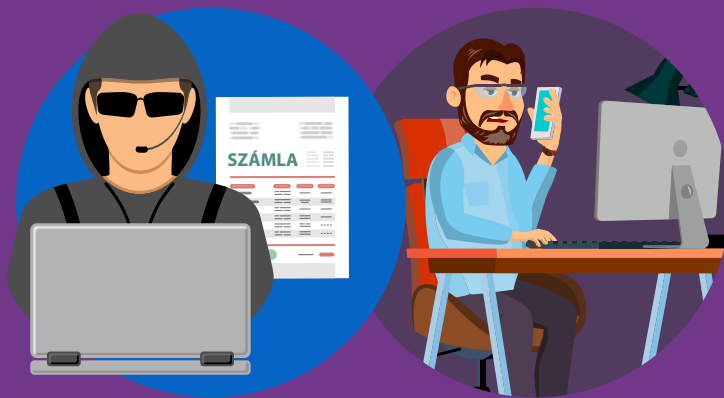
MIT TEHET?

- **Mindig kérjen pénzügyi tanácsot**, mielőtt pénzt ad át valakinek vagy befektet!
- **Ne fogadjon kéretlen telefonhívásokat**, amelyek befektetési lehetőségeket ajánlanak!
- **Legyen gyanús**, ha biztonságos befektetési lehetőségeket ajánlanak, és nagy profitot garantálnak!
- **Figyeljen a későbbi csaló üzenetekre!** Ha egyszer már bedőlt egy csaló üzenetnek, a csalók újra megkereshetik, vagy más bűnözőknek adják el adatait!
- **Értesítse a rendőrséget**, ha csalásra gyanakszik!

SZÁMLA CSALÁS

HOGYAN TÖRTÉNIK?

- > Az elkövetők úgy tesznek, mintha szállítók/szolgáltatók/hitelezők lennének.
- > A kapcsolatfelvétel többféleképpen történhet: telefonon, levélben, e-mailben, stb.
- > A csalók arról tájékoztatnak, hogy a fizetési adatok (pl. kedvezményezett banki adatai) megváltoztak. Az új bankszámlát pedig a csalók felügyelik.



MIT TEHET?

Győződjön meg arról, hogy **az alkalmazottak tisztában vannak** a csalók által használt módszerekkel!

MINT MUNKAADÓ



Figyelmeztesse az alkalmazottakat, hogy mindig **ellenőrizzék, nincs-e valamilyen szabálytalanság a számlán!**

Győződjön meg a fizetési kérés jogosságáról!

Ellenőrizze a cég honlapján szereplő információkat, a szerződéseket és a szállítókat! Figyeljen rá, hogy ki jogosult információt közzétenni a cégről a közösségi médiában!

Ellenőrizze a hitelezőktől érkező kéréseket, különösen ha a bankszámlájuk megváltoztatásáról tájékoztatnak!

MINT ALKALMAZOTT



Bizonyos összeg feletti kifizetés esetére dolgozzon **ki egy eljárást** a bankszámla és a kedvezményezett ellenőrzésére! (pl. találkozzon személyesen a céggel)!

Ne használja a levélben/faxon/e-mailben érkezett kérésekben szereplő kapcsolati adatokat! Inkább a **korábbi levelezésekben** szereplőket alkalmazza!

Ha kifizet egy számlát, **küldjön róla e-mailt a címzettnek!** Írja meg a kedvezményezett bank nevét és a bankszámla utolsó négy számjegyét a biztonság érdekében!

Legyen **személyes kapcsolata** a céghez, aminek rendszeresen utalást intéz!

Lehetőleg **minél kevesebb információt osszon meg** munkaadójáról a közösségi médiában!



Értesítse a rendőrséget, ha csalás áldozata lett vagy csaló üzenetet kapott!

ONLINE VÁSÁRLÁSI CSALÓ ÜZENETEK

Jó dolog online vásárolni, de vigyázni kell a csalókkal!



MIT TEHET?

- > **Használjon hazai weboldalakat**, ha lehetséges - így könnyebben ki lehet szűrni a gyanús tartalmakat!
- > **Nézzon utána** - ellenőrizze az oldalt, mielőtt vásárol!
- > **Használjon bankkártyát** - így könnyebben visszakaphatja a pénzét, ha szükséges!
- > **Mindig használjon biztonságos fizetési szolgáltatást** - Arra kéri, hogy utaljon pénzt? Kétszer is gondolja meg!
- > **Csak akkor fizessen, ha biztonságos az internetkapcsolat** - kerülje az ingyenes vagy nyilvános wifit!
- > **Csak biztonságos eszközről fizessen** - Mindig frissítse az operációs rendszert és a biztonsági szoftverét!
- > Legyen óvatos, ha mindenáron el akarnak adni Önnek valamit, vagy csodaszereket ajánlanak! - **Ha túl szép hogy igaz legyen, akkor valószínűleg nem igaz!**
- > Egy előugró ablak pénznyerési lehetőséggel kecsegtet? **Kétszer is gondolja meg**, lehet hogy vírust nyer vele, nem pénzt!
- > Ha nem érkezik meg a megrendelt termék, vegye fel a kapcsolatot az eladóval! Ha nem kap választ, **értesítse a bankját!**



Minden esetben értesítse a rendőrséget, ha csalást észlel, akkor is, ha nem dőlt be neki!

PÉNZÜGYI ADATHALÁSZ E-MAILEK

A "phishing" olyan adathalász e-mailt jelent, amellyel a csalók arra veszik rá a címzetteket, hogy adják meg személyes, pénzügyi és biztonsági adataikat.

HOGYAN TÖRTÉNIK?

Ezek az e-mailek:

hasonlítanak a bank által küldött e-mailekre.

utánozzák a banki logókat, hasonló a szerkezet és a hangneme is.



arra kéri, hogy töltsse le a mellékletet vagy kattintson a linkre.

olyan megfogalmazásúak, amellyel azt sugallják, hogy azonnal cselekedjen.

MIT TEHET?

- > **Mindig frissítse a szoftvereit**, beleértve a böngészőt, a víruskeresőt és az operációs rendszert is!
- > Legyen kimondottan **óvatos**, ha egy 'bank' üzenetben érzékeny információkat kér Öntől (pl. az online banki jelszót)!
- > **Olvassa el alaposan az e-mailt**: hasonlítsa össze az üzenetet korábbi banki üzeneteivel! Ellenőrizze, hogy van-e elírás vagy nyelvi hiba!
- > **Ne válaszoljon gyanús e-mailekre**, inkább írja fel, ki küldte, majd továbbítsa a banknak!
- > **Ne kattintson a linkre, és ne töltsse le a mellékletet**, inkább keressen rá a címre a böngészőben!
- > Ha kétségei vannak, **ellenőrizze kétszer** a bank weboldalát vagy hívja a fel a bankot!



A kiberbűnözők arra alapoznak, hogy az emberek elfoglaltak; első pillantásra ezek az e-mailek hivatalosnak tűnhetnek.



Vigyázzon a mobil eszközök használata során! Az adathalász emailek nehezebben szűrhetők ki telefonon vagy tableten!

#CyberScams



ÉRZELMEKET KIHASZNÁLÓ CSALÁS

A csalók jellemzően online párkereső oldalakon nézik ki célpontjaikat, de néha a közösségi médián vagy e-mailen keresztül veszik fel a kapcsolatot.



MIK AZ ÁRULKODÓ JELEK?



MIT TEHET?

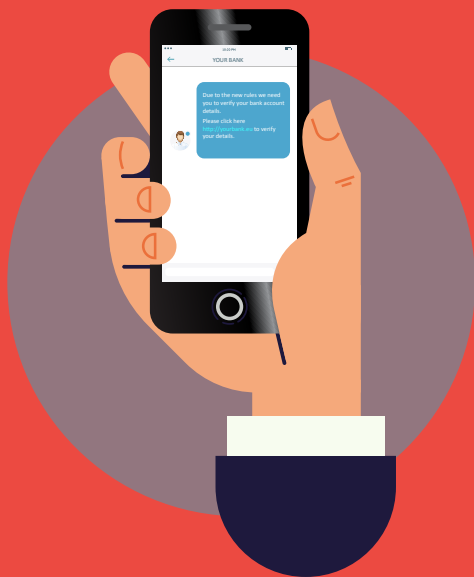
- **Legyen nagyon óvatos**, hogy mennyi személyes információt oszt meg magáról a közösségi médiában és a párkereső oldalakon!
- **Mindig gondoljon a lehetséges veszélyekre!** A csalók a legjobb hírű online oldalakat használják.
- **Ne kapkodja el a dolgokat**, tegyen fel Ön is kérdéseket!
- **Keressen rá az illető fotójára és profiljára**, hogy szerepel-e más oldalakon is!
- **Figyeljen a helyesírási és nyelvtani hibákra**, a következtetlenségekre és a kifogásokra, például hogy a csalók kamerája nem működik!
- **Ne osszon meg** kompromitáló dolgokat magáról, amivel később megzsarolhatják!
- Mielőtt személyesen találkozik valakivel, **mondja el a családjának és a barátainak** hová megy!
- **Legyen óvatos, ha pénzt kérnek Öntől!** Soha ne küldjön pénzt, ne adja meg bankkártya vagy online banki adatait, és ne küldjön másolatot okmányairól!
- **Kerülje, hogy előre fizessen bármiért!**
- **Ne küldjön pénzt másnak:** a pénzmosás bűncselekmény!

ÁLDOZATTÁ VÁLT?

Ne legyen szégyenérzete!
Azonnal szakítson meg minden kapcsolatot!
Ha tudja, mentse el a beszélgetések tartalmát!
Tegyen feljelentést a rendőrségen!
Jelyezze a problémát azon a párkereső oldalon is, ahol a csalóval kapcsolatba került!
Ha megadta a banki adatait, azonnal értesítse a bankot!

PÉNZÜGYI ADATHALÁSZ SMS-ek

A "smishing" (az SMS és a phishing szó kombinációja) azt jelenti, hogy a csalók személyes, pénzügyi vagy biztonsági információkat kérnek szöveges üzenetben.



HOGYAN TÖRTÉNIK?

A csaló SMS-ek arra kérnek, hogy a benne lévő linkre kattintva, vagy telefonszám felhívásával 'hitelesítse', 'frissítse' vagy 'újra aktiválja' a bankszámláját. De... a link egy hamis weboldalra irányít, a telefonszámot pedig csalók használják, akik úgy tesznek, mintha egy törvényesen működő cég ügyintézői lennének.

MIT TEHET?

- **Ne kattintson a linkre, mellékletre vagy képre**, amit a kérértlen üzenetek tartalmaznak, csak miután ellenőrizte a feladót!
- **Ne kapkodjon!** Szánjon rá időt és ellenőrizze az üzenetet, mielőtt válaszol!
- **Soha ne válaszoljon olyan szöveges üzenetekre**, amiben PIN kódot, online banki jelszót vagy más bizalmas adatot kérnek!
- Ha úgy érzi csaló üzenetre válaszolt és megadta banki adatait, **azonnal értesítse a bankot!**

HAMIS BANKI WEBOLDALAK

A pénzügyi adathalász e-mailek általában olyan linkeket tartalmaznak, amelyek hamis weboldalra irányítják, ahol a pénzügyi és személyes adatait kérik.

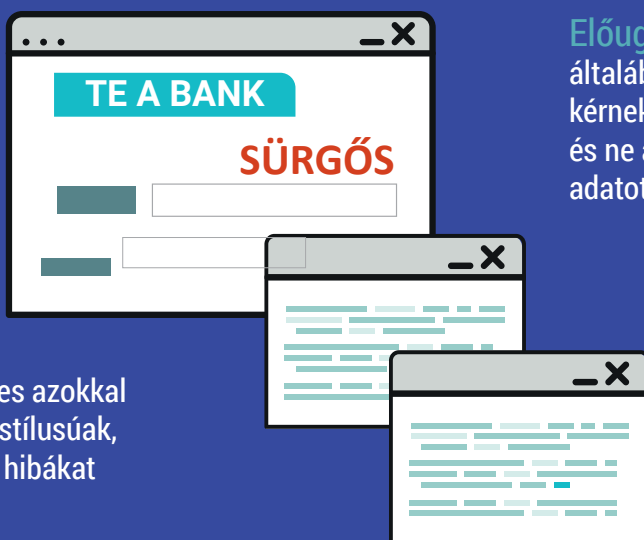


MIK AZ ÁRULKODÓ JELEK?

A hamis banki weboldalak nagyon hasonlítanak az eredetihez. Ezen weboldalak sajátossága az előugró ablak, amelyen banki adatokat kérnek. A valódi bankok nem használnak ilyen előugró ablakokat.

A hamis weboldalak jellemzői:

Sürgetés: a valódi weboldalakon nem kapunk ilyen üzeneteket.



Előugró ablakok: ezek általában bizalmas adatokat kérnek Önről. Ne kattintson rá és ne adjon meg személyes adatot az ilyen oldalakon!

Gyenge dizájn: legyen figyelmes azokkal a weboldallal, amelyek eltérő stílusúak, illetve helyesírási vagy nyelvtani hibákat tartalmaznak!

MIT TEHETÜNK?



Soha ne kattintson az e-mailben szereplő linkekre, amelyek a bank weboldalára irányítanak!



Mindig írja be saját kezűleg a link címét, vagy a kedvencek listából nyissa meg!



Használjon olyan böngészőt, amely blokkolja az előugró ablakokat!



Ha valami tényleg fontos az Ön számára, értesítést fog kapni róla, amikor belép az online bankjába!

BANKI VISHING TELEFONHÍVÁSOK

A 'vishing' (a Voice és a Phishing szavak kombinációja) olyan telefonhívást jelent, amikor a csalók valamilyen trükkel arra vesznek rá mászt, hogy adja meg személyes, pénzügyi vagy biztonsági adatait, vagy utaljon pénzt nekik.



MIT TEHET?

- > **Legyen óvatos** a kérértelen telefonhívásokkal!
- > **Írja fel a hívó telefonszámát** és mondja neki, hogy később visszahívja!
- > Hogy meggyőződjön arról kivel beszél valójában, **keressen rá a szervezet telefonszámára** és hívja fel őket!
- > **Ne hívja fel a telefonszámot, amit üzenetben küldenek Önnek** (valószínűleg a csalókhoz tartozik a telefonszám)!
- > A csalók néhány információt interneten is megtalálhatnak Önről (pl. közösségi média). **Ne gondolja, hogy a hívó nem csaló**, csak mert tud ilyen részleteket is!
- > **Ne adja meg** bankkártyája vagy hitelkártyája PIN kódját, sem online banki jelszavát! A bank soha nem kér ilyen adatot.
- > **Ne utaljon pénzt másik bankszámlára a kérésükre! A bank soha nem kér ilyet.**
- > Ha úgy érzi csaló telefonhívást kapott, **értesítse a bankot!**



BANK ACCOUNT HACKING

