



KEDVEZŐ AJÁNLAT ^{Vagy} KÉRDÉS?

Az online vásárlás arany szabályai

MEGBÍZHATÓ FORRÁSBÓL VÁSÁROLJON!

Válasszon olyan márkákat és üzleteket, amelyeket ismer!

GONDOLJA ÁT KÉTSZER, MIELŐTT FIZET!

Legyen tisztában az online vásárlás kockázataival!



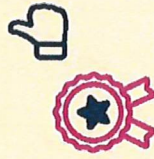
NE KÜLDJÖN PÉNZT ISMERETLEN SZEMÉLYNEK!

Ha az utcán nem adna pénzt egy ismeretlen személynek, ne tegye ezt az interneten sem! Ha lehetséges, először kapja meg az árut, utána fizessen!



ELLENŐRÍZZE A VÉLEMÉNYEKEKET ÉS ÉRTÉKELÉSEKET!

Különösen ismeretlen üzletek és egyéni eladók esetében.



ELLENŐRÍZZE AZ ISMÉTLŐDŐ DÍJAKAT!

Mielőtt megadná a bankkártyája adatait az interneten keresztül egy folyamatos szolgáltatás kifizetéséhez, tudja meg, hogyan mondhatja le a szolgáltatást!



HASZNÁLJON HITELKÁRTYÁT, AMIKOR ONLINE VÁSÁROL!

A legtöbb bankkártyát erős ügyfélvédelmi szabályzat övja. Ha nem kapja meg, amit megrendelt, a kártyakibocsátó bank megtéríti Önnek az árát.



SOHA NE KÜLDJE EL A BANKKÁRTYÁJA ADATAIT E-MAILLEN!

Soha ne küldjön másolatot a kártyájáról, a PIN kódjáról, vagy más kártyainformációról e-mailen!



GYŐZÖDJÖN MEG AZ ADATÁTVITEL BIZTONSÁGÁRÓL!

Használjon HTTPS és SSL protokollokat böngészéskor. Emlékezzen: a lakat szimbólum önmagában nem tesz egy honlapot törvényessé.



MENTSE EL AZ ÖSSZES, ONLINE VÁSÁRLÁSHOZ KAPCSOLÓDÓ DOKUMENTUMOT!

Ezekre szükség lehet az adásvétel körülményeinek megállapításához vagy annak igazolásához, hogy kifizette az árut.



NEM VÁSÁROL? NE ADJA MEG A KÁRTYADATAIT!

Ha nem vesz semmit, ne továbbítsa és ne mentse el a bankkártyaadatait!



ELLENŐRÍZZE A WEBOLDAL FIZETÉSI BIZTONSÁGÁT!

Csak olyan weboldalon vásároljon, amely teljes azonosítási rendszert használ (mint a Verified by Visa / MasterCard Secure Code)



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 pénzátutalásra 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 pénzátutalást kérnek.

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

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

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

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.

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!