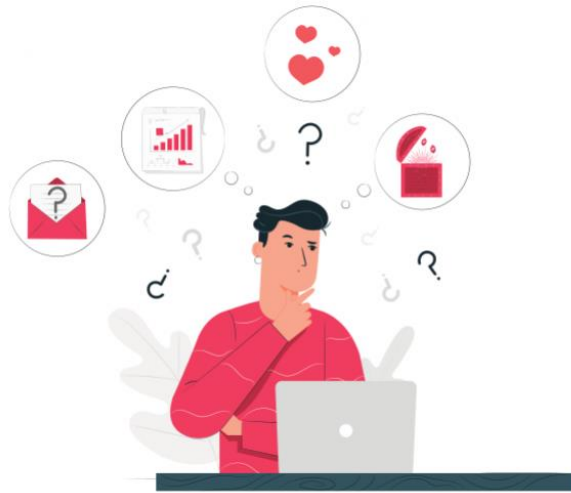


# CSALÁSOK A KIBERTÉRBEN

Az internet a számtalan előnye mellett veszélyeket is rejt a felhasználóknak. A bűnözők a valós élethez hasonlóan a kibertérben is megpróbálják megtéveszteni az embereket, hogy ezzel bevételre tegyenek szert. A személyes találkozás hiánya és az internet nyújtotta anonimitás jelentősen megkönnyíti a csalók munkáját! Az esetek egy részében közvetlenül az anyagi javak, más esetekben bankkártya vagy online banki adatok megszerzése a cél.



## **Romantikus csalás**

Az internetes társkeresőknek, randioldalaknak, appoknak és általában a közösségi oldalaknak köszönhetően a lehetőségek szélesre nyíltak a társat keresők előtt. A bűnözők is felismerték az ebben rejlő lehetőségeket. A csalók jellemzően az online párkereső oldalakon nézik ki célpontjaikat, de néha a közösségi oldalakon vagy e-mailben veszik fel a kapcsolatot.

### **Melyek a gyanús jelek?**

- Ha valaki rövid ismeretség után azt mondja, hogy odavan Önért vagy fülig szerelmes.
- Az üzenetek megfogalmazása semmitmondó, általánosságokat tartalmaz.
- A küldő online profilja nem egyezik azzal, amit magáról állít.
- Ha intim képeket vagy videót kér Öntől!
- Megpróbál a bizalmába férkőzni és rávenni arra, hogy küldjön neki pénzt, ajándékot vagy adja meg bankkártyája vagy netbankjának belépési adatait.

### **Hogyan előzheti meg, hogy áldozattá váljon?**

- 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 legismertebb 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 következetlenségekre és a kifogásokra, például, hogy a csalók kamerája nem működik!
- Ne osszon meg kompromittáló 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!

### **Mit tehet, ha áldozattá vált?**

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

## **Befektetési és kriptovalutákkal kapcsolatos csalások**

Hatalmas nyereséggel és gyorsan megtérülő befektetéssel kecsegető ajánlatokkal találkozhat a felhasználó a közösségi oldalakon küldött üzenetekben vagy e-mailekben, esetleg online hirdetésekben, felugró ablakokban.

- Az ajánlatok külföldi, vissza nem térő lehetőségekről, nyersanyagokról, értékpapírokról, kötvényekről, de leginkább a kriptovalutákról szólnak.
- A korábbi (sosem volt) hozamokat bemutatva próbálják meggyőzni a felhasználót, hogy éljen a csak rövid ideig elérhető lehetőséggel.
- Sok esetben az online ismerős, a saját pozitív példáján keresztül próbálja rávenni a kiszemelt áldozatot a befektetésre.
- Az ajánlatok mögött komoly szervezett bűnözői hálózatok állnak, akik teljes mértékben elhitetik az áldozatokkal, hogy egy valódi és legális befektetési tevékenységet végeznek.
- Ehhez weboldalakat hoznak létre, többek között a korábbi „hozamok” bemutatására és az ügyfélnek befektetéseinek ellenőrzésére, illetve telefonos és e-mailés ügyfélszolgálatot működtetnek.
- A pénzmozgás azonban csak egyirányú, a befektetett összeget a számlán lévő virtuális nyereség ellenére soha nem kapja meg az ügyfél.

### **Tanácsok**

- 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!
- Csak megbízható, leellenőrizhető befektetési szolgáltatót válasszon, olyat semmi esetre sem, amelyik ajánlata kéretlenül e-mailben vagy közösségi oldalon keresztül érkezett, vagy amelyiket online ismerőse ajánl.
- Értesítse a rendőrséget, ha csalásra gyanakszik!

### **Üzleti levél csalás**

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

- A csalók a cég magasszintű vezetőjeként telefonon felhívják az alkalmazottat, vagy e-mailt küldenek neki.
- Gyakran használják a 'Titoktartás', 'A cég bízik Önben!', 'Jelenleg nem vagyok elérhető' kifejezéseket.
- Azt mondják, hogy a részletes instrukciókat később tudatják vele, vagy egy harmadik személy küldi e-mailen.
- A kapott instrukcióknak megfelelően az ügyintéző a pénzt a csalók által kezelt bankszámlára utalja.

#### **Legyen gyanús, ha:**

- Közvetlenül egy olyan vezető keresi Önt, akivel eddig nem került kapcsolatba.
- Teljes titoktartást kér, nyomást, sürgetést, fenyegetés érez a részéről, esetleg a telefonáló szokatlanul kedves vagy jutalmat ígér.
- Arra kéri, hogy térjen el a megszokott ügyintézésről.

#### **Tanácsok cégvezetőknek**

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

### **Tanácsok alkalmazottaknak**

- 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 magán 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 a vezetőjének!

### **Nyereményjáték-csalások**

Az online nyereményjáték-csalásokkal a közösségi oldalakon keresztül küldött üzenetekben vagy e-mailekben, esetleg felugró ablakokon keresztül találkozhat a felhasználó. A csalók célja, hogy a felhasználótól pénzt csaljanak ki vagy megszerezzék a bankkártyájának vagy a netbankjának belépési adatait. Az elkövetők azzal keresik meg a kiszemelt áldozatot, hogy valamilyen nyereményjátékon nyert, de a nyeremény véglegesítéshez szükség van arra, hogy feltöltse egy telefonkártya egyenlegét vagy egy meghatározott kódot SMS-ben küldjön el egy telefonszámra (ez szintén egyenleget tölt fel a küldő számlájának terhére). Az is előfordul, hogy a nyeremény (pl. mobiltelefon, játékkonzol) átvételéhez egy kisebb összeget kell átutalni szállítási vagy kezelési díj címén. Más esetekben nem a díj átutalását kérik, hanem a bankkártya adatokat, azzal, hogy arról vonják le a díjat. Ez utóbbi esetben nem csak a jelzett összeget, hanem akár a teljes egyenleget is elkölthetik.

## **Tanácsok**

- Közösségi oldalon, e-mailben kapott vagy felugró ablakban megjelenő nyereményjátékkal kapcsolatban mindig legyen gyanakvó.
- Mindig ellenőrizze, a nyereményt biztosító cég honlapján vagy közösségi profilján, hogy valóban van-e ilyen nyereményjáték!
- A játékot szervezők a nyeremény átvételéhez szükséges adatokon kívül más adatokat, így különösen bankkártya, netbank belépési adatokat vagy pénz átutalását nem kérik.
- Személyes adatait csak a valódi, leellenőrzött játékokhoz kapcsolódóan, és csak a valódi szervező online felületén adja meg!
- Ellenőrizze a játékhoz kapcsolódó adatkezelési szabályzatot, vagyis, hogy mire használhatják fel az adatait, kinek adhatják át. A nyereményjátékok egy része az adatgyűjtést szolgálja, mivel az személyes és a kapcsolattartási adatok, mint az e-mail cím és telefonszám, jól értékesíthetők. Legyen tisztában ezzel, mielőtt megadja azokat!