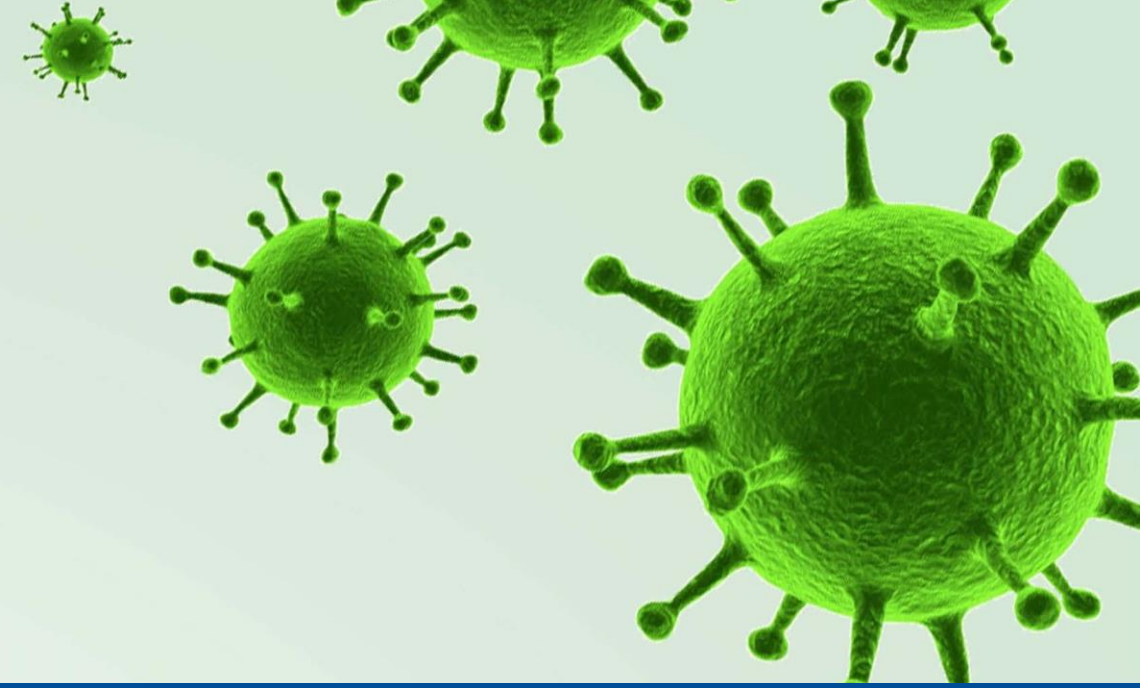


# COVID-19 visszaélések:
# Mit tehetünk ellene?

Habár a koronavírus elterjedése korábban sosem tapasztalt kihívások elé állított mindannyiunkat, a szervezett bűnözés meglepő gyorsasággal és kifinomultsággal reagált a hirtelen jött válsághelyzetre. Ebben a nehéz és bizonytalan időszakban nemcsak a világjárvány okozta félelemmel és szorongással kell tehát szembenéznünk: fontos, hogy tudatosítsuk ezt a kiszolgáltatott helyzetet kihasználó csalási technikákat – mind a magán, mind az üzleti életben.

Világszerte megjelentek a koronavírushoz köthető visszaélések – legyen szó a banki ügyfelek ellen indított támadásokról, a kijárási korlátozások és tilalmak okozta vagy a kétségbeesett bevásárlási láz kiaknázásáról. A gazdaságélénkítő csomagok bevezetése, valamint a munka nélkül maradtak megsegítése következtében a visszaélések száma aligha fog csökkenni a közeljövőben.

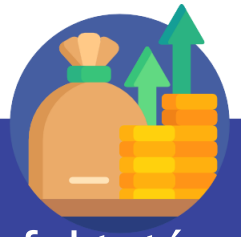
Gyanús linkek, csatolmányok érkeznek a telefonunkra, számítópünkre, hackerek próbálnak profitot kovácsolni a vírus iránti töretlen kíváncsiságból és a járvány miatti aggodalomból. A kártékony programokat koronavírusos tartalomba csomagolják annak érdekében, hogy azok telepítsék magukat és észrevétlenül működjenek tovább eszközeinken.

Néhány területen – különösen a pénzügyi szektorban, gyógyszeriparban és a távközlésben – számos azonnali kihívással kellett szembenézni az új helyzet következtében. Ezen iparágak szereplői már megtették az első lépéseket, és a megváltozott helyzetre reagálva dolgoznak az üzleti fenntarthatóságukon és a visszaélések elleni minél hatékonyabb védekezésen.

## Néhány jelenlegi és várható COVID-19 vonatkozású visszaélés:

Technológiai visszaélés

Fogyasztók megtévesztése



Befektetés és adományozás

## Hogyan tudjuk megvédeni magunkat?

Tudatosság

Prevenció

Visszaélések feltárása

# Néhány jelenlegi és várható COVID-19 vonatkozású visszaélés:

## Technológiai visszaélés

01

**Phishing:** Az elkövetők ismert egészségügyi szervezetek - mint például az Egészségügyi Világszervezet (WHO) - munkatársaiként tüntetik fel magukat, csatolmányt vagy linkeket küldenek emailen keresztül, melyek koronavírussal kapcsolatos oldalakra irányítanak át, új fejleményeket ígérve a vírus földrajzi adataival kapcsolatban vagy a megelőzést/gyógyítást illetően.

A csatolt fájlok vagy a linkek megnyitásuk után a használt eszközre (számítógép vagy telefon) kémprogramot, zsarolóprogramot, stb. telepítenek és különböző adatokat gyűjtenek be az eszközökről - főleg érzékeny személyes és bankkártya adatokat.

A fertőzöttek számának növekedésével megjelentek azok a csalók, akik helyi kórházak nevében keresik fel az áldozatok, azt állítva, hogy fertőzöttel érintkeztek. Ők szintén a csatolmányba rejtett kártékony tartalmakkal dolgoznak.

02

**COVID-19 Visszaélésre létrehozott website-ok:** A COVID internet domain regisztrációk a közelmúltban jelentősen megugrottak, jogos a gyanú, hogy számos esetben adathalászat céljával hozták létre őket. Ezek az ál-weboldalak valós szervezetek valódi oldalainak tűnnek, valójában viszont a rosszindulatú programok terjesztését szolgálják.

03

**Üzleti emailekkel történő visszaélések:** A koronavírusnak köszönhetően gyakorivá és természetesé vált home-office a csalóknak számos lehetőséget kínál, hogy megkörnyékezzék a cégeket és munkavállalókat. COVID-19 híreknek álcázott emailekkel veszik rá az alkalmazottakat, hogy megadják céges hozzáférési adataikat - olykor COVID tartalmú céges álportálokat üzemeltetve. Ha a munkavállaló megadja az adatokat, a csalók szabadon böngészhetnek az áldozat számára elérhető céges hálózatokban.

04

**Zsarolóprogramok:** Mivel a kijárási korlátozások és tilalmak idején természetessé vált az otthonról történő munkavégzés, így a zsarolóprogramok használatában minden bizonnyal fellendülésre számíthatunk. Ezek a programok a szervezetek IT rendszereinek megbénítását veszik célba, „váltságdíjért" cserébe.

Az ilyen típusú támadások során – mellyel egyre gyakrabban kell szembenézni az állami intézményeknek és kereskedelmi szervezeteknek – a zsarolóprogram lezárja az operációs rendszert és a felhasználói fájlokat, elérhetetlenné teszi őket, a feloldásukért pedig súlyos összegeket követelnek a támadók – általában bitcoinban igényelve a fizetést.

05

**Egyéb mobiltelefonos visszaélések:** Az elkövetők applikációkat fejlesztenek – vagy már meglévőket manipulálnak, melyeken látszólag a koronavírus terjedését lehet lekövetni. Valójában az applikáció a telepítés után rosszindulatú programmal fertőzi meg az eszközt és megkezdi a személyes adatok, bankkártya információk, stb. begyűjtését.

# Néhány jelenlegi és várható COVID-19 vonatkozású visszaélés:

## Vásárlói megtévesztések

01

**Online oktatási alkalmazások:** Az iskolák és egyetemek bezárása következtében megnövekedett az érdeklődés az online oktatási platformok iránt – ezzel együtt a csalók is proaktívan fordultak e terület felé. Ismert oktatási platformok képviselőiként bemutatkozva keresik fel az áldozataikat, engedmények ígéretével veszik rá őket, hogy az általuk küldött linkeket megnyitva jelentkezzenek kurzusokra.

02

**Online kereskedelmi visszaélések:** Kihasználva a jelenleg tapasztalható áruhiányt és az általános félelmet, több online kereskedelmi platformot hoztak létre olyan keresett termékek értékesítésére, mint egészségügyi maszkok, kézfertőtlenítő.
A számla kiegyenlítése után azonban a vásárlók sosem kapják kézhez a termékeket, az ál-webshopok üzemeltetői eltűnnek a pénzzel.

03

**Gyógyszer és egyéb egészségügyi termékek hamisítása:** Mivel a kínálat nem győzi követni a keresletet pár alapvető egészségügyi termék esetében, nagy a valószínűsége, hogy hamisított gyógyszerek vagy egyéb egészségügyi eszközök (maszkok, fertőtlenítőszerek) kerülnek a webshopokba. A nem szakértői szem aligha tud különbséget tenni az utánzat és az eredeti között, így könnyen a hamisítók áldozatául esnek.

04

**Teszteléssel és kezeléssel kapcsolatos visszaélések:** A vírust övező pánik következtében sokan szeretnének olyan tesztelési lehetőségekhez jutni, amivel elkerülhetnék a pozitív teszt esetén kötelező kórházi karantént vagy egyáltalán minden kórházi jelenlétet. Szintén hatalmas az érdeklődés a gyógymódok, védőoltások iránt.
A közösségi médián és egyéb online fórumokon keresztül a csalók olyan teszteket, védőoltásokat, egyéb gyógymódokat kínálnak, melyek hatása, érvényessége egyáltalán nem bizonyított és nincsenek engedélyezve.

05

**Egészségügyi szolgáltatásokkal kapcsolatos visszaélések:** Az elkövetők orvosnak vagy más egészségügyi dolgozónak, adminisztrátornak adják ki magukat és kezelést ígérnek, vagy arra hivatkozva kérnek pénzt, hogy sikeresen kigyógyítottak egy rokont vagy közeli barátot. Utóbbi eset különösen az idősebbeket megcélzó, úgynevezett „unokázós" csalók körében jellemző.

# Pár jelenlegi és várható COVID-19 vonatkozású visszaélés:

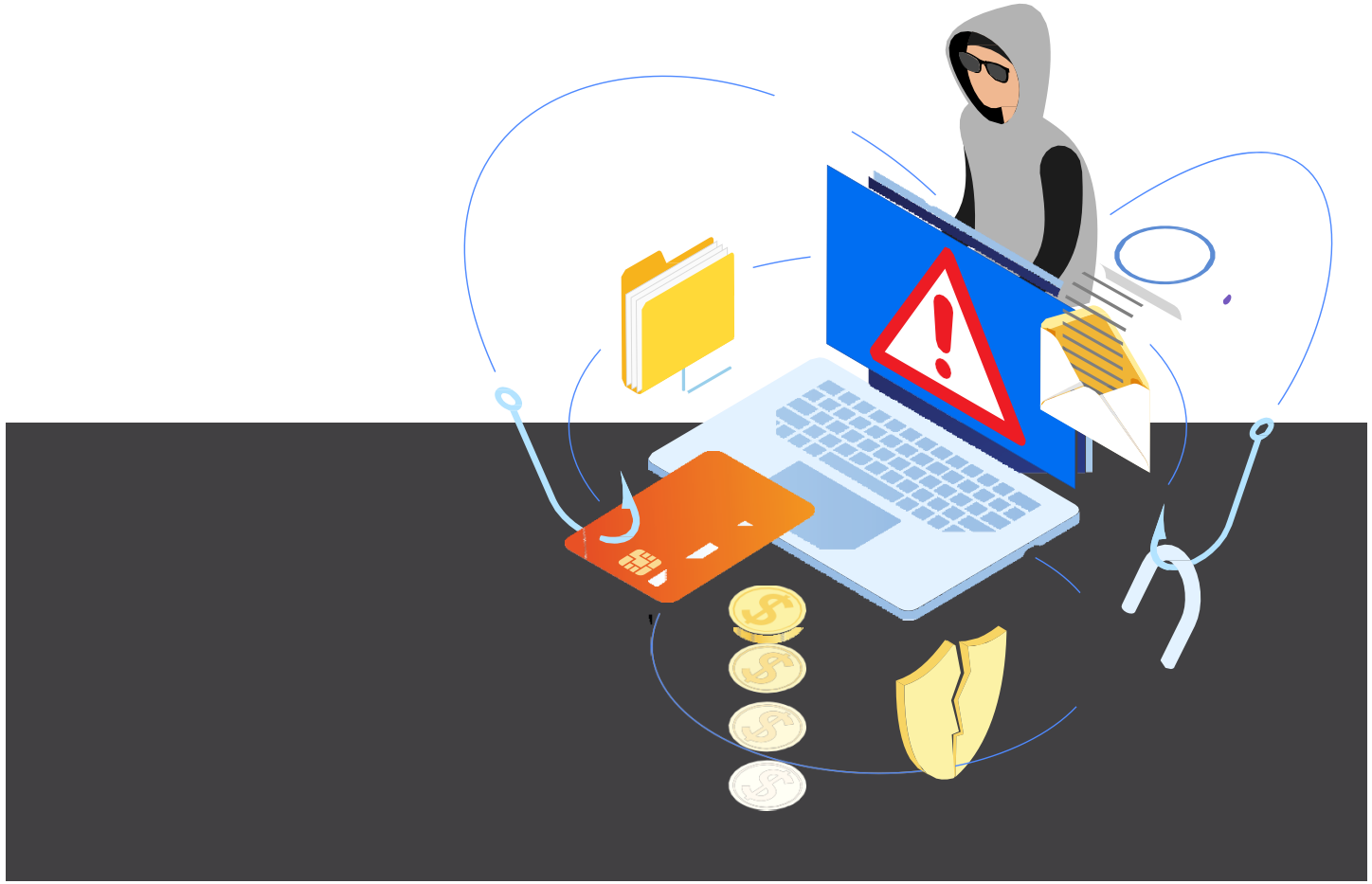
## Befektetés és adományozás

01

**Jótékonysági visszaélések:** Egy ilyen súlyos krízishelyzetben sok emberben felébred a személyes felelősség érzése a közösség és a rászorultak iránt. A csalók épp ezeket a közösségi érzelmeket veszik célba, amikor ismert szervezetek képviselőinek adják ki magukat vagy nemlétező szervezeteknek gyűjtenek, a vírusnak különösen kitett áldozatok vagy a vírus elleni vakcina fejlesztésére hivatkozva.

02

**Befektetési csalások:**
A klasszikus befektetési csalások mintáját követve, az elkövetők szokatlanul magas hozamokat ígérnek, a befektetésre javasolt cégek állítólag előrehaladott kutatásokat folytatnak a vírussal kapcsolatban, gyógyítással és prevencióval kapcsolatos szolgáltatásokat kínálnak.



# Hogyan tudjuk megvédeni magunkat?

## Tudatosság

**Számos dolgot tehetünk azért, hogy megvédjük magunkat, szeretteinket vagy cégünket attól, hogy a COVID-19 visszaélések áldozatává váljunk. A legfontosabb, hogy tudatában legyünk annak, milyen módon igyekeznek a saját hasznukra fordítani a világjárványt a visszaélések elkövetői.**

01

Legyünk óvatosak az emailekkel, melyek magukat szakértőnek feltüntető ismeretlen személyektől érkeznek, fontos információkat ígérve a vírusról. Ne nyissunk meg linkeket és csatolmányokat, ha ezeket ismeretlen feladóktól kaptuk. Ellenőrizzük az email címeket az ilyen tartalmak esetén, mint más kéretlen emailek esetében is, különösen figyeljünk a gépelési hibákra és a szokatlan karakterekre. A csalók általában olyan címeket használnak, amik csak pár karakterben térnek el a valós, ismert szervezeteknek címétől.

02

A visszaélésekre létrehozott online kereskedések sokszor szokatlan fizetési módokat alkalmaznak, mint például a pénzutalvány, kriptodeviza, ajándékutalvány, pénzátutalás. Ne kattintsunk rá az emailben küldött fizetési parancsikonokra, csak biztonságos szolgáltatók platformjain keresztül indítsunk utalást, kártyás vásárlást. A legtöbb banknál elérhető a virtuális bankkártya szolgáltatás, ennek köszönhetően nem kell az alap kártyaadatainkat megadnunk. Amint észrevesszük, hogy visszaélés történt (például nem történt meg a kiszállítás), azonnal jelezzük a bankunknak a gyanút, így letilthatják, hogy az álkereskedő leemelje a pénzt.

03

Adományozás előtt nézzünk utána a fogadó szervezetnek és aktuális kampányainak. Különösen óvatosan bánjunk azokkal a kéretlen jótékonysági emailekkel, melyek szokatlan, nem biztonságos fizetési úton keresztül igényelnek adományokat.

04

Tájékozódjunk a befektetési csalásokat, trendeket illetően – különösen ha a befektetés tárgyát képező cég online tartalommegosztással és a COVID-19-cel kapcsolatos kutatásokkal foglalkozik. A kiemelkedően magas hozamot ígérő befektetések minden körülmények között gyanúsak. Szintén árulkodó jel, ha a kezdeményező fél próbálja sürgetni a döntést.

05

Bizonyosodjunk meg arról, hogy csak olyan webshopról rendelünk gyógyszert, mely rendelkezik gyógyszerkereskedelmi engedéllyel (ellenőrizzük az OGYÉI listáját: https://www.ogyei.gov.hu/internetes_gyogyszer_kereskedelem/ ), és még ezekben az esetekben is fontos ellenőrizni a termék összetevőit, gyártóját, lejáratát. Házilag elvégezhető gyorsteszt jelenleg nem elérhető az országban, így az ilyen tesztek érvényességében nem érdemes reménykedni.

# Hogyan tudjuk megvédeni magunkat?

## Prevenció

01

Gondoskodjunk az IT környezet védelméről és ellenőrzéséről, a hozzáférési jogosultságok megfelelő kialakításáról. A szerver és a hálózat teljesítményét monitorozzuk és állítsunk be alerteket.

02

Figyeljünk a jelszavak minőségére - legyen mindenhova más jelszavunk, ezeket sűrűn cseréljünk. Ha nem akarjuk őket megjegyezni, használjunk megbízható gyártótól származó jelszókezelő alkalmazást, mely helyettünk biztosítja a jelszavak megfelelő minőségét. Cseréljük le a szolgáltató által megadott alapértelmezett wifi jelszót, ha még nem tettük volna meg. Használjunk többlépcsős azonosítást IT eszközeinken és azokon az oldalakon is, ahol nem kötelező, de van rá lehetőség.

03

Biztosítsuk az operációs rendszer, antivírus programok frissítését az eszközökön. Kerüljük az ingyenes szoftverek telepítését, mert ezek potenciális hordozói a rosszindulatú programoknak.

04

Felhasználónevet, vagy jelszót, illetve bármilyen adatot kizárólag SSL tanúsítvánnyal ellátott weboldalon (https:// kezdetű URL, vagy bizonyos böngészőben kis lakat jel az URL-től balra) adjunk meg.

05

Biztonságos hálózatokon keresztül csatlakozzunk az internethez munkavégzés közben– ha lehetséges, virtuális magánhálózaton (VPN) keresztül. Kerüljük el a nyilvánosan elérhető fájlmegosztó oldalak használatát.

# Hogyan tudjuk megvédeni magunkat?

## Visszaélések feltárása

01

Figyeljünk fel minden hibára, adatsérelemre, balesetre, mivel még a kisebbek is nagyobb problémák előjelei lehetnek.
Kibertámadás esetén derítsük fel, honnan indult a probléma, hogy megelőzzük a jövőbeni eseteket.

02

Jelentsük a visszaéléseket az illetékes hatóságoknak (pl. fogyasztóvédelem), hogy mielőbb megtalálják és leállítsák a csalókat.

# Kapcsolat:


**Beer Gábor**
Vezérigazgató helyettes,
Üzleti tanácsadás vezető

KPMG Tanácsadó Kft.
H-1134 Budapest, Váci út 31.

T: +36 1 887 7329
M: +36 70 333 1436
E: Gabor.Beer@kpmg.hu



**Taksz Ildikó**
Partner, Üzleti tanácsadás

KPMG Tanácsadó Kft.
H-1134 Budapest, Váci út 31.

T: +36 1 887 4144
M: +36 70 708 0023
E: Ildiko.Taksz@kpmg.hu



**Kórász Tamás**
Partner, IT tanácsadás

KPMG Tanácsadó Kft.
H-1134 Budapest, Váci út 31.

T: ++36 1 887 7322
M: +36 70 333 1507
E: Tamas.Korasz@kpmg.hu



**Kaszap András**
Igazgató, Forensic
szolgáltatások

KPMG Tanácsadó Kft.
H-1134 Budapest, Váci út 31.

M: +36 70 370 1840
E: Andras.Kaszap@kpmg.hu

**kpmg.com/socialmedia**


**kpmg.hu**