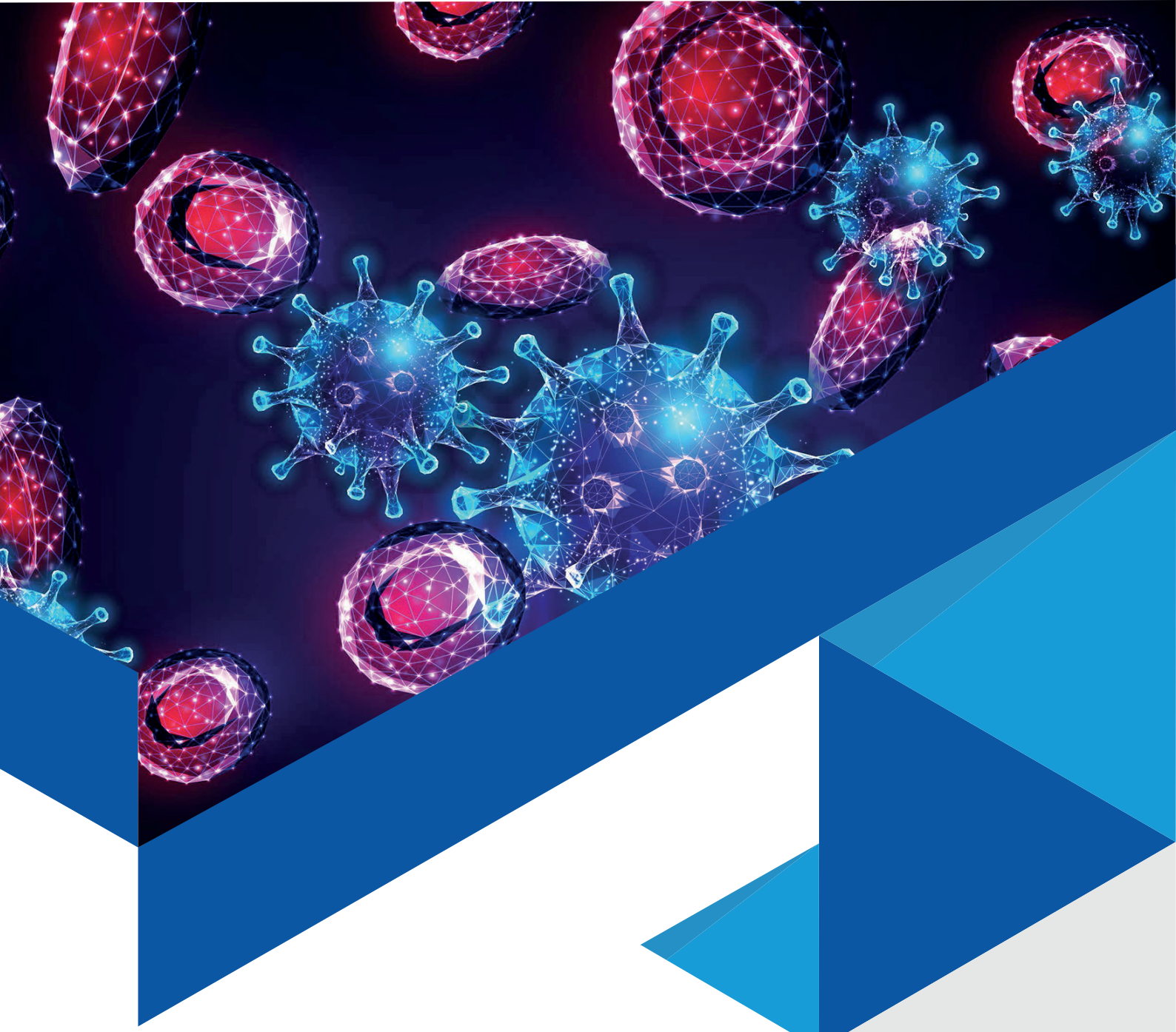
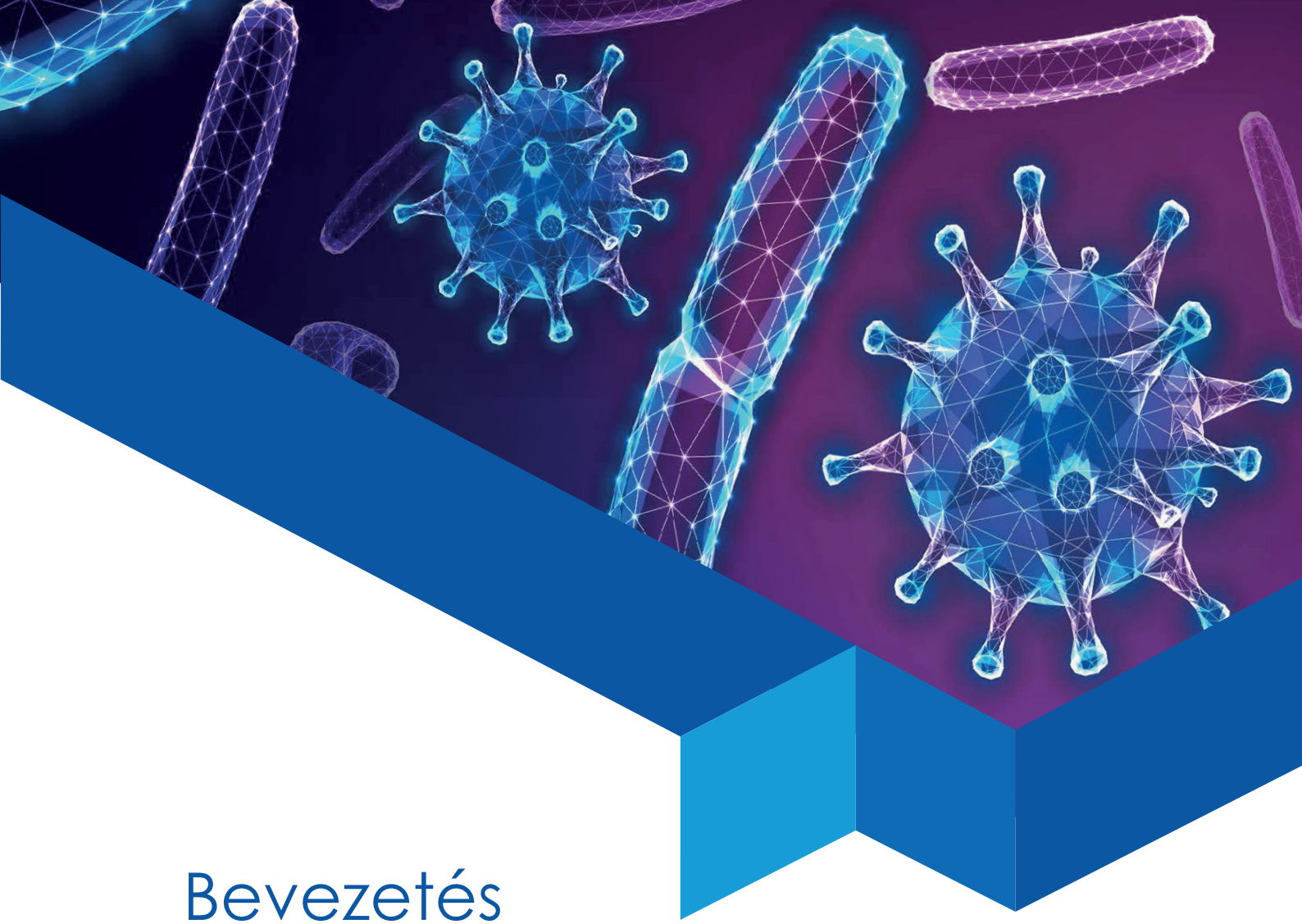


CTI jelentés

Kibertámadások a koronavírus árnyékában

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET



Bevezetés

A kiberbűnözők a koronavírus miatt kialakult helyzetet különféle támadási módszerekkel próbálják kihasználni. A támadók az emberek fokozott érdeklődésére épített megtévesztő technikákat alkalmaznak, amelyek a közeljövőben is megfelelő alapot jelenthetnek számukra a pandémiás helyzetet felhasználó támadásaik során.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet nemzetközi partnereivel együttműködve folyamatosan figyelemmel kíséri a globális kibertérben zajló, **új koronavírussal összefüggő online támadásokat és fenyegetési trendeket**. A megelőző intézkedések ezen időszak során is kiemelt fontossággal bírnak. Az alábbiakban csoportosítva, képekkel szemléltetve soroljuk fel az említett átverések típusait, és részletezzük jellegzetességeiket.

Vezetői összefoglaló

A dokumentum célja, hogy ismertesse az olvasóval a 2020 elején kialakult világjárványhoz kapcsolódó bűnözők által interneten használt és terjesztett átverési technikákat. Mivel a **pandémia miatt** sokak élete szinte csak az **internetes közegben** folyatódott tovább, ezeket a lehetőségeket megragadva, a **kiberbűnözők** soha nem látott mennyiségben kezdték el használni a **hamis weboldalakat**, különböző **valótlan üzenetek elküldését**, akár **hamis gyógyszerek árusítását**. A dokumentumban kategóriánként, illetve témakörönként bemutatásra kerülnek a kiberbűnözők által használt **módszerek**, részletes leírásuk és az adott átveréshez kapcsolódó **ajánlott óvintézkedések** és tanácsok is. Fontos kiemelni, hogy a képek hiteles forrásokból származnak, eredeti átveréseket és pénzszerzési módszereket ábrázolnak, a jobb érthetőség és a későbbi felismerés érdekében.

A leggyakoribb csalási technikák:

- **Covid témájú állami intézményeket célzó támadások**: Ebben az esetben a bűnözők célirányosan állami intézményeket, és azok munkatársait támadják, illetve próbálnak meg átverni. Jellemzően információ- és az anyagi haszonszerzés az elsődleges céljuk. Ezt különböző hamisított levelekkel és weboldalakkal, illetve zsarolóvírussal próbálják meg elérni.

Megtévesztő levelek, álhírek, közösségi média-üzenetek: A vírushelyzet jelenléte óta a különböző álhírek, pánikkeltő képek, üzenetek elterjedése fokozottan megnőtt. Az üzeneteket általában valamilyen nemzetközi szervezet nevében (pl.: WHO) küldik. Előfordulhatnak olyan levelek amelyekben adathalász tevékenységet folytatnak és különböző érzékeny adatok megadására próbálják rávenni a felhasználót.

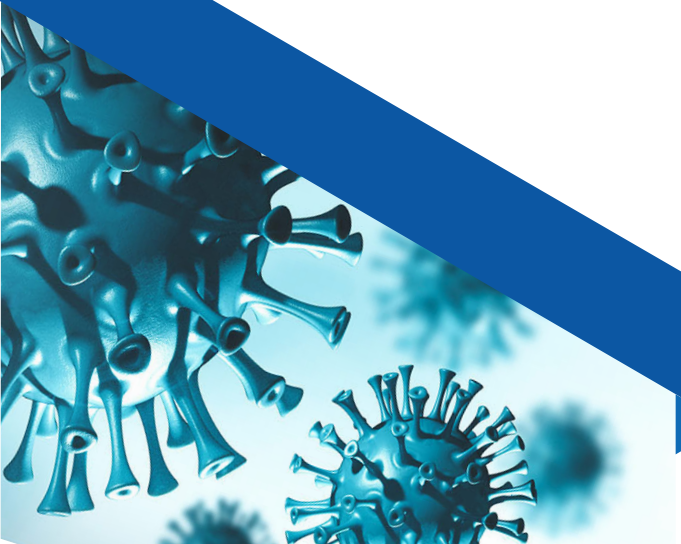
Koronavírus témájú mobilalkalmazások: Számos olyan alkalmazás jelent meg amely azt ígéri, hogy a koronavírussal kapcsolatos híreket, adatokat, térképeket tudunk megtekinteni. Ezzel általában valamilyen káros hatású programot telepítünk készülékünkre. Fontos, hogy csak megbízható áruházból és ellenőrzött applikációt telepítsünk.

Koronavírussal kapcsolatos weboldalak: Számtalan olyan honlapot, illetve webshopot hoztak létre a csalók, amellyel érzékeny információkra és anyagi haszonra tudnak szert tenni. A jelenlegi helyzet miatt, sok esetben olyan tisztítószereket, gyógyszerek és gyógymódokat hirdetnek melyek elpusztítják a vírust. Fokozottan figyeljünk az ilyen oldalakra, semmiképp se vásároljunk és adjuk meg adatainkat. Csak ellenőrzött weboldalakat használjunk, mielőtt belépünk egy hasonló oldalra, keressünk rá az interneten. Nagy esély van rá, hogy már más is találkozott az éppen hiteles vagy hamis weblappal.

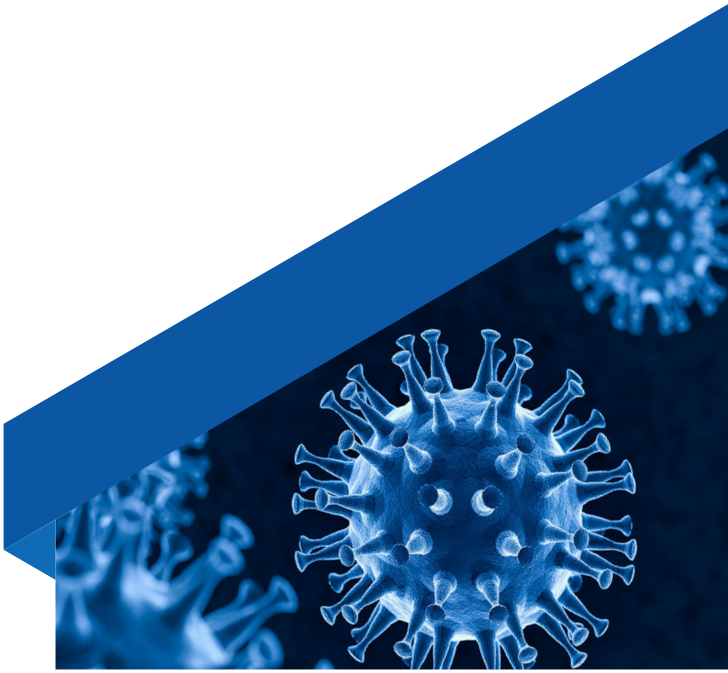
Pénzügyi csalások: Óvakodjunk a koronavírussal kapcsolatos befektetési ajánlatoktól, leginkább azoktól, amelyek a vírus ellenszerét hirdetik. Előfordulhat, hogy a helyi adóhatóság nevében küldenek az áldozatoknak leveleket, amelyekben megpróbálnak pénzügyi információkra szert tenni.

Pénzmosás: A bűnözők a vírushelyzetet kihasználva, álláshirdetéssel kereshetik meg a felhasználókat. A munkát általában az otthonról végezhető, biztonságos és egyszerű címszavakkal hirdetik. Ez általában valamilyen pénzmozgatással kapcsolatos tevékenységeket takar, legtöbbször a munkavállaló tudta nélkül. Gyakran adományként álcázzák a mosásra váró összegeket.

Online oktatási alkalmazások: Mivel nagyban megnőtt az otthon tanulók aránya, ezért a bűnözők is jobban odafigyelnek ezekre a területekre. Csaló leveleket kaphatunk, hogy felfüggesztették valamilyen oktatási platform fiókunkat. Minden esetben győződjünk meg a levél hitelességéről, ha nem vagyunk biztosak, akkor a gyártó eredeti oldalon végezzük el a számunkra szükséges műveleteket.



Tartalomjegyzék



Covid témájú állami támadások a világban - nemzetközi kitekintés -

A digitális eszközök egyre elterjedtebb alkalmazásával és az alig vagy nagyon gyengén védett otthoni hálózatokból történő munkavégzéssel a Covid-19 pandémia remek bemutatója annak, milyen **intézkedéseket** kellene hoznunk az **IT eszközök és infrastruktúra védelmében**. Például a frankfurti központú DE-CIX internet-exchange központ 2020 márciusában a központ életében rekordméretű, 9,1 Terabit forgalmat mért másodpercenként, köszönhetően az országokat érintő korlátozásoknak és a kötelező home office bevezetésének.

1. ábra: Egyesül királyság nemzeti kiberbiztonsági központ (NCSC) figyelem felkeltő plakátja

Ebben a helyzetben a kiberbűnözés jelentősen kihasználja a helyzetből fakadó **bizonytalanság érzését** és az emberek **információ-éhségét**. 2020 áprilisában egy Németországban kiadott tájékoztatás szerint jelentős növekedést tapasztaltak a koronavírussal kapcsolatos visszaélésekben. Ugyanebben a hónapban a nyugatvesztfáliai gazdasági minisztérium beszüntette a gyorssegély folyósítását az egyéni vállalkozók részére a sorozatos visszaélések miatt, melyet a bűnözők hamis weboldalak segítségével gyűjtött adatok alapján saját részükre igényeltek meg.

Az Egyesült Királyság Nemzeti Kiberbiztonsági Központjának (NCSC) jelentése szerint, 2019 szeptembere és 2020 augusztusa közötti időszakban az **incidensek számában 10%-os növekedés** volt megfigyelhető, illetve az incidensek **több mint negyede köthető a koronavírus témaköréhez**. A szervezet számos olyan hamis kampányt akadályozott meg, amelyek a koronavírushoz kapcsolódó témákkal hívták fel az emberek figyelmét. Ezek közé tartoznak a rosszindulatú szoftverek, hamis linkeket tartalmazó levelek, sőt olyan webshopok amik hamis védőeszközöket, COVID teszteket, akár vakcinákat is árultak. Megjelentek az oltásellenes kampányok, amik nem csak a félretájékoztatást segítik elő, hanem a különböző alternatív gyógymódok és orvosi terápiák terjedését is.

Az intézet figyelmezeti a felhasználókat arra, hogy a **zsarolóvírus támadások is gyakoribbá váltak**. Az előző évhez képest háromszor több esetet kezeltek ebben a témában. A megfigyelések szerint ezek a támadások egyre **célzottabbak** és **agresszívabbak** lettek, gyakran most már nem a felhasználó adatainak lezárásával, hanem a kényes információk nyilvánosságra bocsátásával zsarolják az áldozatokat. Példaként lehet említeni, az egyes szervezeteknél dolgozók béreinek online közzétételét.

Egy másik esetben az amerikai Johns Hopkins Egyetem nevével visszaélve ígértek valós információkat a pandémia terjedéséről a csalók egy Android applikáción keresztül. Az alkalmazás letöltésével azonban egy malware települt a telefonra.

Kiemelt célpontok lettek az **egészségügyi infrastruktúra** intézményei is. 2020 március 13.-án a Brno Egyetemi Kórház (Csehország) kényszerült részleges leállásra, miután a belső számítógépes rendszerük zsarolóvírus áldozata lett.

A **működő vakcina** és annak összetevői, illetve az előállítási adatok nagyon **értékes szellemi tulajdont képeznek**. A gyógyszerkészítményen túl, akár az egyes hatóanyagok tesztelése és annak körülményei is meghatározóak lehetnek egyes szervezetek számára. Mivel néhány országban nagy kihívást jelent egy hatásos vakcina kidolgozása, ezért ezek az adatok megfelelő célpontok lehetnek a kiberbűnözők támadásai során. A **támadók** valószínűleg vagy állami szférában, vagy **állami szponzorálással dolgoznak**. Ezzel olyan erőforrásokat tudnak kihasználni, amelyek által komoly előnyre tesznek szert, a támadott vállalatokkal szemben.

Az egészségügyi és kutatóintézeteknél a szellemi tulajdon védelmének követelményei miatt, **megnövelt szintű biztonsági intézkedéseket** kell betartani. A támadások azonban üzleti partnereket és harmadik feleket is megcéloznak, amelyek **biztonsága alacsonyabb** lehet az egyes szervezetek **beszállítói láncában**.

Az egész világ a vírussal versenyez, hogy az adott ország lakosságának beoltása, minél hamarabb megtörténjen, mielőtt a vírus még több embert megfertőzne. Minél gyorsabban oltják be a lakosságot, annál gyorsabban tud visszatérni a gazdaság a normál kerékvágásba. Néhány nemzet számára a verseny megnyerése egyben előrelépést is jelent a versenytársnak tekintett országokkal szemben. Ez a folyamat nem csak gyorsasággal, hanem a többi résztvevő lelassításával is véghez vihető. Az utóbbi időben számos egészségügyi intézményt ért zsarolóvírus támadás, amivel a fentebb leírt hatást lehet elérni. A bűnözők mellet az **államilag támogatott szereplők (APT)** is működnek a kibertérben, politikai előnyökre, aktuális információkra a koronavírus terjedésével kapcsolatban vagy lehetséges gyógymódok után kutatva. Számos ilyen támadásról esett szó a 2020-as évben, köztük a WHO ellen indított adathalászati kampányról, vagy a kínai kémprogram kampányról melynek vietnámi, mongol és fülöp-szigeteki kormányhivatalok voltak a célpontjai.

Remek példa hasonló esetre a 2020-as év áprilisi **Zoom botránya**, amikor a brit és német kormányzati megbeszélések során fény derült a programban található számos súlyos titkosítási hiányosságra.

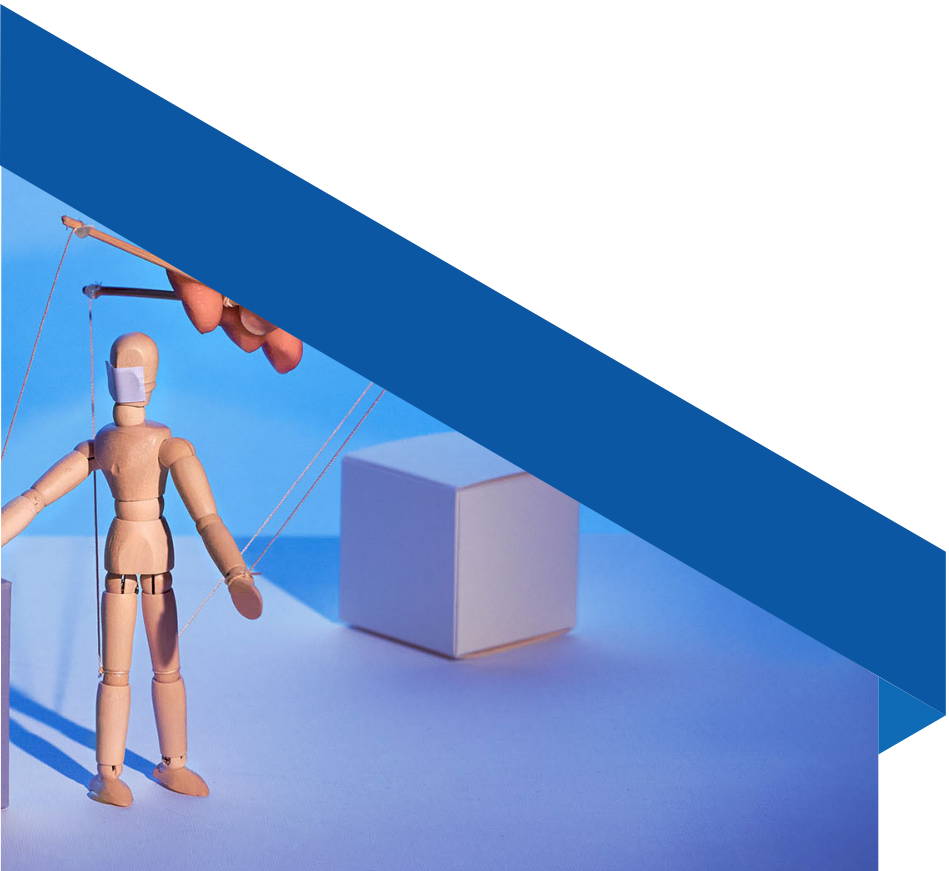
Az észak-koreai állam által támogatott **hackerek próbálták megszerezni a Pfizer covid vakcina technológiáját**, a Pfizer gyógyszergyártó cég elleni kibertámadás keretein belül. A dél-koreai hírszerzés szerint a vakcina összetevőit, illetve kezelési technológiáit próbálták meg ellopni, azonban a dél-koreai állam több információt nem árult el az esetről, többek között azt sem, hogy a támadások sikeresek voltak-e vagy nem. Észak-Korea eddig nem jelentett koronavírus esetet, aminek hitelességét egészségügyi szakértők erősen megkérdőjelezik. A tervek szerint Észak-Koreába kétmillió adag, az AstraZeneca és az Oxfordi Egyetem által közösen fejlesztett vakcinát fognak szállítani a COVAX program keretein belül ebben az évben. Dél-Korea szerint, több korábbi támadás is köthető Észak-Koreához, ezek is a Covid-19 elleni vakcinák kutatásában és fejlesztésében résztvevő szervezetek ellen irányultak. A több hónapra visszanyúló támadásokat számos, hamisított online portál bejelentkezési felületével eszközölték, így kicsalva a szervezet munkatársainak jelszavait. Általánosan tanácsolható az olyan szervezetek, vállalatok számára, melyek bármilyen kapcsolatban állnak a COVID vakcinával, hogy **ellenőriztessék a biztonsági rendszereiket** és ha szükséges **javítsák**, bővítsék azokat! A Covid-19 pandémia remekül bemutatta, mely intézmények és szervezetek kritikusak egy válság idején. Mint tapasztalhattuk, nem elég ezeket intézményi szinten megvédeni, hanem **állami és nemzetközi kereteken belül is szükséges fokozni a védekezést**.

Megtévesztő levelek, álhírek, közösségimédia-üzenetek

Amióta a koronavírus mindennapi életünk részévé vált, azóta folyamatos az álhíreket (fake news, hoax) és káros programokat terjesztő **adathalász (phishing) kampányok** jelenléte. Ezek sok esetben nemzetközi szervezetek (pl. a WHO, egy-egy ország egészségügyi minisztériuma) nevében íródott levelek, amik **érzékeny személyes adatok megszerzésére készített káros programokat terjesztenek**. Ugyanakkor a csalók – a pánikhelyzetet, és az emberek kíváncsiságát kihasználva, már célzott adathalász módszerekkel is igyekeznek rávenni az áldozatot pénzátutalások indítására, szenzitív — például banki — adatok megadására. A nemzetközi és a hazai közegészségügyi, járványügyi intézmények, kormányzati szervek nem küldenek a fentiekhez hasonló információkat e-mailen keresztül, nem kérnek be érzékeny adatokat, és nem kérik bejelentkezési azonosítók megerősítését, megváltoztatását.

A csalók a pandémiára építve és a leendő áldozatok hiszékenységét és jóindulatát kihasználva, **e-maileken keresztül** próbálnak **adathalász** tevékenységet, illetve **zsarolóvírus** kampányt folytatni és megtéveszteni a felhasználókat, vagy káros kódokat, programokat juttatni eszközeikre.

A csaló levelek jellemzően valamilyen **hamis hírrel keltik fel a figyelmet**, például a vírus ellenszerével kapcsolatos nagy áttörésről, alternatív gyógymódokról, egészségügyi eszközök hiányáról és beszerzésének lehetőségeiről, fontos biztonsági intézkedésekről számolnak be, vagy azzal igyekeznek pánikot kelteni, hogy a vírus az adott településen is felütötte a fejét. Ezek a csaló levelek azonban különböző **káros kódokat tartalmazó csatolmányokat**, vagy **káros webhelyekre mutató hivatkozásokat** tartalmazhatnak, amelyek szenzitív – például pénzügyi – információk megszerzésére irányulnak.



Példák csaló e-mailekre

A regisztráltak részére ingyenes védőeszközök kiosztását ígérik Müller Cecília nevében, valójában azonban adathalászati tevékenység áll a héttérben. Megfigyelhető a nem szokványos megszólítás, a magyartalan megfogalmazás, a magázás és a tegeződés keveredése, a sürgető megfogalmazás és a hivatalos szervezetek elérhetőségének hiánya, illetve az indokoltalan mellékletek jelenléte.

Válaszcím: Muller.Cecilia@nnk.gov.hu

NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT

Állami Népegészségügyi és Tisztiorvosi Szolgálat

Kedves mindenkinek,
A magyar kormány által kiadott covid-19 válaszadási utasítások szerint mi, a Magyar Nemzeti Egészségügyi Központ a covid-19 védőeszközöket ingyenesen kívánjuk eljuttatni a magyarországi összes regisztrált vállalathoz és iparághoz. Kérjük, töltse ki egyértelműen a mellékelt űrlapot. győződjön meg arról, hogy az alkalmazottak száma és a cég címe egyértelműen meg van írva ebben a formában.

Töltse ki a mellékelt űrlapot, és a mai bezárás előtt küldje vissza nekünk a másolatot, várva a gyors választ.

Az összes kitöltött nyomtatványt erre az e-mailre kell küldeni: Müller.Cecília@nnk.gov.hu

Szia

- Dr. Müller Cecília
- osztályvezető
- Országos Tisztifőorvos
- NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT
- 1097 Budapest, Albert Flórián út 2-6.
- Müller.Cecília@nnk.gov.hu

Covid-19 megelő...ek.ppt Jelentkezési lap a covi-...ára.pot

A lenti levéllel bankszámlával kapcsolatos adatokat próbáltak meg kicsalni. Itt is szemet szúrhat a - láthatóan gépi fordítással készült - szöveg, a furcsa megszólítás, továbbá sem az e-mail küldője, sem a vállalat, ahonnan küldte nem beazonosítható.

Jó reggelt uram,

A (COVID-19 vírus) széles körű elterjedésére vonatkozó jelenlegi körülmények miatt:
Óvintézkedésként megpróbáljuk minimalizálni a közvetlen személyes kapcsolatot,
Ennek megfelelően a papíralapú ellenőrzések felszabadítását a banki átutalással helyettesítjük,
Felkérjük, hogy küldje el bankszámlaadatait a csatolt űrlapon, aláírva és lepecsételtítve.

Ha bármilyen kérdése van, kérjük, ne habozzon kapcsolatba lépni irodánkkal.

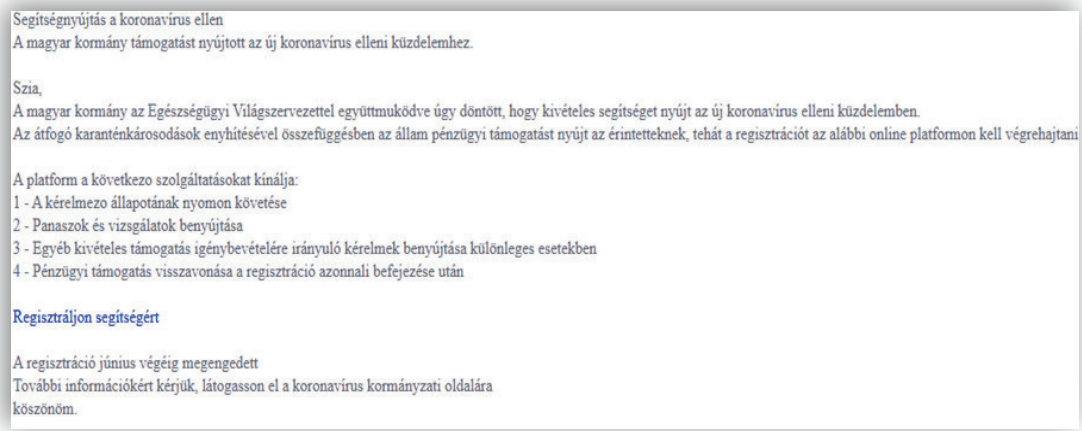
Dániel Majtényi
Pénzügyi / Számviteli Osztály
H-2040 Budaörs, Budapark, Keleti 4.

Hungary

+36 23 885 155

+36 707745074

Újabb csaló e-mail, ami a magyar kormány nevében ajánl fel pénzügyi segítséget. Árulkodó jel a nem hivatalos megszólítás egy hivatalosnak tűnő levélben, valamely kormányzatra, kormányzati intézményre vagy nemzetközi szervezetre - mint a segítségnyújtás forrására - történő hivatkozás. Ez a levél is valószínűleg gépi fordítás segítségével készült, és ismét láthatunk példát a nem beazonosítható linkre.



Segítségnyújtás a koronavírus ellen
A magyar kormány támogatást nyújtott az új koronavírus elleni küzdelemhez.

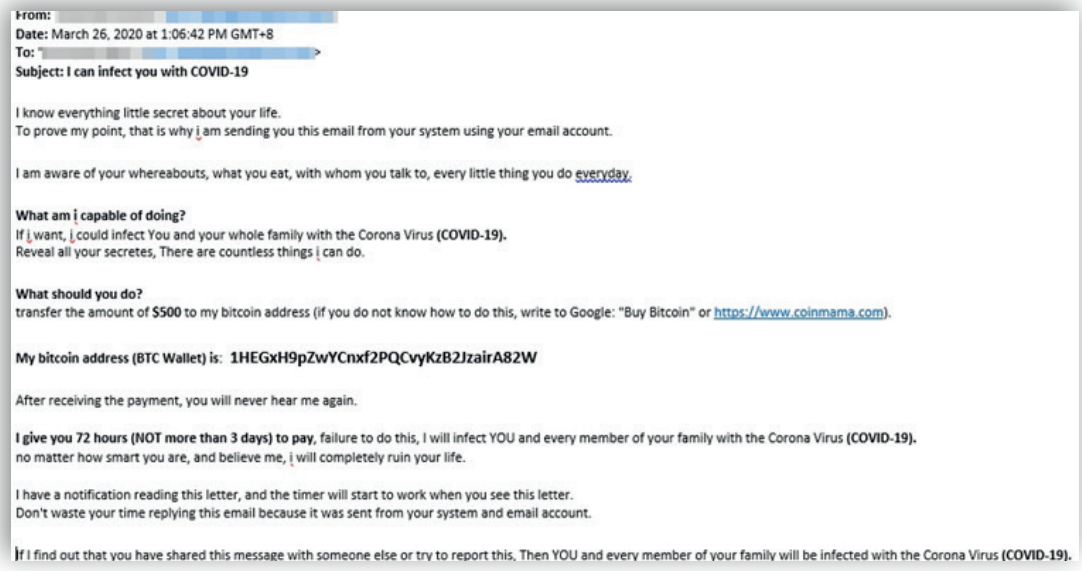
Szia,
A magyar kormány az Egészségügyi Világszervezettel együttműködve úgy döntött, hogy kivételes segítséget nyújt az új koronavírus elleni küzdelemben.
Az átfogó karanténkárosodások enyhítésével összefüggésben az állam pénzügyi támogatást nyújt az érintetteknek, tehát a regisztrációt az alábbi online platformon kell végrehajtani

A platform a következo szolgáltatásokat kínálja:
1 - A kérelmezo állapotának nyomon követése
2 - Panaszok és vizsgálatok benyújtása
3 - Egyéb kivételes támogatás igénybevételére irányuló kérelmek benyújtása különleges esetekben
4 - Pénzügyi támogatás visszavonása a regisztráció azonnali befejezése után

Regisztráljon segítségért

A regisztráció június végéig megengedett
További információkért kérjük, látogasson el a koronavírus kormányzati oldalára
köszönöm.

Az alábbi e-mailben zsarolással igyekeznek pénzt kicsalni az áldozattól, akit azzal fenyegetnek, hogy megfertőzik az egész családját koronavírussal, ha nem fizeti be az 500$-os díjat a csaló bitcoin tárcájába.



From:
Date: March 26, 2020 at 1:06:42 PM GMT+8
To:
Subject: I can infect you with COVID-19

I know everything little secret about your life.
To prove my point, that is why i am sending you this email from your system using your email account.

I am aware of your whereabouts, what you eat, with whom you talk to, every little thing you do everyday.

What am i capable of doing?
If i want, i could infect You and your whole family with the Corona Virus **(COVID-19).**
Reveal all your secretes, There are countless things i can do.

What should you do?
transfer the amount of **$500** to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin" or https://www.coinmama.com).

My bitcoin address (BTC Wallet) is: 1HEGxH9pZwYCnxf2PQCvyKzB2JzairA82W

After receiving the payment, you will never hear me again.

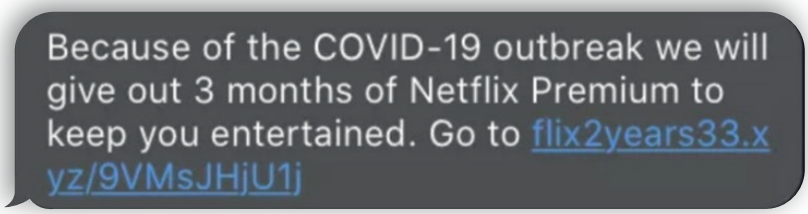
I give you 72 hours (NOT more than 3 days) to pay, failure to do this, I will infect YOU and every member of your family with the Corona Virus **(COVID-19).**
no matter how smart you are, and believe me, i will completely ruin your life.

I have a notification reading this letter, and the timer will start to work when you see this letter.
Don't waste your time replying this email because it was sent from your system and email account.

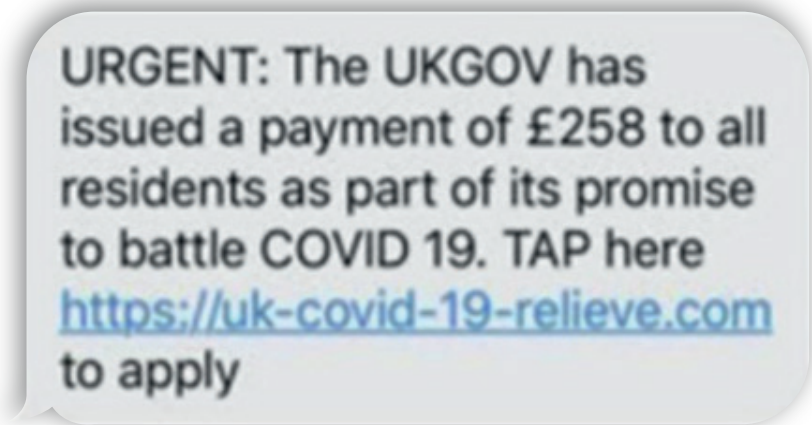
If I find out that you have shared this message with someone else or try to report this, Then YOU and every member of your family will be infected with the Corona Virus **(COVID-19).**

Példák csaló üzenetekre

Ingyenes Netflix szolgáltatással akarják rávenni a címzettet a link megnyitására. Mindamellett, hogy a link egyértelműen nem beazonosítható, hiányzik a részletes tájékoztatás is, amely elengedhetetlen részlete a szerződésnek.



Az alábbi üzenetben az angol kormány nevében ígér pénzt. Már elsőre gyanús az üzenet küldője (COVID19) és a csupa nagybetűs, sürgető tartalmú szövegrészek. Ismét egy nem beazonosítható linkkel próbálják meg rászedni az áldozatokat, miközben egy hivatalosnak tűnő forrásra (UKGOV) hivatkoznak. Az angol kormányzat hivatalos weboldala egyébként pont a fordítottján érhető el: gov.uk.



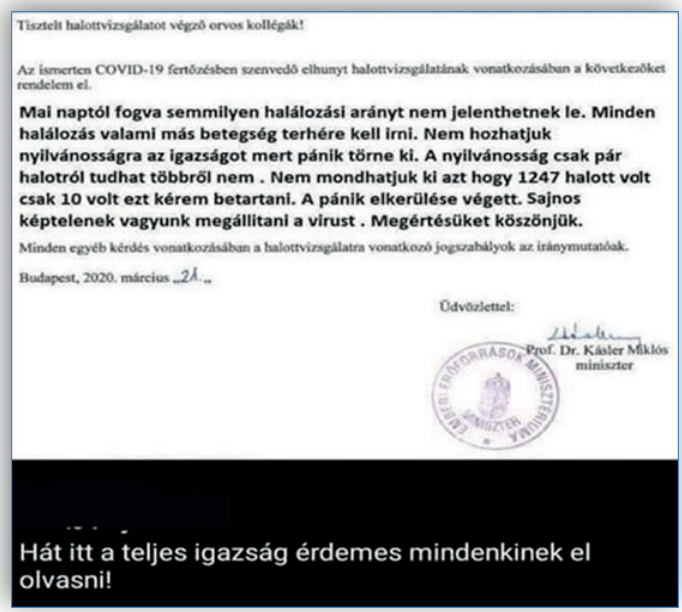
Példák közösségi oldalakon terjedő álhírekre

Az Országos Korányi Pulmonológiai Intézetről terjesztettek valótlan híreket a közösségi oldalakon. Árulkodó jel a meghökkentő figyelemfelkeltő, félkövér cím. A hírből hiányzik az intézmény hivatalos elérhetősége vagy bármilyen hivatalos forrás, ahol tájékozódásra lenne lehetőség.

Összeesküvés-elméletre alapozó álhír:

Tessék tegnapról egy videó! Olaszországban senki sem halt meg a koronavírustól, állítja a videóban látható Genovai kórházigazgató. Influenza van, de az most már épp a végét járja. Idén kevesebb embert érintett az influenza mint tavaly! Ha otthon maradsz, és nézed a TV -t, a hírek megmérgeznek és megmérgezik a várost.
Ami velünk most történik az egy globális terv része, és pontosan az a cél hogy minden leálljon, tönkremenjen, leértékelődjön. A vírus csak az eszköz amit a hatalom felhasznál céljaik megvalósítása érdekében ! (Új Világrend)

Az emberi erőforrások miniszterének nevével visszaélő álhír, amely a klasszikus figyelemfelkeltő - félkövér, nagyobb méretű betűk - eszközökkel állít valótlanságokat. Szerencsére maga a szöveg is segítségünkre van, mivel nehezen értelmezhető és rossz a tagolása.

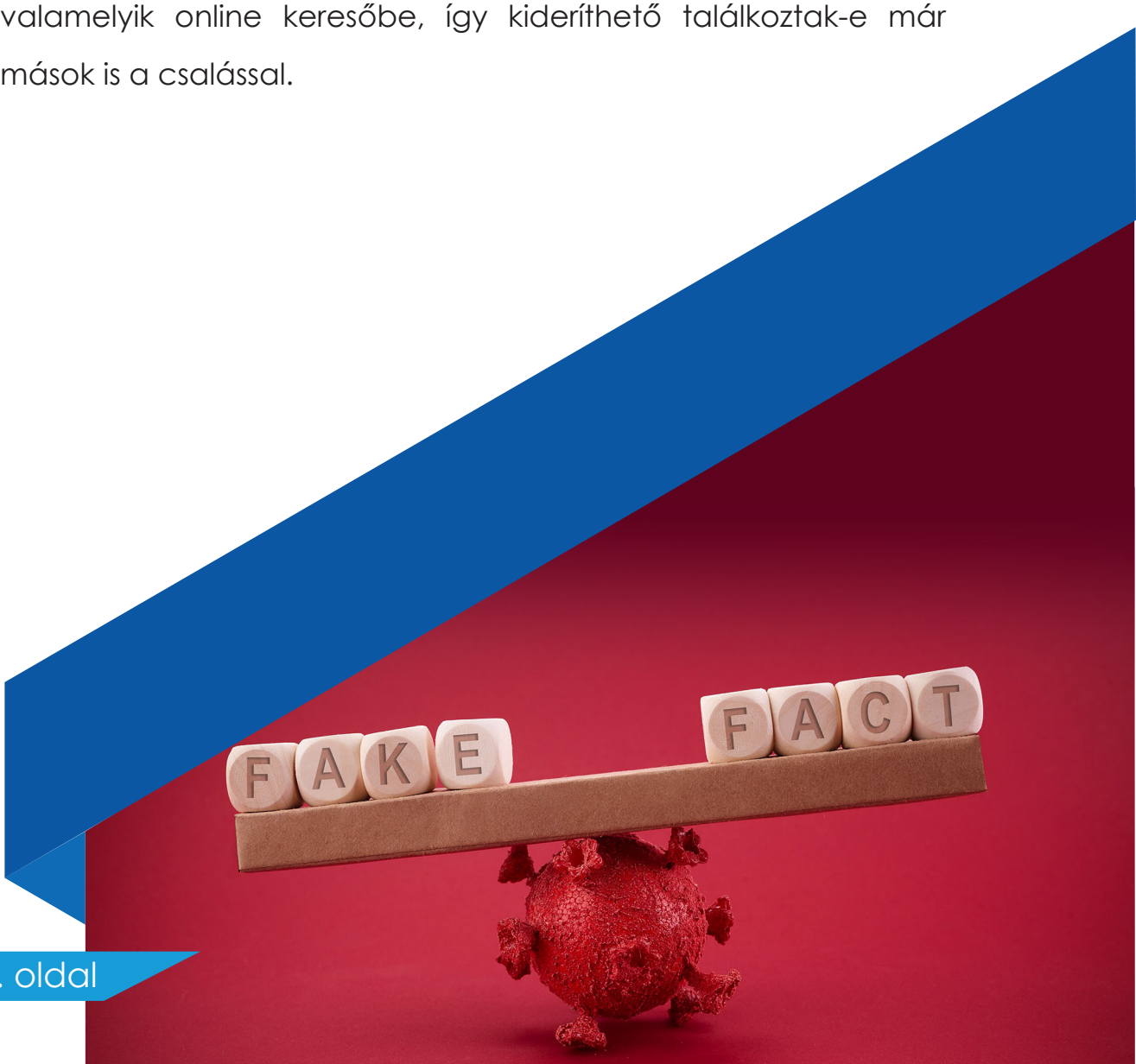


Egy felhasználó profilját és képeit felhasználó hirdetés, ami kölyökkutyát árul. Jól olvashatóak a felhasználói hozzászólások a kép jobb oldalán, amik felhívják a figyelmet a hirdetés csaló mivoltára. A koronavírus pandémia alatt megszaporodtak az ilyen jellegű csalások.

Védelmi javaslatok

- **Ne kattintsanak** az ilyen tárgyú e-mailekben szereplő hivatkozásokra, akkor sem, ha látszólag ismerőstől érkezett a megkeresés!
- **Ne töltsék le** a mellékletben szereplő – legtöbbször Microsoft Word, PDF, EXE, illetve MP4 kiterjesztésű – fájlokat!
- A közösségi média oldalakon is fokozott óvatossággal kezelendők a témakörben terjedő információk, ne adjunk hitelt a pánikkeltő információknak, információért **forduljunk a hivatalos szervekhez**!
- **Tartsák naprakészen** a vírusvédelmi szoftvereket és telepítsék a biztonsági frissítéseket, valamint tiltsák a Microsoft Office makrókat!
- Kövessék a **hivatalos tájékoztatási csatornákat**, például az NNK weboldalát!
- **Fokozott óvatossággal** járjanak el bármilyen koronavírus (COVID-19) témájú ismeretlen eredetű e-mail, közösségi portálról érkező megkeresés esetén!
- Egy valódinak tűnő megkeresés esetén is **tájékozódjanak** az adott szervezet, intézmény weboldalán, vagy vegyék fel a kapcsolatot közvetlenül a feladóval!

- **Vigyázzanak** az egyre gyakoribb **pénzgyűjtő kezdeményezésekkel**, ha adományozni szeretnének előtte mindig ellenőrizzék le az adott szervezetet!
- **Kezeljék fenntartással** a közösségi média oldalakon terjedő adománygyűjtéseket!
- **Csak hiteles és megbízható forrásból** tájékozódjanak, és ne dőljenek be az ún. lánclevelek (hoax) útján terjedő hamis híreknek!
- Gyanúsnak tűnő üzenet esetén másolják be az üzenet egy részét valamelyik online keresőbe, így kideríthető találkoztak-e már mások is a csalással.

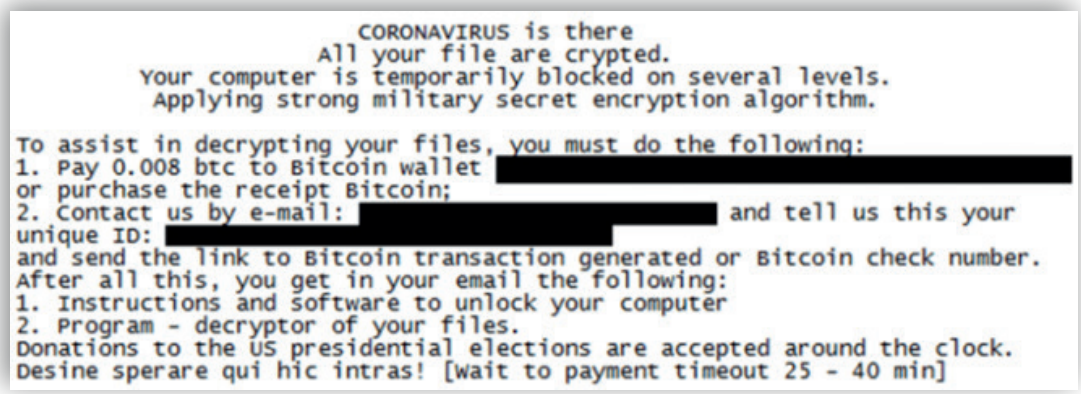


COVID-19 témájú mobil alkalmazások

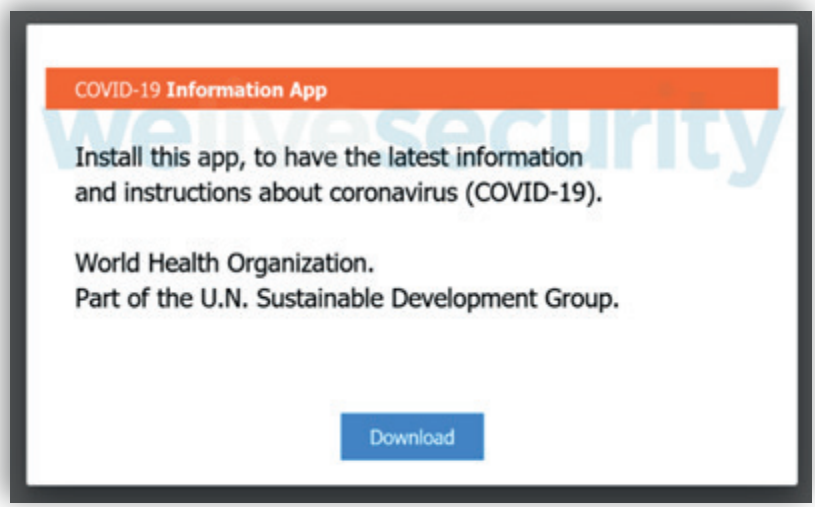
Nagy számban jelennek meg olyan alkalmazások, amelyek látszólag a koronavírussal kapcsolatos fontos információk közlésével kecsegtetnek, azonban használatukkal **káros hatású programot** töltünk le a készülékre. Ilyen applikáció – többek között a leggyakrabban előforduló – Androidos „**COVID 19 Tracker**", amely igazából a **CovidLock** elnevezésű **zsarolóvírust** telepíti a gyanútlan felhasználó eszközére. A coronavirusapp[.]site weboldal egy Androidos applikáció letöltésére próbálja meg rávenni a felhasználókat, amely az ígéret szerint segítséget nyújt a vírus terjedésének nyomon követéséhez az Egyesült Államokban, azonban valójában egy zsarolóprogramot, ún. ransomware-t tartalmaz. A CovidLock ransomware alapvető funkciója, hogy a **telefon képernyőjét zárolja**, amely megoldására nem nyújt megoldást az eszköz újraindítása. A káros kód képes ellenőrizni a felhasználó jogosultsági szintjét. A CovidLocknak a működéshez szüksége van, adminisztrátori jogosultságra, és amennyiben a felhasználó ezt engedélyezi, a CovidLock közel **teljes hozzáférést szerez az eszközhöz**. Az engedélyt a felhasználó megtévesztésével szerzik meg, a képernyőn látszólag az "online COVID statisztikák engedélyezése", illetve az "ismert COVID fertőzöttek lokációjának ismerete" engedélykérések jelennek meg. A kért engedélyek megadása után a zsarolóvírus megkezdi működését és a képernyő zárolása után 2 napos határidőt ad a váltságdíj megfizetésére. A váltságdíj változó, általában 100-250 USD közötti összeg. A fizetés megtagadása esetén a telefon adattartalma törlésre kerül.

Pédák rosszindulatú mobilalkalmazásokról

Képernyőmentések egy zsarolóvírus által zárolt eszközökről:



Üzenet, ami káros applikáció letöltésére buzdít, melyet a WHO egy nemzetközi szervezet nevében próbálnak terjeszteni:



Védelmi megoldások, javaslatok

- **Ne telepítsenek** COVID-19 témájú alkalmazásokat: a megbízhatónak tűnő weboldalak is veszélyt rejthetnek, és az olyan megbízhatónak tartott források is, mint a Google Play Store, vagy az App Store!

- **Ne töltsenek le** megbízhatatlan, ellenőrizetlen forrásból származó, a koronavírus terjedését mutató online térképet, ugyanis az eredetihez hasonló, csaló online térképeken keresztül is történhet káros kód terjesztés!

- Amennyiben a felhasználók hiteles és megbízható információkat szeretnének kapni a vírus terjedéséről, elsősorban a **hivatalos** koronavirus.gov.hu oldalon keresztül elérhető online térképet használják.

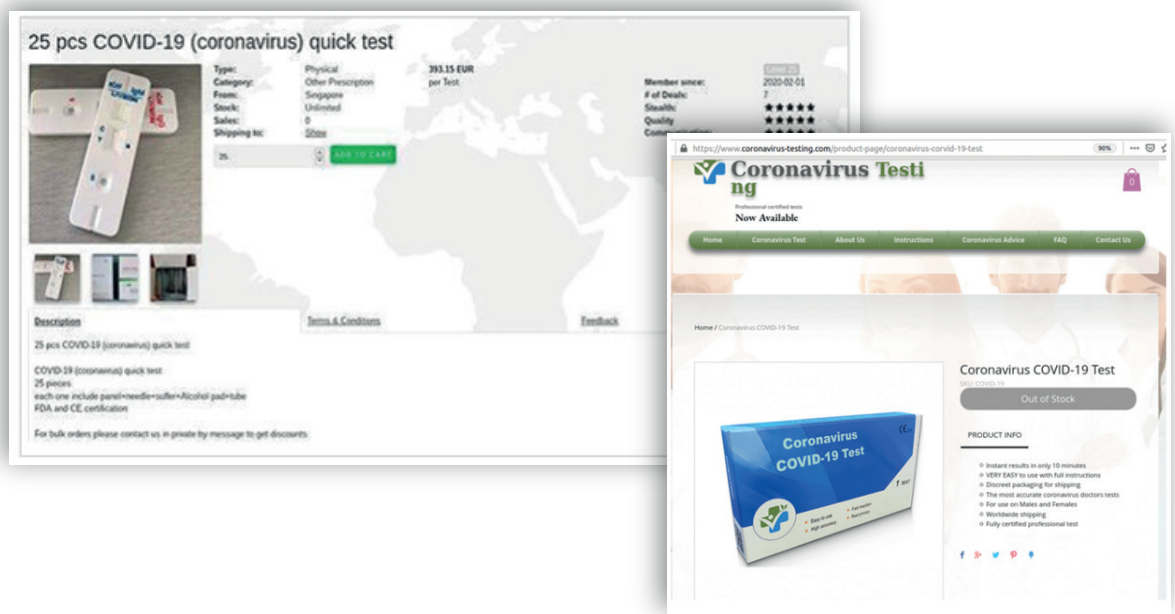
COVID-19 témájú weboldalak

A csalók arcmaszkokat, tisztítószereket vagy más, a vírus elpusztítására képes eszközöket és módszereket kínálnak a levelekben, amelyek egy **átverős oldalra irányítják** a gyanútlan áldozatokat. Az ilyen helyzetek sajnos nagyon jó terepet kínálnak kiberbűnözőknek, ezért a felhasználóknak még jobban oda kell figyelniük az internetes vásárlások során. Az oldal általában **nem használ https** sémát (titkosított kapcsolat), ezért bármilyen forgalom a weboldal irányában más támadók számára is lehetőséget kínál a kommunikációba való beavatkozásra. A webshop **semmilyen adatot nem közöl** az oldal üzemeltetőjéről, vagy az eladóról. Az oldal alján található adathalász formula mellett, a webshop aloldalakat és valósnak tűnő hozzászólásokat, terméktapasztalatokat is tartalmaz a jobb hatás kedvéért. A minél nagyobb haszon elérése érdekében a bűnözők úgy állítják be ezeket a „gyógyszereket", mint amelyek szigorú bevizsgálásokon estek át. A nagyobb hitelesség elérése érdekében az elkövetők **gyakran hamis szakértőket szólaltatnak meg**, stúdióbeszélgetéseket imitálnak és tudományosnak látszó tanulmányokra is hivatkoznak hirdetéseik során. Az ilyen különleges helyzetekben, amikor a kiberbűnözők az emberek félelmeit kihasználva próbálnak bevételhez jutni, **fokozottan oda kell figyelni** a felhasználóknak, mert könnyen csalás áldozatává válhatnak a gyanútlan vásárlók, amelynek hatásai (ellopott személyes adatok), akár hónapokkal később is komoly gondokat okozhatnak.

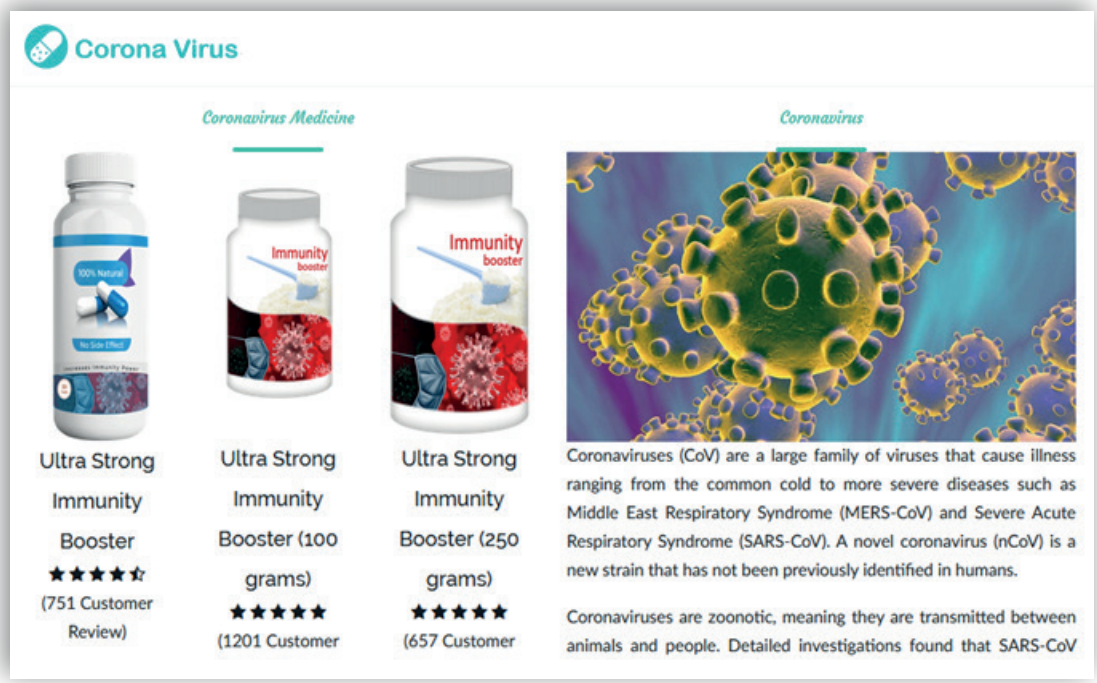
Példák káros weboldalakra

Szájmaszkot áruló csaló weboldal, ami adathalász tevékenységet folytat. Általában semmilyen vagy erősen hiányos információkat tartalmaz az üzemeltetőjéről. Irreálisan magas áron kínálják termékeiket azok hiányára alapozva. Az oldal nem ellenőrizhető forrásból származó hozzászólásokkal próbál vásárlásra buzdítani. Az utánvétes fizetési módszer a banki követés kijátszására szolgál ebben az esetben.

Koronavírus gyorstesztet árusító csaló weboldalak:



A koronavírus leküzdésére alternatív gyógymódokat ígérő honlap:



Rendőrség által lefoglalt, hamisított, rossz minőségű kézfertőtlenítők, amelyet egy webáruházon keresztül próbáltak meg értékesíteni.

Védelmi megoldások, javaslatok

- Online vásárlás során mindig **használjunk biztonságos eszközöket** (frissített operációs rendszert, megfelelő védelmi szoftvert)!
- Használjunk **biztonságos internetkapcsolatot** (pl. nyilvános helyett otthoni Wifi hálózatot)!
- Használjunk olyan kibervédelmi megoldást, amely s**pam és adathalászat elleni védelmet** is tartalmaz!
- **Csak megbízható**, ismert **webshoptól vásároljunk**: nézzük meg a visszajelzéseket, ahol esetleg a felhasználók visszaélésekről írnak!
  - vásárlói fiók létrehozásakor használjunk **erős, egyedi jelszavakat**!
  - érdemes az **utánvételes fizetési** opciót előnyben részesíteni!
  - soha **ne mentsük el** bankkártya adatainkat a webshopban, vagy a böngészőben!
- Kizárólag **https weboldalakon** vásároljunk, így a kommunikáció titkosított lesz, és kevesebb valószínűséggel zavarhatják meg a támadók! Arra azonban figyeljünk, hogy a támadók is használhatnak https webshopokat, ezért csak megbízható oldalaktól vásároljunk!
- Ha bármilyen furcsaságot észlelünk a tranzakció során, azonnal **jelezzük bankunknak**!

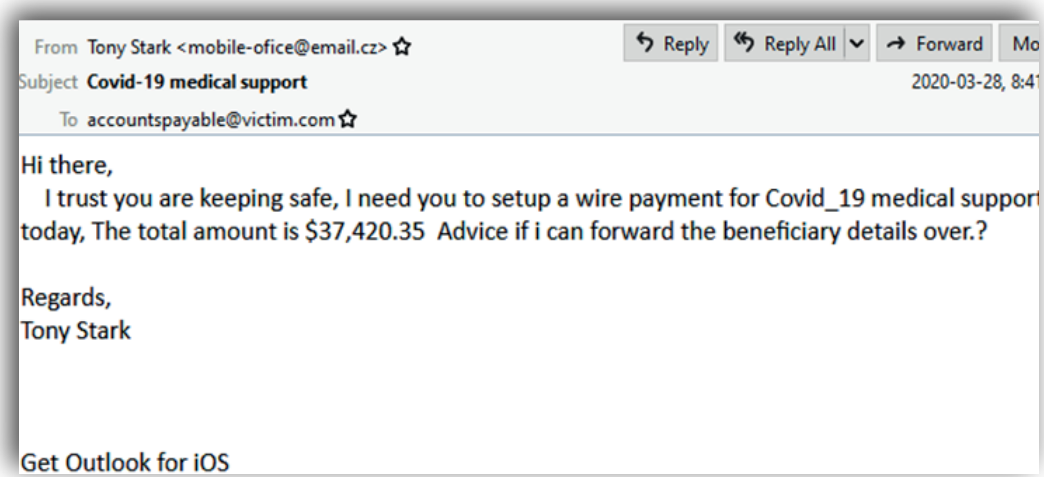
Pénzügyi csalások

A befektetők óvakodjanak a koronavírussal kapcsolatos **befektetési csalásoktól**, főképp az olyan termékek vagy szolgáltatásoktól, amelyek a v**írus megelőzését, észlelését vagy ellenszerét hirdetik**. A csalók lehetnek akár jó szándékú emberek is, akik ellenőrzés nélkül továbbítanak „tuti" pénzügyi tanácsokat, például bizonyos vállalatok részvényárainak emelkedését vagy csökkenését. Az egyik legismertebb közülük egyfajta **piramisjáték**, ahol a korábbi befektetőket az újonnan érkezett befektetők pénzéből fizetik ki, egészen a rendszer összeomlásáig. Ezt is általában egy **e-mail küldésével kezdik** a csalók, amiben bemutatnak egy jónak tűnő üzletet a befektetés megtízszerezésére. Előfordulhat, hogy a csaló létező befektetési társaság képviselőjének adja ki magát. A szakértők szerint alaposan meg kell vizsgálni a lehetőséget, és a mögötte álló céget. Az adócsalások során a bűnözők a **helyi adóhatóság nevében adathalász e-maileket küldenek**, amelyek révén megpróbálnak személyes és pénzügyi információkat kicsalni áldozataiktól. A megszerzett adatokat pénzügyi csalásokra és **személyazonossággal való visszaélésre** használják. Egy újabb átverési technika a **lottó és nyereményjáték csalások**: az áldozat egy kéretlen e-mailt, telefonhívást vagy SMS-t kap, amelyikben azt állítják, hogy egy nagyobb összeget vagy valamilyen luxusnyereményt nyert, amiért csak korlátozott ideig tud jelentkezni.

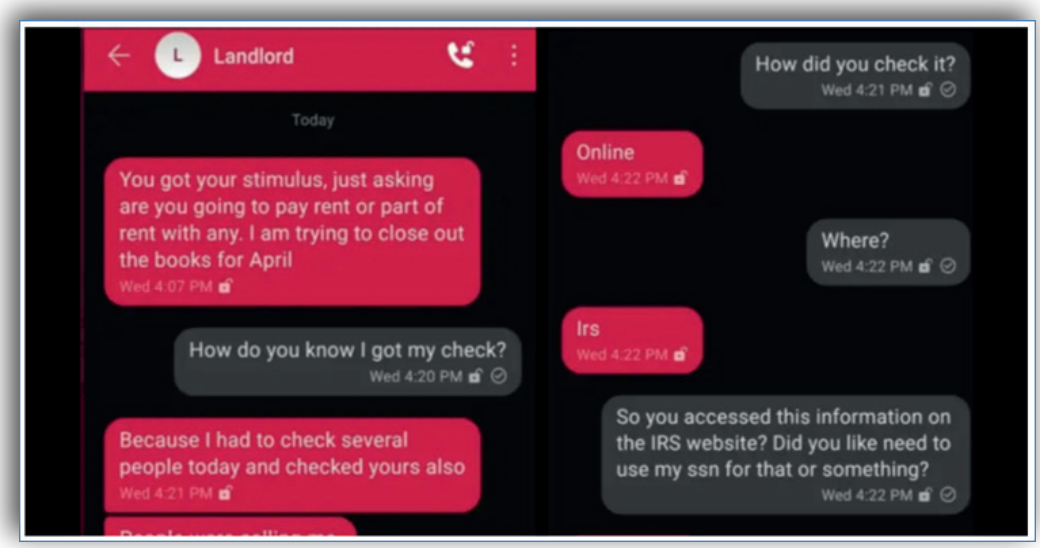
Ehhez először meg kell fizetnie egy bizonyos összeget, például az adók fedezetét vagy a szállítási, esetleg más képzeletbeli költséget. Mivel a nyereményjáték nem is létezik, az áldozat soha nem kapja meg az ígért nyereményét, hiába fizeti meg a kért összeget. Jellemzően Magyarországon, az úgynevezett „unokázós" csalók is meglátták a lehetőséget a járványban. A bűnözők telefonon kínálnak időseknek egy magyar doktornő által kifejlesztett vakcinát, 12 ezer forintos áron.

Példák

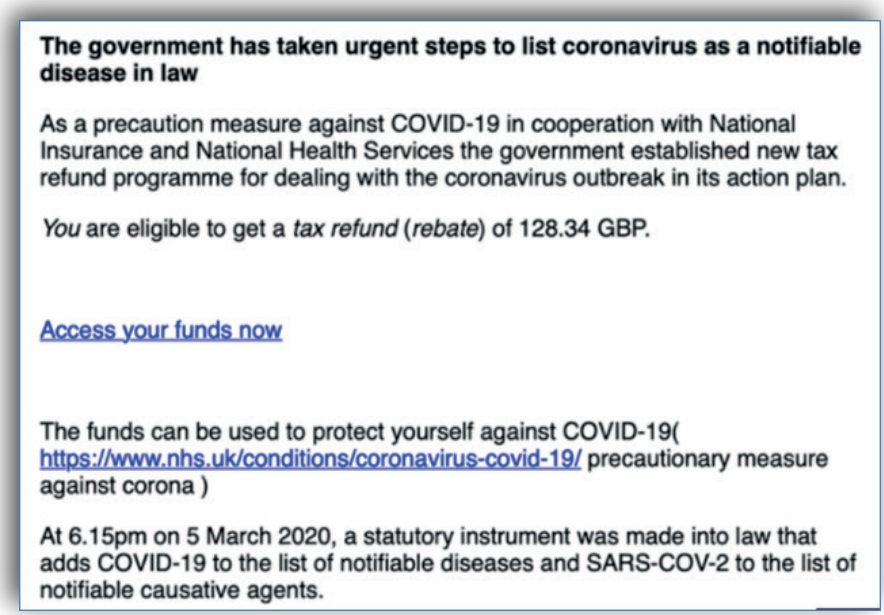
Ismeretlen feladótól származó csaló e-mail, ami orvosi biztosításra alapozva próbál meg pénzt kicsalni a gyanútlan áldozatoktól.



Az alábbi képen egy üzenetváltást láthatunk, melyben a bűnözők az albérleti díj kifizetésére szólítják fel a bérlőt a tulajdonos nevében. Itt is a jól bevált taktikát, a sürgető jellegű üzenetet próbálták meg alkalmazni, kevés sikerrel.



Adóvisszatérítéssel kecsegtető adathalász e-mail. Figyelmeztető jelzés a nem beazonosítható link, az állami és nemzetközi szervezetekre hivatkozás és a levélben található állítások ellenőrzésére szolgáló elérhetőségek teljes hiánya.



The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

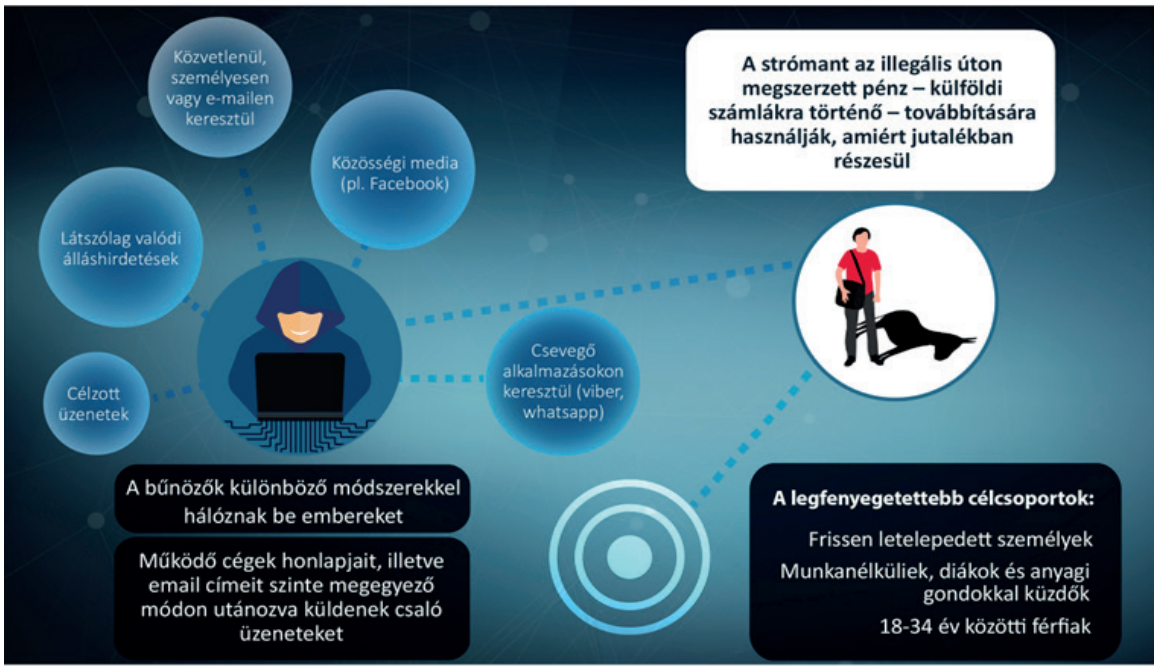
At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

Védelmi intézkedések, javaslatok

- Mielőtt pénzt adna át vagy befektetne, **mindig kérjen** megbízható, minősítéssel rendelkező független pénzügyi tanácsadótól **tájékoztatást**!
- **Utasítsa el** a befektetési lehetőségekkel kapcsolatos marketing hívásokat!
- **Kezelje gyanakvással** a biztonságot, garantált visszatérítést és nagy hasznot ígérő ajánlatokat!
- A jövőben is **óvakodjon a csalásoktól**! Ha már esetleg befektetett egy átverésbe, a csalók valószínűleg újra megcélozzák Önt, vagy a megszerzett adatokat továbbadják más bűnözőknek.
- Általában az ilyen típusú átverések és csalások telefonhívás formájában próbálják meg lebonyolítani, így ha számunkra **ismeretlen számról keresnek** vagy hívószám kijelzés nélküli hívást kapunk **fokozott óvatossággal járjunk el**!

Pénzmosás

A bűnözők a vírushelyzetet kihasználva gyanútlan embereket használnak fel pénzmosási tevékenységük működtetésére. **Hamis egészségügyi szervezeteket hoznak létre** és online hirdetéseken keresztül becsalogatják a munkavállalókat. Az új dolgozókat megkérik, hogy dolgozzák fel az „adományokat" a koronavírus elleni harc érdekében. Fizessék be a pénzt a bankszámlájukra, majd küldjék tovább, megtartva a jutalékot maguknak. Az esetek többségében **otthoni munkavégzéssel**, vagy **online társkereső** platformokat használva szedik rá az áldozatokat. Ha egy távmunkalehetőség magában foglalja pénz utalását egy állítólagos ügyfél számára, illetve ha egy társkeresőn megismert udvarló kéri, hogy küldjenek pénzt valakinek az ő nevében, javasolt visszautasítani a kéréseket.



2. ábra: A pénzmosás folyamata és kommunikációs csatornái

Pénzmosási példák

Otthoni munkát kínáló hirdető, aki valószínűleg pénzmosási céllal tervezi kihasználni áldozatát. Havi 5000$ bevétellel és otthoni munkavégzéssel kecsegtet.

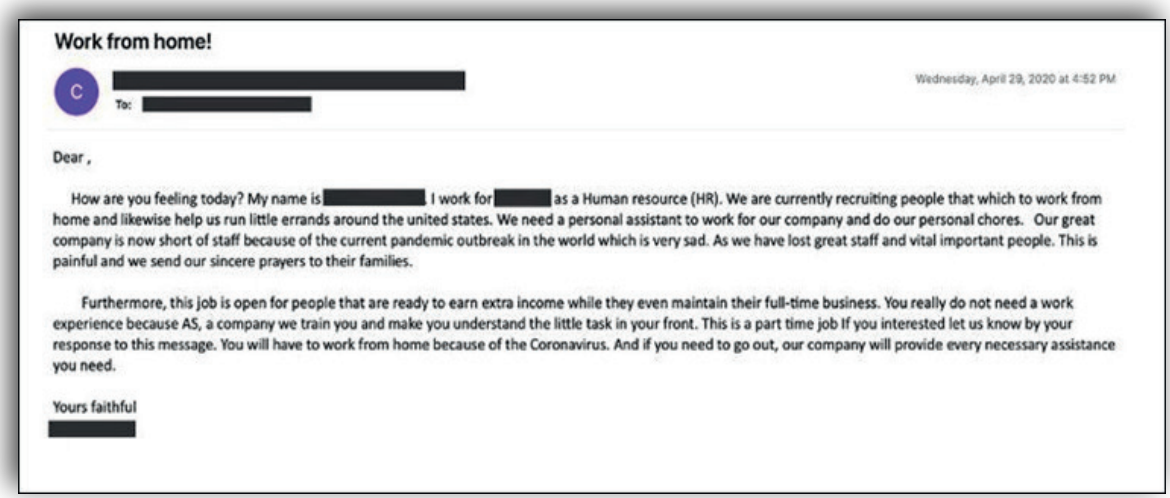
From: shenyeh5@gmail.com
Sent on: Saturday, April 11, 2020 7:39:58 PM
To: [redacted]
Subject: WORK FROM HOME

Hello,

DO you live in CANADA/USA and you are laid off from work due to the recent global crisis with Covid 19? You can work from home and get paid $5,000 monthly. email me for more details.

shenyeh5@gmail.com

Egy másik online munkát kínáló e-mail. Érdekes módon megszólítás nélkül, elég furcsa megfogalmazású angol nyelvezettel.



Work from home!

C [redacted]
To: [redacted]

Wednesday, April 29, 2020 at 4:52 PM

Dear ,

How are you feeling today? My name is [redacted]. I work for [redacted] as a Human resource (HR). We are currently recruiting people that which to work from home and likewise help us run little errands around the united states. We need a personal assistant to work for our company and do our personal chores. Our great company is now short of staff because of the current pandemic outbreak in the world which is very sad. As we have lost great staff and vital important people. This is painful and we send our sincere prayers to their families.

Furthermore, this job is open for people that are ready to earn extra income while they even maintain their full-time business. You really do not need a work experience because AS, a company we train you and make you understand the little task in your front. This is a part time job If you interested let us know by your response to this message. You will have to work from home because of the Coronavirus. And if you need to go out, our company will provide every necessary assistance you need.

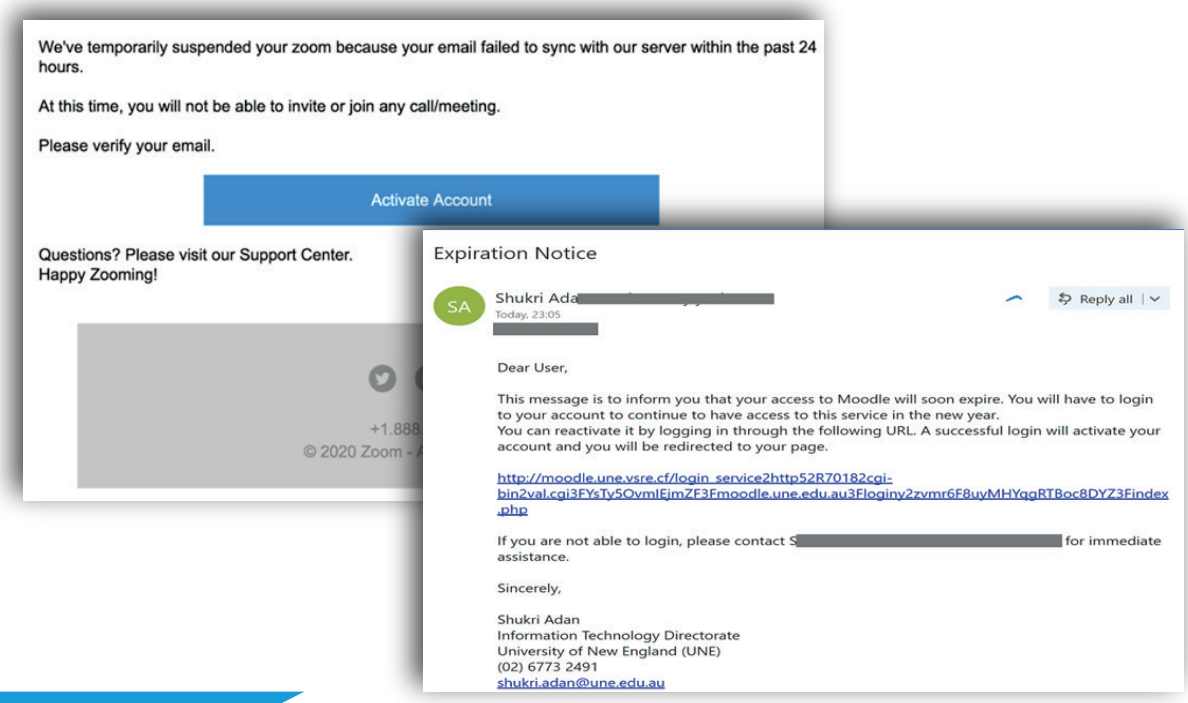
Yours faithful
[redacted]

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. A Kaspersky felmérése szerint 60%-al nőtt meg a támadások száma ezeken a platformokon az előző félévhez képest.

Példák

Egy csaló üzenet, ami a Zoom fiók ideiglenes lezárásával fenyeget, ha nem kattintunk a megadott linkre (ismét nem ellenőrizhető), valamint egy adathalász üzenet, ahol a rosszul beazonosítható linkre kattintást a Moodle fiók közeljövőben történő lejárásának hírével próbálják meg elérni.



Távmunka, otthoni munkavégzés (home office) kockázatai

A távmunka jelen helyzetben sok munkáltató számára biztosíthat megoldást az **üzletfolytonosság fenntartása érdekében**, azonban a kiberbiztonsági szempontokról, a biztonságtudatos magatartásról az ilyen munkavégzés során sem szabad megfeledkezi. A szervezet távoli munkavégzésre történő átalakítása ugyanis **sérülékennyé teheti a munkahelyi infrastruktúrát**, ezért kiemelten fontos a megszokott IT biztonsági alapelvek megtartása az otthonról végzett munka bevezetése után is.

Erre nagyon jó példa a Deloitte felmérése, aminek adatai szerint az otthonról dolgozó munkavállalók negyede észlelt **sűrűbb adathalászatra utaló kísérleteket** és csaló e-maileket a koronavírus megjelenése óta. A válaszolók 26%-a tart a saját adatain kívül a munkáltató adatainak ellopásától is, hiszen az otthoni munkavégzésnek köszönhetően néha nem várt helyzetek alakulhatnak ki, mondjuk vállalati adatok tárolására kényszerülünk a magán számítógépünkön.

Az NBSZ NKI weboldalán egy részletes ajánlásgyűjtemény érhető el azon szervezetek számára, amelyek a jelenlegi helyzetben akarnak azonnali megoldást találni a home office kérdéskörére. Az otthoni környezet biztonságos átalakításához további hasznos információk érhetők el a SANS Intézet ingyenes webes képzésén is.

Átverésre utaló, gyakori jelek

- Rossz magyarsággal, akár szemmel láthatóan gépi fordítással készített szöveg;
- Eltérő elköszönési módok, például megszólítás: Kedves mindenki, elköszönés: Szia;
- Ékezeteket tartalmazó e-mail címek;
- Ingyenes vizsgálatokat, gyógymódokat vagy gyógyszereket ígérnek;
- Koronavírus áldozatok, ismert személyek vagy intézmények nevében adományok gyűjtése;
- Elektronikus üzeneteknél indokolatlan mellékletek jelenléte, például csatolt prezentációk, videók, vagy dokumentumok formájában;
- Nem, vagy csak nehezen beazonosítható linkek, amelyek különböző weblapokra irányítanak át;
- Bármilyen üzenet vagy telefonos megkeresés, amely során személyes adatokhoz próbálnak meg hozzájutni;
- Segítséget, elsősorban pénzt kérő bejegyzések a közösségi médiában, amik akár közelebbinek tűnő ismerőstől is származhatnak (a csalók megpróbálhatják az ismerőseink adatait felhasználva kicsalni tőlünk pénzt);

- Kevésbé használt fizetési módszerek igénybevétele, például kriptovaluta vagy webshop kedvezmény kártyák (iTunes ajándékkártya);
- Gyors döntéshozatalra kényszerítő megkeresések, például: „gyorsan tessék dönteni, tegnap is egy óra alatt elvitték az egész készletet”;
- Állami és nemzetközi intézmények, közszereplők nevében kapunk megkeresést, például: WHO, bankok, népjóléti miniszter, operatív törzs, közszereplők;

Fogalomjegyzék

Kiberbűnöző: Olyan egyének vagy csoportok, akik a technológiai lehetőségeket kihasználva okoznak kárt számítógépes rendszerekben, pénzügyi nyereség reményében.

Fake news: A valóságnak nem megfelelő, gyakran szándékosan, mások lejáratására vagy pénzszerzési célra létrehozott álhírek.

Hoax: Leggyakrabban e-mailben terjedő álhírek és lánclevelek.

Adathalászat (phishing): Adathalászatnak azt az eljárást nevezzük, amikor egy internetes csaló oldal egy jól ismert cég hivatalos oldalának láttatja magát és megpróbál bizonyos személyes adatokat, például azonosítót, jelszót, bankkártyaszámot stb. illetéktelenül megszerezni. A csaló általában e-mailt vagy azonnali üzenetet küld a címzettnek, amiben ráveszi az üzenetben szereplő hivatkozás követésére egy átalakított weblapra, ami külsőleg szinte teljesen megegyezik az eredetivel.

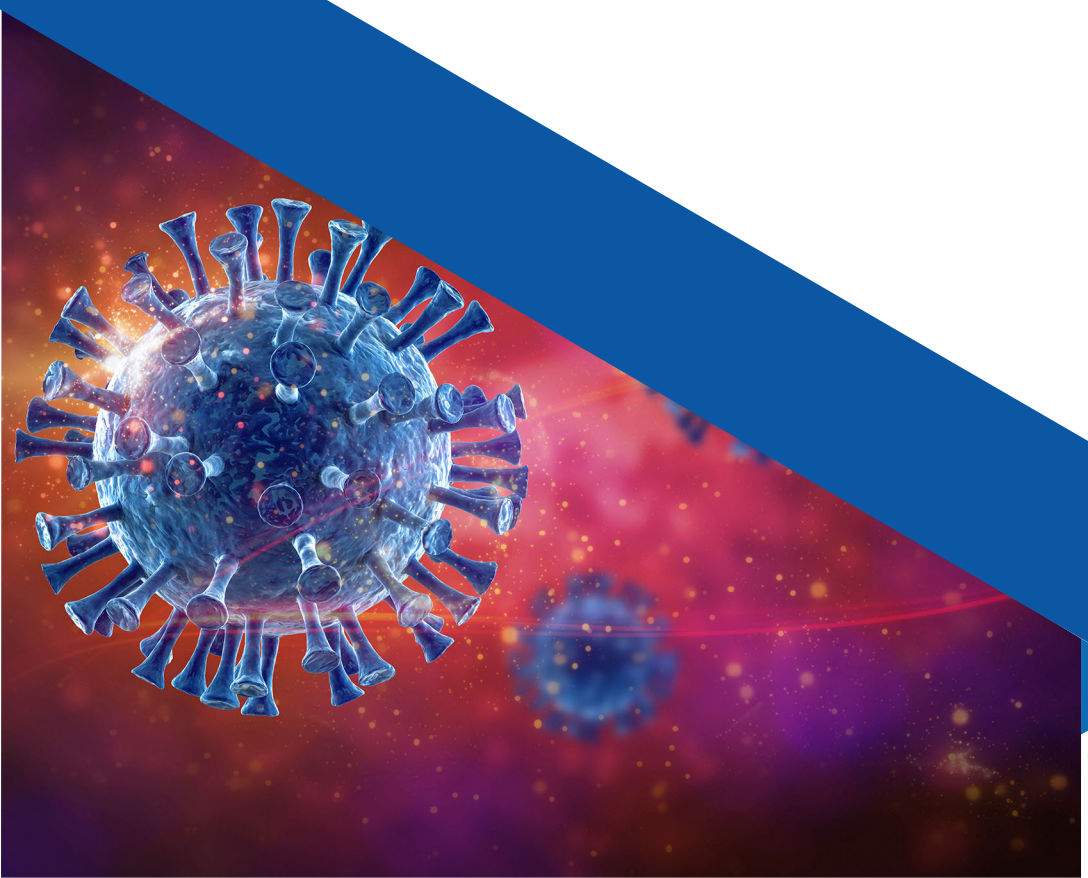
Makró: A makró az informatikában a felhasználó által egy adott programon belül létrehozott szoftverek egyik típusa. A makró fő feladata az, hogy az ismétlődő feladatok elvégzését megkönnyítse, például lehetővé teszi több parancs kiadását egyetlen lépésben.

Applikáció, app: Okoseszközökre (pl. mobiltelefon, tablet) letölthető program.

Zsarolóvírus (ransomware): Olyan kártékony szoftverek, melyek zárolhatják az eszközöket vagy titkosíthatják az eszközökön lévő adatokat annak érdekében, hogy pénzt csikarjanak ki a tulajdonostól.

Adminisztrátori jogosultság: A számítástechnikai eszközökön (PC, mobiltelefon, tablet, laptop, stb.) a felhasználó által létrehozott fájlokon kívül sok olyan, a működéshez szükséges fájlt tartalmaz, amely a rendszer megfelelő működéséhez szükséges. Ezek a fájlok védve vannak például a véletlen törlés ellen és módosításukhoz, törlésükhöz magasabb szintű hozzáférés szükséges.

https: Olyan hálózati kommunikációra kifejlesztett séma, amely titkosítás segítségével külső fél által nem lehallgathatóvá teszi kapcsolatot két eszköz között.



NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36(1)325 7672

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

Kibertámadás!
podcast

2022