A kiberbűnözők az új koronavírus miatt kialakult helyzetet különféle támadási módszerekkel próbálják kihasználni. Olyan, az emberek fokozott érdeklődésre épített megtévesztő technikákat alkalmaznak, amelyek a közeljövőben is megfelelő alapot jelenthetnek számukra a pandémiát 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.

NEMZETI
KIBERVÉDELMI INTÉZET

Megtévesztő levelek, álhírek, közösségimédia-üzenetek

Február óta folyamatos az álhíreket (fake news) 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.

Az NBSZ NKI javaslatai szerint a felhasználók:

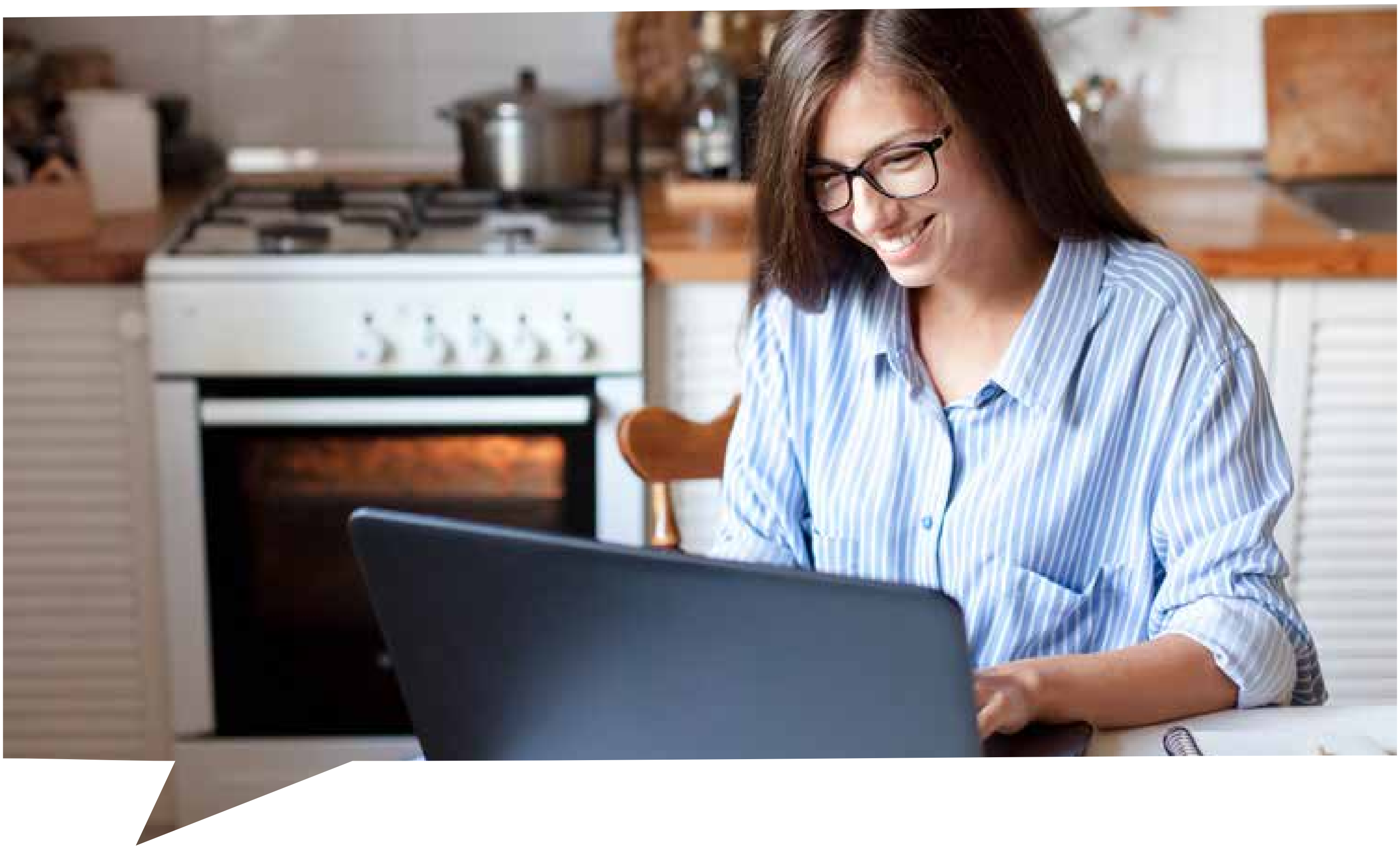
- fokozott óvatossággal járjanak el bármilyen új koronavírus (COVID-19) témájú ismeretlen eredetű e-mail, közösségi portálról érkező megkeresés esetén;
- egy **valódinak tűnő** megkeresés, tájékoztató esetén is tájékozódjanak az adott szervezet, intézmény weboldalán, vagy vegyék fel a kapcsolatot közvetlenül a feladóval;
- **ne kattintsanak** az új koronavírus témájú e-mailekben szereplő hivatkozásokra, abban az esetben sem, ha úgy tűnik, mintha munkatársaktól érkeztek volna;
- **ne töltsenek le, és ne nyissanak meg** mellékletben szereplő – legtöbbször Microsoft Word, PDF, EXE, illetve MP4 kiterjesztésű – fájlokat;
- 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.

Az új koronavírussal kapcsolatos, COVID-19 témájú mobil alkalmazások és weboldalak

Nagy számban jelennek meg olyan alkalmazások, amelyek látszólag az új koronavírussal kapcsolatos fontos információk közlésével kecsegtetnek, azonban valójában káros tartalmúak. Ilyen applikáció – többek között a leggyakrabban előforduló - androidos „COVID 19 Tracker", amely igazából a **CovidLock** elnevezésű zsarolóvírust telepíti a gyanútlan felhasználó eszközére.

Az NBSZ NKI javaslatai szerint a felhasználók:

- 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 vírus 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 koronavirus.gov.hu oldalon keresztül elérhető online térképet használják.



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.

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.

Az új koronavírus témájú kiberfenyegetésekről az NBSZ NKI folyamatosan hiteles információkat, tippeket és tanácsokat szolgáltat honlapján és Facebook oldalán.

Amennyiben a járvánnyal összefüggésben online támadást, csalást tapasztal, kérjük, haladéktalanul jelentse be az NBSZ NKI weboldalán elérhető ún. „Incidensbejelentő űrlapon”, vagy e-mail üzenetben a csirt@nki.gov.hu címen!

nki.gov.hu Nemzeti Kibervédelmi Intézet

1996
Fortes fortuna adiuvat
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERVÉDELMI INTÉZET