



YOU HAVE BEEN
HACKED!

Komárom,
2023.05.12.

Feltörték? Nem enged belépni?
Tanácsok biztonsági problémák kezeléséhez

Szilassi Andrea Informatikus könyvtáros

Ezekről
beszélgetünk
ma:

Bevezetés – Miért fontos ezekkel a dolgokkal foglalkozni?

1. **A belépési nehézségek okai** (Google és Microsoft fiók, Facebook)
2. **Hogy ne veszítsük el fontos fájljainkat, dokumentumainkat, képeinket?** Hová történjen a mentés?
3. **Milyen védelem legyen okoseszközeinken, számítógépeinken?** Mi a megfelelő, az optimális vagy a túl kevés?
4. **Online vásárlás és bankügyek intézése** körültekintően. Lehetséges ez?
5. **Utolért egy zsarolóvírus?** Mit lehet tenni, és mit nem érdemes?



Vannak, akik ilyen
mondatok hallatán
elégedetten
hátradőlnek, és azt
mondják:

***„Jól döntöttem, hogy ebből az egész
digitális őrületből kimaradok!***

***Nincs szükségem nekem ilyen
izgalmakra, szorongásra, félelmekre,
sem pedig arra, hogy még az interneten
keresztül is becsapjanak, kifosszanak!”***

A RENDELET SZERINT AZ ALÁBBI

21

SZOLGÁLTATÁSNAK 2023 VÉGÉIG
A BELSŐ PIAC ORSZÁGAINAK
ÖSSZES ÁLLAMPOLGÁRA SZÁMÁRA
ELÉRHETŐVÉ KELL VÁLNIA EGY KÖZÖS
EURÓPAI FELÜLETEN.

1 Születés anyakönyvezésének igazolása	8 Európai egészségbiztosítási kártya igénylése	15 Állami nyelvből származó adatok igénylése
2 Lakóhely igazolásának kérése	9 Jövedelemadó-bevallás benyújtása	16 Üzleti tevékenység megkezdésének bejelentése és a vállalkozás nyilvántartásba vétele
3 Felsőfokú tanulmányok finanszírozásának ügyintézése	10 Lakcímváltozás bejelentése	17 Munkáltatói egészségbiztosítási járulékok befizetése
4 Felsőoktatási intézménybe történő felvételi	11 Más EU országból származó gépjármű nyilvántartásba vétele	18 Munkavállalás megkezdésének bejelentése és a vállalkozás nyilvántartásba vétele
5 Oklevelek és bizonyítványok online, közhiteles lekérése	12 Útdíjak befizetéséhez kapcsolódó matrica megszerzése	19 TAO bevallás benyújtása
6 Munkavállaláshoz kapcsolódó alkalmazandó jogszabályok megállapításának kérvényezése	13 Károsanyag-kibocsátási matrica elérése	20 Munkaviszony megkezdésének bejelentése
7 Szociális ellátásban részesülők körülményeiben történt változás bejelentése	14 Nyugdíj igénylése	21 Társadalomtudományi járulékok befizetése

Nincs igazuk ezeknek az embereknek ...

- 2023. január 1-én kormányunk elfogadta, útnak indította a Digitális Állampolgárság Programot.
- Ennek jegyében újra értelmezik az állam és a polgárok közötti hivatalos kapcsolatot.
- Már 2023 végéig 21 olyan hivatalos ügy lesz, amelyeket kizárólag elektronikusan lehet majd rendezni, és az ezzel kapcsolatos befizetést teljesíteni.
- A döntéshozók célja, hogy négy éven belül mindent digitálisan lehessen intézni.

Részlet a Rogán Antal nyilatkozatából

„Olyan mobilalkalmazást fejlesztünk, amely lehetővé teszi, hogy mobilon mindenki magával vigye az összes igazolványát, de még a horgászengedélyét is. Mobilon intézhetünk majd ügyeket, mobilon igényelhetünk majd bármilyen igazolást, igazolványt. Nem kell bemenni az okmányirodába semmiért. A mobilalkalmazás lehetővé teszi, hogy a felhasználók egyetlen felületen láthassák adataikat, dokumentumaikat, kezelhessék többek között családpolitikai vagy éppen adózási ügyeiket.”

Forrás: Pénzcentrum.hu, 2022. december 23.



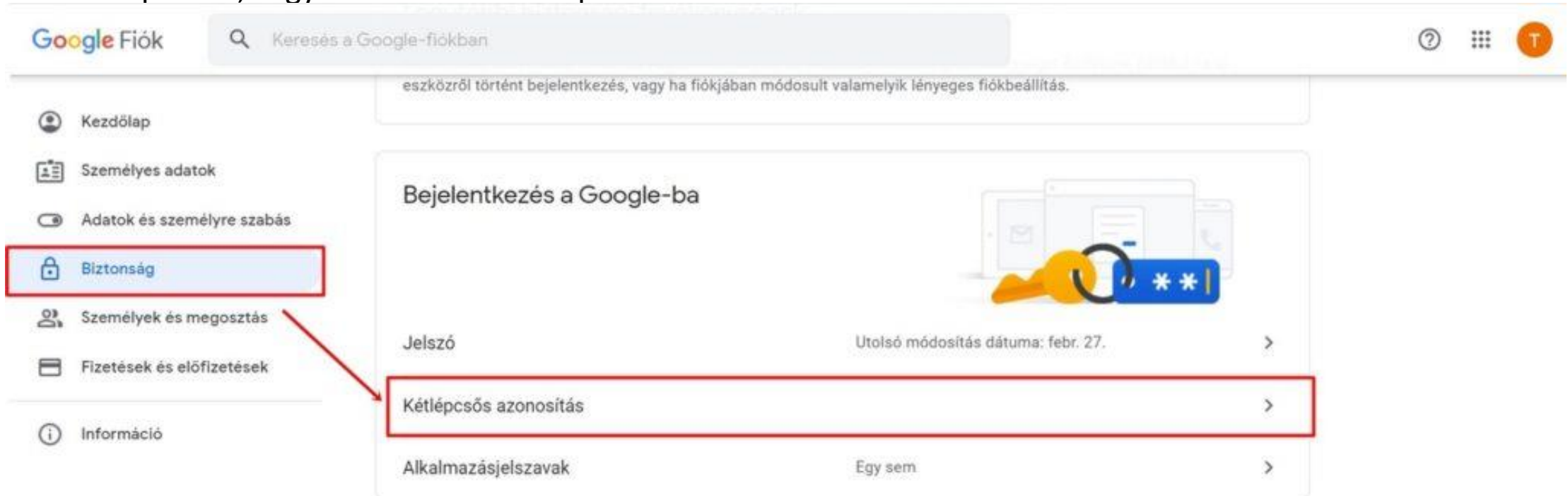
1. Belépési gondok email fiókoknál, közösségi portáloknál

- Lehet, hogy hibásan írtad be a jelszót! Az elmentett jelszavakkal ritkán foglalkozunk, ezért feledésbe merülhetnek. Legyen felírva egy noteszbe!
- A nagy email és közösségi portál szolgáltatók figyelik, hogy milyen IP címről akar belépni használójuk a fiókjába. Ha szokatlan IP címről próbálsz bejelentkezni, akadályokat gördítenek eléd – még helyes jelszó esetén is!
- Nyilvános WIFI-ről (nem titkosított kapcsolat) szintén nem engednek be!
- Ha többször is téves jelszót adsz meg, **felfüggeszthetik a fiókodat** is, tehát máshonnan sem fogsz tudni belépni, amíg nem igazolod azonosságod!
- **Ezért javaslom, csak a megszokott helyszínekről lépünk be fiókjainkba!**



A kétlépcsős azonosításról

- Tény, hogy nagyon idegesítő, de a szolgáltatók a mi fiókunk védelmében alkalmazzák!
- Azt jelenti, hogy a belépési kísérletet követően egy másik eszközünkre, általában a telefonunkra küldenek egy értesítést. Ez alapján igazolnunk kell, hogy valóban mi akarunk belépni. Ameddig ez nem sikerül, addig nincs belépés.
- Zavaró tényező a folyamat során, hogy a szolgáltató szinte mindig hibás helyszínekre állítja (nálam legalábbis), hogy utoljára honnan próbált valaki a fiókunkba bejelentkezni.
- Itt lehet kikapcsolni, vagy módosítani a kétlépcsős azonosítást:



The background of the slide is a dense, repeating pattern of small triangles in various colors including green, blue, purple, and yellow, set against a dark background. The triangles are arranged in a way that creates a sense of depth and texture.

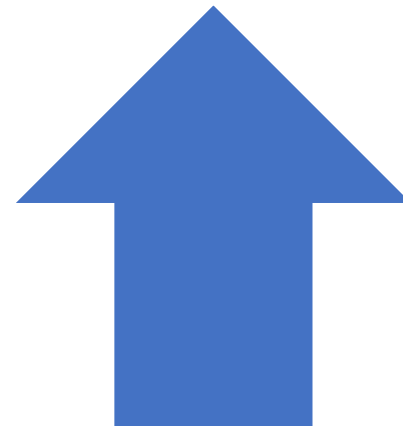
Egyetlen noteszbe, és ne
apró cetlikre, és ne is
naptárba jegyezzük fel
felhasználóneveinket,
jelszavainkat!

Fontos, hogy
minden ilyen
azonosító együtt
legyen, és persze
tudjuk, hová
tesszük.

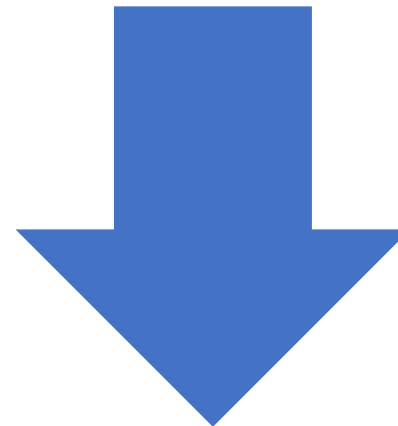
Ne osszuk meg
másokkal, csak
ha nagyon
szükséges!

2. Hogyan ne veszítsük el fontos fájljainkat, dokumentumainkat, képeinket? Hová történjen a mentés?

- Javasolt, hogy **legalább két helyre** mentsünk, amelyek ráadásul fizikailag távol vannak egymástól.
- Így, ha az egyik információhordozó megsérülne, akkor is megmarad minden anyagunk.



Felhő alapú tárhelyre
(Google Drive, vagy
Microsoft-féle One
Drive)



Külső winchesterre
(és nem a
számítógépre)



Melyik miért jó? - Felhő

- A felhő alapú tárhely előnye, hogy mind telefonunkról, mind számítógépeinkről elérhetővé válik a mentett anyag.
- Nem foglal számottevő tárhelyet a készülékünkön
- Az ingyenes tárhelyhasználat azonban kisebb kapacitást jelent. A Google Drive 20 GB-ot, a Microsoft OneDrive csupán 5 GB-ot ad.
- Én mindkettőt ismerem, használom, mégis utóbbit kedvelem, és fizetek is a Prémium szolgáltatásokért. Egyebek mellett 1000 GB tárhellyel rendelkezem a Microsoftnál.
- Hátrányuk ugyanakkor, hogy internetkapcsolat nélkül elérhetetlenek fájljaink számunkra.



Melyik miért jó? – Külső winchester / merevlemez

- Egy külső winchester szintén bármilyen, általam használt számítógéphez csatlakoztatható.
- Nem igényel internetkapcsolatot.
- Kapacitása nagyobb lehet, mint akár a számítógép merevlemeze.
- Ezek az anyagok titkosabban tároltak, kizárólag számunkra érhetők el, nem úgy, mint a felhőben tároltak. (Szolgáltató hozzáfér, + időnként feltörnek, megszereznek jelszavakat)
- Amennyiben valamilyen kártevő férkőzik a számítógépünkre, és a vírusirtó nem tudná eltávolítani, egyszerűen helyreállítható a Windows, a gépen tárolt fájlok pedig mind megsemmisíthetők. A külső winchesterünkön eközben minden rendben megtalálható maradt.
- Egy pendrive meghibásodása esetén olvashatatlaná válik. Egy külső winchesternél ilyen esetben még helyreállítható a teljes tartalom.

3. Milyen védelem legyen
okoseszközeinken, számítógépeinken?





Számítógép, okostelefon, tablet

- Minden okoseszközre szükséges valamilyen védelmet alkalmazni!
- Lehet, hogy eszközünkön előtelepített alkalmazás van erre a célra. Ha nincs, le kell tölteni egyet.
- Csak megbízható, ismert vírusirtó alkalmazást töltsünk le!
- Szánjunk arra időt, hogy ellenőrizzük, milyen alkalmazás végzi a kártevők kiszűrését.
- Ne felejtjük el, hogy időnként vizsgálatot kell futtatni az eszközön.



Az okostelefonok / tabletek speciális helyzete

- Mind a Google (Androidos készülékek), mind az Apple (iPhone, iPad készülékek) ragaszkodnak ahhoz a régi keletű állításukhoz, hogy sürgősszerűen külön vírusirtót telepíteni a telefonra, mivel a letöltéseket kizárólag a saját webáruházukból engedik meg, azt pedig előzetesen ellenőrzik, megszűrik.
- Sajnos ez nem így van, időről időre átcsúszik a védelmi kapujukon néhány, magát hasznos programnak álcázó alkalmazás. Akik letöltik, azoknak valamilyen módon kárt okoznak.
- A kínai telefonokban (Huawei, Honor) évek óta van eleve vírusvédelem. A koreai Samsung készülékekben szintén van már, a McAfee és a Samsung közös alkalmazása.
- Futtatni kell időnként vizsgálatot!

Zavarba ejtő kínálat a Google Play-en. Melyiket választanád? Az ismert fejlesztő termékét, vagy egy „noname” alkalmazást? Az elég, ha egy fejlesztő saját applikációját jónak, hasznosnak mondja? Mindegy, csak ingyen legyen?



AVG Vírusirtó & Védelem
AVG Mobile
4,8 ★



Avast Antivirus & Biztonság
Avast Software
4,8 ★



Vírusirtó - Telefontisztító
Phone Cleaner, Booster & Antivirus Tools
4,4 ★



ESET Mobile Security Antivirus
ESET
4,8 ★



Security Antivirus Max Cleaner
Power Both App Inc.
4,7 ★



Antivirus - Takarítás + VPN
TarrySoft
4,8 ★

Gyanús jelek ...

- Ha a telefonod gyakran önállósul, és mindenféle reklámokat, nem kívánt tartalmakat mutat a kívánt alkalmazás helyett, az legyen gyanús!
- Nagyon lassú a telefonod az applikációk használatakor? Ez szintén intő jel!
- Amikor túl kevés már a tárhely a készüléken, az kártevő jelenléte nélkül is okozhat működésbeli problémákat. Ezért nem szabad megvárni, amíg betelik a tárhely!
- Ha gyanakszol, hogy valószínűleg valamilyen kártékony alkalmazás van a készüléken, vizsgálatot kell végezni! **Amikor egy vizsgálat 10 másodpercen belül véget ér egy készüléken, az valójában semmit sem ér, csak porhintés a szembe!**
- Bizonyosság esetén célszerű a telefont alaphelyzetbe állítani! *(Beállítások / Fiókok és biztonsági mentés / Visszaállítás)* Ezzel visszaállítjuk a gyári beállításokra a készüléket, és a rendszer garantáltan eltávolít majd minden, nem odavaló alkalmazást.

Windows Biztonság – az operációs rendszer részeként

- Előfordulhat, hogy már az üzletből úgy kerül haza a számítógép, hogy rátelepítettek egy időkorlátos, fizetős vírusvédelmet. 30 nap után pedig pénzt vár tőlünk a munkáért – pl. a McAfee.
- **Pedig a Windows 10-es, 11-es gépekben eleve ott van egy komplex, valós idejű biztonsági védelem, amelyet a fenti védelem azonnal kikapcsol.**
- Ha eltávolítjuk az állandóan vásárlásra agitáló, időkorlátos szoftvert, a Windows biztonsági rendszere azonnal visszakapcsolja magát.
- Innentől már biztonságban vagyunk, de minden nap tegyük lehetővé a vírusadatbázis frissítését!
- Előfordulhat, hogy hitelt adtunk egy rosszindulatú emailnek, és a kattintással fertőzést okoztunk a gépen, ezeket elcsípi majd. Ha nem boldogulna vele, akkor is jelzi, és azokban az esetekben a gép helyreállítása, alaphelyzetbe állítása is segíthet.

Védelmi területek



Vírus- és veszélyforrás-kezelés
Nincs szükség intézkedésre.



Fiókvédelem
Nincs szükség intézkedésre.



Tűzfal és hálózatvédelem
Nincs szükség intézkedésre.



Alkalmazás- és böngészőszabályozás
Nincs szükség intézkedésre.



Eszközbiztonság
Nincs szükség intézkedésre.



Eszközteljesítmény és -állapot
Az eszköz állapotáról készít jelentéseket.



Családi beállítások
Szabályozhatja, hogy a család tagjai
hogyan használják eszközeiket.



4. Online vásárlás és bankügyek intézése körültekintően. Lehetséges ez?

- Csak ismert webáruházból vásárolj, a hirdetések gyakran félrevezetők!
- Email-es ajánlatoknál légy óvatos! A kattintásod következménye lehet más is, mint amire számítasz! Informáld le előbb az ajánlatot adó webáruházat! Ha nincs székhely megadva, vagy túl kevés a céginformáció, az legyen gyanús!
- A biztonságos vásárlás és banki átutalás alapvető követelménye, hogy a készülék, amelyről a vásárlást indítod, kártevőtől, kémprogramoktól mentes legyen! Erről neked kell gondoskodnod!
- Pénzintézeted pedig gondoskodik arról, hogy a használandó alkalmazás elég biztonságos legyen. Amikor az alkalmazás frissítést kér, tedd lehetővé azt!
- Biztosan hallottad már százszor is, hogy banki alkalmazott sem telefonon, sem emailben nem kérheti el a belépési azonosítót!

Addig jár a korsó a kútra, míg el nem törik?

„Nem szükségszerű, hogy az éveken át történő online vásárlások és interneten történő bankolások előbb-utóbb anyagi veszteséghez vezetnek!

Engem sosem ért kár sem a számítógépen keresztüli internetbankolás, sem mobiltelefonon történtő vásárlások, utalások során, immár sok-sok év óta. Igaz, eszközeim biztonságosságára mindig odafigyeltem.”



Utolért egy
zsarolóvírus? Mit
lehet tenni, és mit
nem érdemes?

Zsarolóvírusok 1.

- Ezek a kártevők olyan módon okoznak fertőzést, hogy számítógépünk, okostelefonunk fájljait átnevezik másféle fájltypusra, így a szokásos alkalmazásokkal lehetetlen lesz megnyitni őket. A számítógépes programok nem fogják felismerni a fájlokat, amelyeket akár egy órával azelőtt még használtunk, nézegettünk.
- Más zsarolóvírusok pedig zárolják eszközeinket (akár egy okostévé is), tehát használhatatlanná válnak számunkra.
- A fertőzést követően egy vírusirtó képes lehet ugyan eltávolítani az adott vírust, de nem fogja tudni dekódolni az átnevezett fájlokat.
- A dekódolásért cserébe pénzt követelnek a heckererek. Hogy biztosan értesüljünk erről, több mappában is elhelyeznek ilyen tartalmú üzenetet, amellyel találkozni fogsz fertőzés esetén.
- Elveszíteni emlékeinket, fontos digitális iratainkat igen nagy veszteség!
- Mégsem tanácsos fizetni, hiszen semmi garancia, hogy megtörténik a helyreállítás. Ha fizetünk, még inkább kedvet kapnak a heckererek további támadásokhoz.

Zsarolóvírusok 2.

- Jó tudni, hogy megfelelő védelem esetén a károkozás helyrehozható váltságdíj megfizetése nélkül is.
- Például ha van felhő alapú tárhelyünkön fájljainkról automatikus másolat, vagy más adathordozón. *(Utóbbi esetben nem automatikus a másolatok mentése, nekünk kell megtenni folyamatosan.)*
- A Microsoft-féle One Drive zsarolóvírus-fertőzés esetén is megoldást kínál fájljaink visszanyerésére. Ehhez azonban megfelelő méretű tárhely szükséges!
- Fontos odafigyelni eszközeink rendszeres frissítésére (operációs rendszer, illesztőprogramok, biztonsági intelligencia) , és akkor minimalizáljuk a kockázatot.
- Ha mégis utolérne egy zsarolóvírus bennünket, látogassunk el a következő oldalra: <https://www.nomoreransom.org/hu/index.html>
- Innen letölthető számos dekódolási szoftver az egyes zsarolóvírusokhoz.
- A zsarolóvírussal nem tévesztendő össze a zsaroló email, amelyben pl. azzal fenyegetnek, hogy nyilvánosságra hoznak rólad intim helyzetben készült videókat, fotókat. Ez legtöbbször csak blöff, amely révén könnyen szerzett pénzhez akar jutni az email feladója. Persze más a helyzet, ha valóban rendelkeznek ilyen, kompromittáló fájlokkal ☹ .



NO MORE RANSOM

SEGÍTSÉGRE VAN SZÜKSÉGE

készüléke vagy fájljai
visszanyeréséhez,
miközben nem sze-
retne fizetni a
támadóknak*?

IGEN

NEM

Jelenleg nincs megoldás minden zsarolóvírus ellen. Az oldalon folya-
matosan közzétesszük az újabb kulcsokat és alkalmazásokat, ezért
figyelmes időközönként visszalátogatni.

Címlap

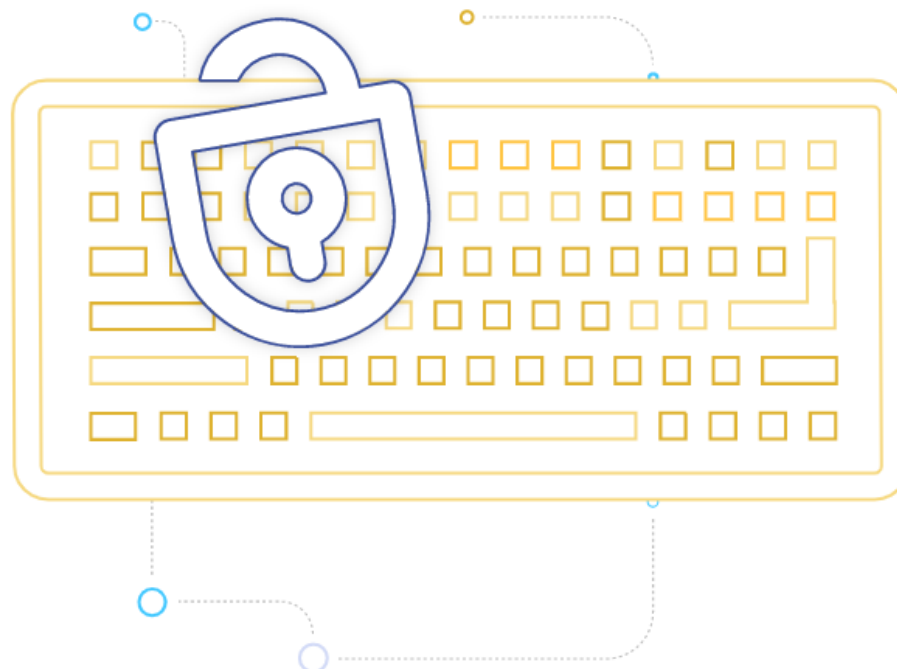
Crypto Sheriff

Gyakori kérdések a zsarolóvírusról

Megelőzési tanácsok

Dekódolási eszközök

Bűntény bejelentése



A zsarolóvírusok a kártevők a
portját alkotják, amelyek záró
számítógépeket és a mobilké
ket, vagy titkosítják a rajtuk t
fájlokat. Ezt követően az áldo
váltságdíj megfizetése ellenél
het hozzá az adataihoz.

**A titkosítás feloldása
azonban semmiféle g
cia nincs, ezért sosem
lott fizetni a zsarolók**

OLDAL TETEJÉRE



Új dekódolási megol-

Köszönöm a figyelmet!

szilassi.andrea@jmvk-komarom.hu