



SOMOGY MEGYEI RENDŐR-FŐKAPITÁNYSÁG
Elektronikus Lakossági Bűnmegelőzési Információs
Rendszer
ELBIR HÍRLEVÉL



Az Internet veszélyei

Napjainkban egyre fontosabb gyermekeink védelme az Internet káros tartalmaival szemben. A felnövekvő nemzedék otthonosan mozog az Internet világában, azonban egyre többször találkozhatunk megtévesztő, hamis, erkölcsi – és szellemi fejlődésre káros tartalmú weboldallal.

A gyermekek képtelenek helyesen szűrni és értékelni a kapott információt, megkülönböztetni az értékest és az értéktelent. Védelmüket legjobban a szülői felügyelet szolgálhatja, valamint rendelkezésre



állnak egyéb szűrőprogramok is, azonban a technikai megoldások teljes mértékben nem helyettesíthetik a szülői felügyeletet. Ennek érdekében az Internetet használó gyermek szüleinek kell az Internet használatával és tartalmával megismerkednie, mert így válhat képessé arra, hogy gyermekével megbeszélje azokat a kérdéseket, problémákat, amelyeket a gyermek észlel. A káros weboldalak elkerülése érdekében fontos, hogy a szülő irányítsa

a gyermek Internetes tartalmakkal kapcsolatos érdeklődését, legyen segítségére felfedezni azokat a honlapokat, amelyek a gyermekek számára hasznosak, káros tartalmaktól mentesek.

Ajánlás szülőknek:

1. A szülő érdeklődjön, ha a gyermek valamilyen általa felfedezett Internetes újdonságról számol be!
2. Szakítson időt közös szörfözésre, így gyermekét hozzászoktathatja ahhoz, hogy az Internetezés közös program is lehet!



3. A káros tartalmak elleni védekezéshez használjon szűrőprogramokat, az ilyen tartalmú oldalakra jellemző kulcsszavak alkalmazásával, vagy egyes weboldalak címei alapján le lehet tiltani azok látogatásának lehetőségét!

4. Fontos annak tudatosítása, hogy a chatszobában való beszélgetés, ismerkedés során előfordulhat, hogy egyes személyek másnak adják ki magukat, nem a valóságnak megfelelő adatokat közölnek magukról!

5. Amennyiben tudomására jut, hogy gyermekét bármilyen formában zaklatják az Interneten keresztül, forduljon a rendőrséghez!



Ajánlás gyermekeknek:



1. Amit a világhálóra feltöltünk, az örökre ott marad!
2. Gondolj meg, hogy milyen képeket raksz fel magadról, családotról a közösségi oldalakra!
3. Mindig más regisztrációs nevet és jelszót használj, jelszavaidat folyamatosan változtasd!
4. Soha ne jelöld be a jelszó megjegyzése részt!
5. Internet kávézóban vagy wifi pontról ne intézz személyes ügyeket!
6. Ne hagyd őrizetlenül a számítógéped, ne maradj bejelentkezve, amikor nyilvános helyen chatelsz!
7. Erotikus tartalmú képeket soha ne küldj senkinek, mert bárki bármikor visszaélhet vele!

Tanácsok felhasználóknak a zsarolóvírusokról:

Az elmúlt években egyre elterjedtebbé váltak a zsarolóvírus programok, melyek közös jellemzője, hogy váltságdíjat követelnek az adathordozókon általuk titkosított állományok hozzáféréseért vagy a teljesen lezárt rendszer, illetve a blokkolt internet feloldásáért. A fizetést követően a titkosítás feloldásához szükséges információkat csak az esetek elenyésző részében adják meg a kiberbűnözők.

A titkosítás jellemzően feloldhatatlan. Az egyetlen megoldás a megelőzés, ennek érdekében az alábbi tanácsokat érdemes megfogadni:

1. Rendszeresen külön meghajtóra készítsen számítógépének adattartalmáról biztonsági mentést, vagy állítsa be rendszerét úgy, hogy a számítógép újraindításakor a rendszere végezze el a biztonsági mentést!
2. Rendszeresen frissítse operációs rendszerét, vírusirtóját!
3. Ne nyisson meg olyan elektronikus leveleket, amelyek feladója ismeretlen!

4. Ne dőljön be a felugró ablakokban található állítólagos rendőrségi hivatkozásoknak, mivel a rendőrség nem alkalmaz ilyen megoldásokat, ezért semmilyen befizetést ne kezdeményezzen!
5. Ne töltsön le és ne telepítsen nem megbízható, nem hivatalos weboldalról szoftvereket!
6. Fokozott óvatossággal böngéssze a felnőtt és warez tartalmakat terjesztő oldalakat! A vírusok túlnyomóan az ilyen oldalak látogatását követően fertőzi meg a felhasználók gépeit.



A legelterjedtebb zsarolóvírus blokkolja a fájlokat, majd egy figyelmeztetést jelenít meg, amin keresztül egy megadott határidőig több száz dolláros „váltásdíjat” követel. A programot szinte lehetetlen eltávolítani. A káros programok elsősorban a kódot tartalmazó weboldalak vagy gyakran hivatalosnak tűnő, például elmulasztott befizetésekkel, adózással, vásárlás-visszaigazolással kapcsolatos üzenetek csatolmányainak megnyitásával települnek. Az esetek többségében nincs olyan ismert módszer vagy eszköz, amellyel a titkosítás feloldható, de egyes káros programok bizonyos verziói esetében van lehetőség az eredeti fájlok legalább részleges visszaállítására. Ez történhet például célszoftverrel vagy törölt állományok visszaállításával.

A legújabb, legfejlettebb rosszindulatú programokat sok biztonsági szoftver nem érzékeli, és nem tudja elhárítani, így az egyetlen hatékony védekezés a megelőzés. Az adatokról minden esetben szükséges rövid időközönként háttérmentést készíteni, illetve szűrni kell a meglátogatni kívánt weboldalakat, valamint az e-maileket. Elengedhetetlen a jogtisza és naprakész operációs rendszer és vírusirtó szoftver telepítése a számítógépre.

Ha a leírtakkal kapcsolatban tanácsra, segítségre van szüksége, hívjon bennünket az alábbi elérhetőségeken, vagy a 112-es és 107-es segélyhívó számokon!



SOMOGY MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNÜGYI IGAZGATÓSÁG
Bűnmegelőzési Osztály

7400 Kaposvár, Szent Imre u. 14/c. Pf.:121
TEL:82/502-700-2732, FAX:82/502-700-2772
E-mail:bunmeg@somogy.police.hu

