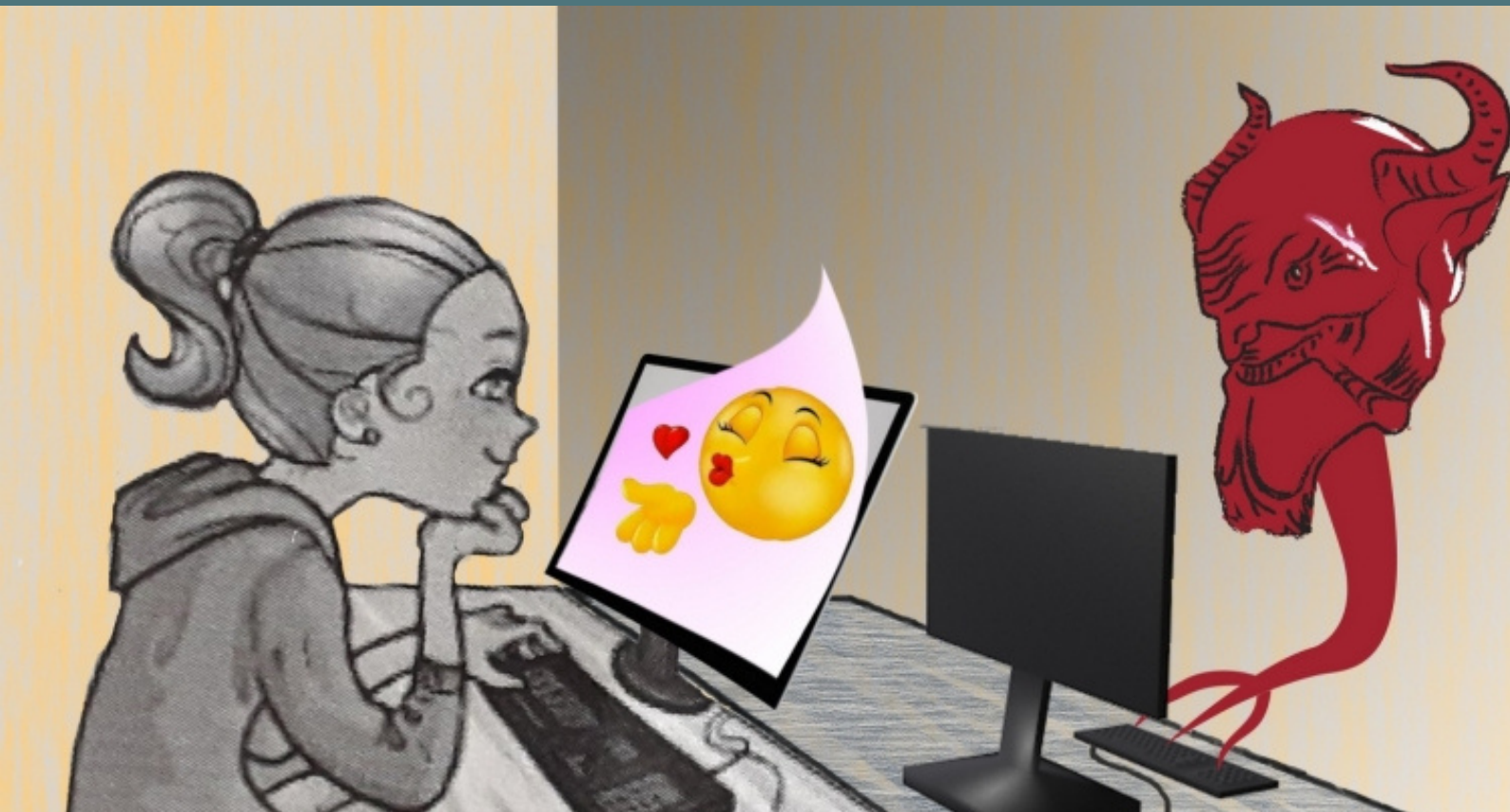


# ELBIR

Elektronikus Lakossági Információs Rendszer  
2021. február



## SID

SAFER INTERNET DAY

A közösségi média  
veszélyei

Az ingyenes wifi  
hálózat hátulütői

Online zaklatás



## BIZTONSÁGOS INTERNET NAP SAFER INTERNET DAY FEBRUÁR 9.

A "Safer Internet Day"-t, vagyis a Biztonságos Internet Napját világszerte február második keddjén rendezik meg. A program célja, hogy felhívja a figyelmet az online technológiák tudatosabb és biztonságosabb használatára. A Jász-Nagykun-Szolnok Megyei Rendőr-főkapitányság bűnmegelőzési munkatársai ebből az alkalomból néhány ajánlást fogalmaznak meg a felelősségteljes internethasználatról. Felhívják a szülők és a gyerekek figyelmét az interneten történő barangolás veszélyeire.

### A közösségi média veszélyei

#### A szülők szerepe

A közösségi média hasznos lehet, ha az ember felelősségteljesen, kellő óvatossággal használja. Fontos, hogy mind a szülők, mind pedig a gyerekek tisztában legyenek a különböző veszélyekkel. Beszélgessenek el a gyermekekkel az internet használatának lehetőségeiről és példákkal illusztrálva hívják fel a gyerekek figyelmét a veszélyekre!

#### Idegenek az online térben

A gyerekeknek tisztában kell lenniük azzal, hogy ahogyan az utcán, úgy az interneten sem mindenki az, akinek mondja magát, vagy akinek látszik. A virtuális világban kötetett barátságok gyakran nem állnak közel a valósághoz és valódi, személyes kapcsolat nélkül sohasem lehetünk biztosak a „vonal” másik oldalán ülő személyben.



**Akik eddig  
gondolkodás nélkül  
csatlakoztak  
bármilyen publikus  
wifi hálózathoz,  
fontolják meg  
tanácsainkat!**



### **Túl sok információ megosztása**

Bizonyos közösségi oldalak elvárják, hogy a felhasználók minél több személyes információt adjanak meg magukról. Sajnos sokan jóval többet árulnak el, mint amennyi biztonságos lenne, ez pedig különösen veszélyes lehet a gyerekekre nézve.

### **Tartózkodási hely megadása**

A szülőknek ellenőrizniük kell, hogy gyermekeik ne tegyék nyilvánossá azt, hogy éppen hol tartózkodnak, hol laknak és melyik iskolába járnak. A gyerekeknek meg kell érteniük, hogy ezek az információk segíthetnek a rossz szándékú embereknek abban, hogy személyesen is felkereshessék őket!

### **Hosszútávú problémák**

Van egy mondás az internetről, miszerint ha valami egyszer felkerül oda, akkor az ott is marad. Minden interneten közzétett információról, képről, bejegyzésről és más tartalomról is ezt kell feltételezni. Lehetőség van a feltöltések törlésére, de nem lehet tudni, hogy ezeket előzőleg nem töltötte-e le valaki, például későbbi zsarolás céljából. Szülőként erről is el kell beszélgetni a gyermekekkel, mert a meggondolatlan döntéseknek hosszútávú következményei lehetnek.

### **Felhasználói fiók biztonsága**

Az illetéktelen hozzáférés megelőzése érdekében válasszon megfelelő jelszót, amely nem kapcsolódik a személyéhez. A különböző oldalak többféle lehetőséget biztosítanak a felhasználói fiókok védelmére. Ismerjék meg ezeket, és válasszák ki a megfelelőt! A közösen használt számítógépen (iskolában, munkahelyen, ismerősnél, nyilvános helyen) mindig jelentkezzon ki a felhasználói fiókból! A böngésző bezárása nem elegendő, mivel az oldal újbóli megnyitása esetén automatikusan belép az utoljára használt felhasználói fiókba. A legfontosabb szabály, hogy kellően érett, felkészített korosztály használja a számítógépet, különösen az online felületeket! A szülők feladata és egyben felelőssége, hogy nyomon kövessék a gyermekük által látogatott tartalmakat és azt lehetőség szerint, a kifejezetten ezt a célt szolgáló szűrőprogramokkal, alkalmazásokkal kontrollálják!

### **Az ingyenes wifi hálózat hátulütői**

#### **Veszélyes az ingyenes wifi?**

Ingyenes wifi szolgáltatás szinte már mindenhol elérhető, de ha felelőtlenül használják, annak súlyos ára lehet. Publikus wifi hálózatra csatlakozáskor a böngészés során megadott adatok nem titkosított csatornán „közlekednek”, ezért veszélyben vannak. Viszonylag egyszerűen rájöhethet valaki, hogy az illető milyen oldalakat látogat, de belenézhet az üzeneteibe vagy megszerezheti a jelszavait is, ezért alaposan meg kell gondolni, hogy hogyan és pontosan mire használja az ingyenes internetezési lehetőséget!

#### **Mielőtt nyilvános wifi hálózatra csatlakozik:**

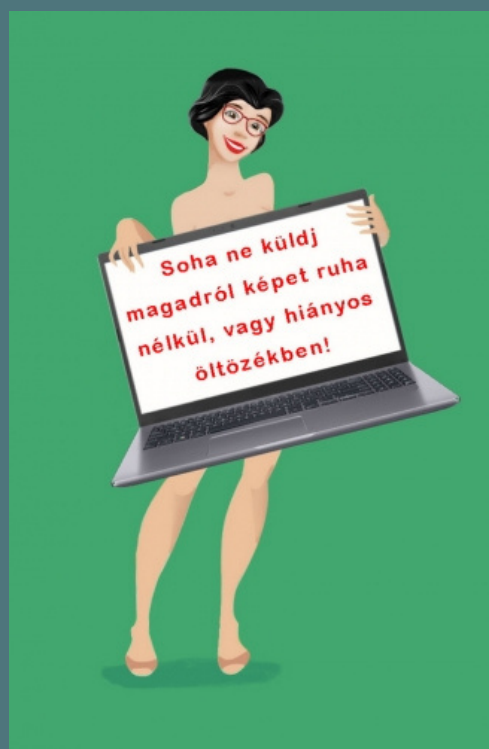
- Eszközén kapcsolja ki a fájlmegosztó funkciót, hogy biztonságban legyenek a dokumentumai!
- Kizárólag a <https://> előtagú honlapokat nyissa meg!
- Használjon tűzfalat! Ha nem rendelkezik ilyennel, akkor ajánlott telepíteni a védelmi funkciót az eszközére!
- Kapcsolja ki eszközén a publikus wifi hálózatra történő automatikus kapcsolódást!

#### **Az alábbiakat soha ne tegye, ha publikus wifire csatlakozik:**

- Kerülje az online vásárlásokat és banki ügyintézéseket!
- Ne küldjön személyes adatokat és információkat tartalmazó üzeneteket!
- Ne továbbítson munkahelyi információkat a nyílt hálózaton!
- Ne frissítse eszközeit, hiszen sok esetben valódinak látszó, de igazából hamis frissítések ugorhatnak fel a képernyőn, amik telepítésével valójában rosszindulatú programok kerülhetnek az eszközeire!



**Fontos tudni, hogy 18 év alatti személyekről tilos szexuális tartalmú képet készíteni, ilyen képeket, videókat továbbadni, megosztani! Komoly jogi következményekkel, feljelentéssel is számolnia kell annak, aki akár csak viccből, mást meztelenül vagy intim helyzetekben ábrázoló képeket küldözget vagy tölt fel az internetre.**



## Online zaklatás (Cyberbullying)

Az internetes zaklatásnak bárki áldozatul eshet, de legjobban a fiatal korosztályt veszélyezteti. A zaklatás célja lehet a fiatal megalázása, fenyegetése, nevetségessé tétele, kiközösítése. A háborgató jellegű bejegyzéseket jelenteni lehet az oldal üzemeltetőjének. Javasoljuk, hogy ilyen esetben mindenképpen éljenek ezzel a lehetőséggel!

### A zaklatás formái:

- A fiatal bántó, sértő, fenyegető üzeneteket kap egy közösségi oldal üzenőfalán vagy privát üzenetben.
- Feltörik az e-mail jelszavát, vagy a közösségi profil jelszavát és a nevében írnak ismerőseinek olyan üzeneteket, amiket ő vállalhatatlannak tart, vagy épp közzéteszik a titkait és hasonlók.
- Előfordulhat, hogy egy „álprofil” hoznak létre, ahol az ő nevében írnak, vagy adatokat, információkat adnak meg vele kapcsolatosan.
- Feltehetnek róla olyan képet, videót, ami kényelmetlen helyzetbe hozza.
- Terjeszthetnek a személyéről álhíreket, rosszindulatú pletykákat.

### Az online bántalmazás jelei:

- Az internet-használati szokásaiban változást vesznek észre – sokkal kevesebbet netezik, bezárkózik.
- Rosszkedvű, ideges, ingerült lesz, miután internetezik.
- Barátai elkopnak, nem mozdul ki szívesen.
- Csökken az önértékelése, negatív gondolatai vannak saját magáról (esetleg csúnyának, értéktelennek érzi magát).
- A szokásos szabadidős tevékenységeit, hobbijait elhanyagolja.
- Az iskolai teljesítménye romlik, nem tud koncentrálni.
- Magába zárkózik, nem közlékeny, nem osztja meg élményeit.
- Törli a közösségi oldalon létrehozott profilját.

### Mit tehet a szülő?

- A szülő elsődleges eszköze az odafigyelés és a beszélgetés. Fontos, hogy az internetről történő beszélgetés jelen legyen a családkommandóiban. A gyerekek azt érezhessék, hogy nyugodtan megoszthatnak bármit a szüleikkel, és nem lesz részük elutasításban, megrovásban.
- Legfontosabb, hogy tisztában legyen a gyermeke az online zaklatás tartalmával.
- Támogassa gyermekét és közösen keressenek megoldást a helyzetre.
- Készítsenek a zaklató üzenetekről képernyőmentést, illetve tiltsák le a zaklatót! Ha a zaklatás folytatódik (esetleg más felhasználói fiókkal vagy más csatornán), forduljanak a rendőrséghez!

### Sexting (Szexuális tartalmú, erotikus, meztelen vagy félig meztelen képek)

A tinik egy része szereti megmutatni egyre nőiesebbé – férfiasabbá váló testét a kortársainak, barátainak. A súlyos probléma az, hogy a megosztott képekkel bárki visszaélhet. Előfordulhat, hogy pornográf oldalakra is átteszik (nem ritkán névvel, telefonszámmal együtt), például szexhirdetésként.

### Mi lehet a megoldás?

- Ebben az esetben is igaz az, hogy a legjobb a megelőzés!
- Figyelmeztessék a gyerekeket, hogy a közösségi portálokra körültekintően helyezzenek fel fényképeket, kerüljék a saját magukat vagy másokat kellemetlen helyzetbe hozó fotók/videók feltöltését, hiszen, amit egyszer feltöltenek az internetre, annak örökre nyoma marad, azokhoz bárki hozzáférhet, így azzal bármikor visszaélhet!
- Azt is tudatosítsa gyermekében, ha mástól kap ilyen fotókat, videókat, ne küldje tovább, inkább hívja fel a küldő figyelmét is a sexting veszélyeire!





# 8 tanács az unokázós csalások elkerülése érdekében

Annak ellenére, hogy számos bűnözői csoportot felszámolt a rendőrség, újabb módszerekkel próbálkoznak a bűnözők. Míg korábban készpénzt és ékszereket kértek, most már banki utalásra is megpróbálják rávenni az időseket.

Az időskorúak megtévesztésére szerveződött bűnözői körök által elkövetett unokázós csalások során a csalók a bűncselekmények elkövetésére ugyanazt a módszert használják. Az időskorú sértetteket a szervezet egyik tagja hívja fel és a beszélgetés során a rokonának adja ki magát. A telefonáló legtöbbször azt állítja, hogy balesetet okozott, és a kár megtérítéséhez azonnal pénzre van szüksége.

Az áldozatokon, hogy elkerülje a közvetlen találkozásokat, meggyőzi a sértetteket, hogy ő nem tud elmenni a pénzért, hanem egy ismerőst küldi el érte. Az idősek lakcímére ezután egy futárt irányítanak, aki átveszi a pénzt, ékszereket. Az utóbbi időkben azonban a bűnözők már arra próbálják rávenni az időseket, hogy ismert pénzküldő hálózatokon keresztül utaljanak el egy meghatározott összeget egy – általában külföldi – bankszámlaszámra. Ha ezt a sértett nem tudja otthonról megtenni, akkor taxit küldenek a lakcímére, ami elviszi egy olyan helyre, ahonnan tud utalni. Olyan eset is előfordult, hogy a bankkártya adatok bediktálását kéri, amivel különböző online tranzakciókat hajtanak végre, jelentős kárt okozva a sértettnek.

**A rendőrség célja, hogy az elkövetési módszer tudatosításával lehetőleg senki se dőljön be a csalóknak. Beszélgessenek minél többet erről idős rokonaikkal, ismerőseikkel, így kisebb eséllyel csaphatják be őket. Mutassák meg hozzátartozóinak a rendőrségi videókat is, amelyek különböző csalási módszereket dolgoznak fel!**

**FIGYELJÜNK IDŐS  
HOZZÁTARTOZÓINKRA,  
ISMERŐSEINKRE!**



## **A RENDŐRSÉG 8 TANÁCSA, HOGY NE VÁLJANAK CSALÓK ÁLDOZATÁVÁ:**

Ha ilyen telefonhívást kap, járjon utána, hogy valóban baj van-e! - Tegye le a telefont, majd hívja fel a hozzátartozóját, akire hivatkoztak!

Soha ne felejtse el: hivatalos személy soha nem kér pénzt! - Se rendőr, se mentő, se tűzoltó.

Tegyen fel ellenőrző kérdéseket, ha bizonytalan, hogy tényleg hozzátartozója hívja-e! - „Hogy hívnak? Mikor születettél? Mikor találkoztunk utoljára?”

Legyen gyanús, ha pénzáttalásra kéri, illetve felajánlják, hogy az utalás lebonyolításában közbenjárnak!

Bankkártyaadataikat semmilyen körülmények között ne adják meg idegeneknek!

Nyilvános helyen, idegenek jelenlétében ne beszéljenek magánügyeikről, mert az idegenek visszaélhetnek az információkkal!

Ne adja meg személyes adatait ismeretleneknek!

Ha felmerül, hogy bűncselekményt próbáltak meg elkövetni Ön vagy hozzátartozója sérelmére, hívja azonnal a 112-es segélyhívószámot!

# "MEGCSALT LELKEK"

Az időseket érintő ingatlancsalások visszaszorítása érdekében a Jász-Nagykun-Szolnok Megyei Rendőr-főkapitányság bűnmegelőzési szakemberei kisfilmmel kampányolnak.

A prevenciós videó megtekintéséhez olvassa be az alábbi QR kódot!

