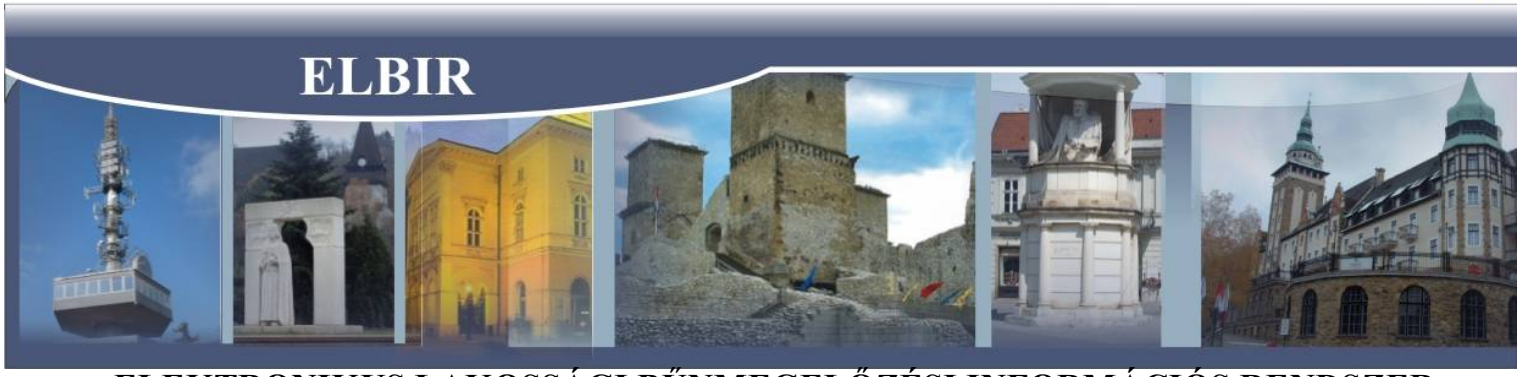

ELEKTRONIKUS LAKOSSÁGI BŰNMEGELŐZÉSI INFORMÁCIÓS RENDSZER

LAKOSSÁGI HÍRLEVÉL

Gyermekeink online biztonsága

2020-ban a Biztonságos Internet Nap február 11. napjára esett. Az esemény célja, hogy felhívja a szélesebb közönség, ezen belül is elsősorban a gyermekek és fiatalok figyelmét a mobiltelefonok és online technológiák tudatosabb és biztonságosabb használatára.

A fiatalok mindennapi használói a világhálónak, a szabadidejük egy részét a közösségi és videómegosztó oldalakon töltik, ahol online tartalmakat böngésznek, osztanak meg másokkal, illetve tartják a kapcsolatot a barátaikkal. Mindezt a legnagyobb természetességgel teszik, azonban abba ritkán gondolnak bele, hogy az ingyenes szolgáltatásért az adataikkal fizethetnek a szolgáltató, fejlesztő felé. Az egyes – ismeretlen forrásból származó – alkalmazások számára olyan hozzáférhetőséget biztosítanak az eszközeik funkcióihoz (pl.: helymeghatározás, kamera indítása), melyekről nincs tudomásuk, hogy milyen adatokat és hová továbbítanak. Az adatvédelmi tájékoztatót sok esetben olvasatlanul lépik át a telepítéskor.

Mindezen túl az online térben fennáll a zaklatás, kiközösítés, megalázás, szexuális jellegű visszaélések veszélye is.

Mit tehet a szülő gyermeke biztonsága érdekében?

- **Legyen nyitott** a gyermeke által kedvelt játékok, alkalmazások, videók megismerésére. Kérje meg, hogy **tanítsa meg önt** ezek működésére.
- Az alkalmazásokkal történő közös ismerkedés során **vesse fel a biztonsági rendszabályok betartását**, ezzel egyben megismeri gyermeke hozzáállását a kérdéskörhöz.
- Ne kötelezni akarja gyermekét az online szabályok betartására, hanem **próbálja vele megértetni, hogy miért fontos ezek követése**. Sokszor a fiatalok át sem gondolják, hogy milyen következményei lehetnek az általuk meggondolatlanul megosztott képeknek, videóknak, kommenteknek.

Mely biztonsági szabályokat célszerű betartani?

- A közösségi oldalak lehetőséget biztosítanak a személyes adatok megadására, amelyek **nem megfelelő biztonsági beállítások esetén mások, akár idegenek számára is láthatóak lesznek**. Mindig mérlegelje, hogy milyen személyes adatot ad meg és azt is, hogy azt ki láthatja. A személyes adatok – mint a születési hely vagy idő, lakcím, családi kapcsolatok – **visszaélésre adnak lehetőséget**, így ezek láthatóságát **érdemes korlátozni**.

- Egy bejegyzés, fénykép szintén tartalmazhat olyan **információt, ami visszaéléshez vagy zaklatáshoz vezethet.** Gondolja végig, hogy valóban szerencsés-e az adott bejegyzést, fényképet megosztani, illetve azt, hogy azt **kikkel osztja meg**. Több közösségi oldalon lehetőség van arra, hogy egy **bejegyzést csak az ismerősök egy részével** (pl. közeli családtagokkal) osszon meg. Mindig tartsa szem előtt, hogy a feltöltött információ, fénykép **interneten történő terjedését nem tudja a továbbiakban kontrollálni**, így az eljuthat idegenekhez is!

GONDOLJA ÁT, MIELŐTT MEGOSZTJA!

1. teljes születési dátum
2. lakcím
3. telefonszám
4. családi állapot és családi kapcsolatok
5. aktuális tartózkodási hely
6. utazási terv
7. olyan információk, amelyeket nem osztana meg családjával, munkatársaival vagy a szomszédjaival
8. munkájával kapcsolatos aktualitások
9. másról készített fotók az adott személy beleegyezése nélkül

- **Ne fogadja el olyan személyek ismerősnek jelölését, akit személyesen nem ismer**. Bármennyire is vonzó a sok „like”, illetve követő. Gondolja meg, hogy a lakásába, mindennapi életébe beengedne-e egy vadidegent, hogy figyelje önt.
- A felhasználói fiókhoz (e-mail, közösségi oldalak, videómegosztók, steam, stb.) való illetéktelen hozzáférés megelőzése érdekében **válasszunk megfelelő jelszót** (pl.: B1zT0n§@Gos J3l§Zo), amely nem kapcsolódik a személyünkhöz. A különböző oldalak többféle lehetőséget biztosítanak a felhasználói fiókok védelmére. Ismerjük meg ezeket, válasszuk ki a nekünk megfelelőt.
- A nem kizárólag az ön által használt számítógépen (iskolában, munkahelyen, ismerősnél, nyilvános helyen) mindig **jelentkezzen ki a felhasználói fiókból. A böngésző bezárása nem elegendő**, mivel az oldal újbóli megnyitása esetén automatikusan belép az utoljára használt felhasználói fiókba. Az ilyen számítógépeken a **felhasználói nevét és jelszavát se jegyeztesse meg a böngészővel**.
- Amennyiben nem elengedhetetlenül fontos, úgy **nyílt wifi hálózaton** (free wifi) **felhasználói fiókjaiba ne jelentkezzen be, internetes bankolást ne indítson.** A nyílt hálózatok biztonsági beállításait, **titkosítását, annak üzemeltetőjét legtöbb esetben nem ismerjük.** Az internetes adatforgalom ilyen esetben nem tudható, hogy milyen eszközön halad keresztül és hol kerül rögzítésre.

Érdekesség

Egy olyan jelszónak, ami **négy karakterből és számokból áll** (mint pl.: a PIN kódok) 10.000 lehetséges változata van és viszonylag **könnyen** feltörhető.

A **nyolc karakterből** álló, kisbetűket és számokat is tartalmazónak, már 2,8 billió kombinációja van. Ennek feltöréséhez is elegendő lehet **néhány óra**.

A **12 karakterből álló, nagybetűket, kisbetűket és számokat, valamint egyéb karaktereket is tartalmazónak**, 96^{12}, azaz 621 trilliárd. Ennek feltörése a jelenlegi legnagyobb teljesítményű számítógéppel is több mint **63 ezer évig tartana**.

- A közösségi oldalak lehetővé teszik, hogy **idegenek is kapcsolatba lépjenek önnel**. Az önmagáról közzétett információk alapján könnyen **csalók céltáblájává válhat**. A csalások jellemző formái: online nyereményjátékokon nyert nagy nyeremény, álom nő/férfi keres párt, csodálatos befektetési lehetőségek, jól fizető külföldi munka. Mindegyik közös jellemzője, hogy mielőtt a nem létező nyereményhez, befektetéshez, stb. hozzáférhetne, előbb pénzt kell utalnia a csalónak.
- A közösségi oldalak könnyen válthatnak az **online zaklatás színtereivé**. A zaklatás megvalósulhat **bántó, fenyegető, gúnyoldó személyes üzenetek vagy csoportban írt hozzászólások formájában, lejáratő, előnytelen képek nyilvánosságra hozatalával**. Az ilyen bejegyzéseket **jelenteni lehet az oldal üzemeltetőjének**. Javasoljuk, hogy ilyen esetben készítsen a zaklató üzenetekről **képernyőmentést**, szakítson meg minden kapcsolatot a zaklatóval, **tiltsa le**, hogy ne tudjon önnel kapcsolatba lépni. Ha a zaklatást folytatja (esetleg más felhasználói fiókkal vagy más csatornán), **forduljon a rendőrséghez**.


Képek forrása: Internet

Cím: 3527 Miskolc, Zsolcai kapu 32. szám; 3501 Miskolc, Pf. 161.
Telefon: (06-46) 514-523, BM: (31) 23-27; Fax: (06-46) 514-500/27-37, BM: (31) 27-37
E-mail: bunmeg@borsod.police.hu