ONLINE GROOMING

A **grooming** angol kifejezés, arra a jelenségre használják, amikor egy felnőtt az interneten keresztül alakít ki kapcsolatot egy gyermekkel, azzal a céllal, hogy szexuális kapcsolatra vegye rá és szexuálisan kihasználja. Az elkövetők legtöbbször úgy cserkészik be a gyerekeket, hogy barátságot vagy szerelmet színlelnek, azért, hogy a fiatal érzelmileg elkezdjen kötődni hozzájuk.

A GROOMING JELLEMZŐI

- A kapcsolat kialakítása során az elkövető a valós személyét, életkorát, nemét sokszor eltitkolja, másnak adja ki magát, mint aki valójában.
- Az elkövetők előszeretettel használják a közösségi oldalakat és a nyilvános chat-szobákat.
- A megosztott személyes információk, különösen a kihívó képek figyelemfelkeltőek az elkövetők számra, és növelik a célponttá válás kockázatát.
- A bizalom elnyerése érdekében hamis, a célszemély számára vonzó információkat közöl magáról (nem, életkor, fénykép, érdeklődési kör), kedvesen viselkedik vele, esetleg kisebb ajándékokat küld.

Az elkövető szándéka sokszor csak akkor lesz nyilvánvaló, amikor a célszemély valamilyen szexuális ajánlatot kap a tőle, vagy az áldozat személyesen is találkozik az elkövetővel, aki erőszakoskodni próbál vele. Előfordulhat az is, hogy a célszemély egy idő után a beszélgetésben kellemetlenül érzi magát, mert az elkövető egyre rámenősebben és tolakodóbban próbálja szexuális tartalmú beszélgetésbe is bevonni. Lehetséges az is, hogy az elkövető intim képeket küld magáról, illetve a másikat is erre kéri.

Az elkövető általában egy olyan felnőtt, aki nála jóval fiatalabbakkal szeretne szexuális kapcsolatot létesíteni.

- Célja, hogy rábírja a neten megismert gyerekeket arra, hogy személyesen is találkozzanak, és akkor – akár – erőszakkal is szexuális kapcsolatot létesítsen.
- További cél lehet, hogy pornográf tartalmú képeket vagy felvételt akar készíteni vagy kérni a gyerektől saját célra, illetve azért, hogy másokkal megossza.
- Az is gyakori, hogy az elkövető a szexuális vágyait a gyerekekkel történő szexuális tartalmú beszélgetésekben, fantáziálásokban éli ki, ezért tart kapcsolatot fiatalokkal.
- Az elkövető a kapott képekkel vagy a beszélgetési előzményekkel zsarolhatja is az áldozatát, hogy az újabb képet, videót küldjön magáról, vagy egyezzen bele a személyes találkozóba és a szexuális kapcsolatba.
- Előfordulhat az is, hogy külföldi munka ígéretével külföldre utaztatja áldozatait, ahol prostitúcióra kényszerítheti.

A MEGELŐZÉS LEHETŐSÉGEI

- Legyen nyitott a gyermeke irányába!
- Tudatosítsa benne, hogy megbízhat Önben és számíthat a segítségére!
- Beszélgessen vele az online tér veszélyeiről és az ottani biztonsági szabályokról!
- Hívja rá fel a figyelmét, hogy az interneten bárki mondhatja magát bárkinek.
- Akit személyesen nem ismerünk az idegen, még ha az interneten rendszeresen beszélgetünk is vele.
- Tanítsa meg gyermekének, hogy ne tegyen közzé és ne osszon meg mással kihívó képet, idegennel pedig semmilyen személyes információt (adatot, képet, stb.)
- Ha találkozni akar valakivel, akit online ismert meg, mindig szóljon előtte Önnek, és csak az Ön engedélyével és jelenlétében találkozzanak!
- A fentiek alól nincsenek kivételek!

MIT TEGYEN GROOMING ESETÉN?

- A gyermek szóljon a szülőjének, ha
  - egy beszélgetés során veszélyben, fenyegetve vagy kellemetlenül érzi magát,
  - szexuális tartalmú beszélgetést kezdeményeznek vele,
  - fényképeket kérnek tőle vagy személyes találkozóra hívják.
- Tiltsák le a felhasználót!
  Mentsék le az üzeneteket, beszélgetéseket képernyőmentéssel!
- Jelentsék a honlap üzemeltetőjének!

Ha az elkövető zaklatja vagy fenyegeti gyermekét üzenetekkel, forduljon a rendőrséghez!

112 SOS

ONLINE MEGFÉLEMLÍTÉS

Az **online megfélemlítés** (online bullying) során a célszemély sorozatosan és hosszabb ideig fennálló szándékos sérelem okozás áldozatává válik az interneten vagy mobiltelefonon keresztül.
Ennek célja a célszemély fenyegetése, nevetségessé tétele, kiközösítése, lejáratása, negatív színben feltüntetése. Az online és az offline világban előforduló megfélemlítés között átfedés van: általában azokat zaklatják az interneten, akiket az iskolában is piszkálnak, bántalmaznak.

JELLEMZŐ ELŐFORDULÁSI FORMÁK

- A célszemély bántó, sértő üzeneteket kap Facebook-üzenőfalán vagy személyes üzenetben.
- Lejáratók üzeneteket, kommenteket írnak róla nyilvános üzenőfalon vagy zárt csoportban.
- Egy „álprofilt" hoznak neki létre, ahol az ő nevében írnak, vagy adatokat, információkat osztanak meg róla.
- Megszerzik az e-mail vagy közösségi profil jelszavát, és az ő nevében írnak az ő ismerőseinek olyan üzeneteket, amiket ő vállalhatatlannak tart, vagy közzéteszik a titkait.
- Feltehetnek róla olyan képet, videót, ami kényelmetlen helyzetbe hozza, terjeszthetnek róla álhíreket, rosszindulatú pletykákat.

Az online megfélemlítés elsősorban, de nem kizárólag a fiatalabb korosztályt érinti. Ennek egyik magyarázata az életkori sajátosság, illetve az, hogy a fiatalabb korosztály aktívabb az online térben, mint az idősebb generáció. Manapság már szinte mindenki használ számítógépet vagy okostelefont, és a különböző alkalmazások (Facebook, Viber, Instagram, WhatsApp, Twitter) segítségével gyakorlatilag folyamatos az online (internetes) jelenlét. Ezért a zaklatás nemcsak valós térben (iskolában, utcán), hanem online térben is megvalósulhat. A zaklatás elhúzódó, folyamatos lehet, mivel nem szükséges a résztvevők találkozása. A találkozást követően (pl. iskola után) is folytatódhat, illetve akár találkozás és személyes ismeretség nélkül is megvalósulhat. Heti 7 nap, a nap 24 órájában bármikor megtörténhet, így még az otthon sem jelent biztos védelmet ellene.

A szülőknek az alábbi jelek utalhatnak arra, hogy gyermekét online zaklatják:

- az internethasználati szokásaiban változást veszünk észre: sokkal kevesebbet netezik, bezárkózik, amikor internetezik;
- rosszkedvű, ideges, ingerült lesz, miután internetezik vagy belép a Facebook-fiókjába;
- társas kapcsolatai elszegényesednek, visszavonulóvá válik, nem barátkozik szívesen;
- csökken az önértékelése, negatív gondolatai vannak saját magáról;
- a szokásos szabadidős tevékenységeket, hobbijait elhanyagolja;
- az iskolai teljesítménye romlik, nem tud koncentrálni, a gondok elvonják a figyelmét;
- magába zárkózik, nem közlékeny, nem osztja meg, mi jár a fejében, mi történt vele;
- törli a Facebook- vagy egyéb profilját.

A MEGELŐZÉS LEHETŐSÉGEI

- Tanítsa meg gyermekének az alábbi szabályokat:
  - Minél kevesebb információ érhető el róla az interneten, annál kevesebbet lehet felhasználni zaklatásra.
  - Csak olyan képet, videót készítsen, amit megmutatna szüleinek, tanárainak és az utcájukban lakóknak! Soha nem lehet biztos abban, hogy ők nem látják majd.
  - Csak azokat jelölje vissza ismerősnek, akiket tényleg ismer!
  - Korlátozza, hogy ki léphet vele kapcsolatba, ki láthatja a közzétett bejegyzéseit!
- Beszélgessen rendszeresen gyermekével, hogy idejében kiderüljön, ha zaklatják őt!

MIT TEGYEN ZAKLATÁS ESETÉN?

- Hallgassa meg gyermekét türelmesen és figyelmesen!
- Készítsenek képernyőmentéseket a zaklatás bizonyítására (üzenetekről, chatbeszélgetésekről stb.)!
- Szakítsanak meg minden kommunikációt az elkövetővel!
- Ha az elkövető osztály- vagy iskolatárs, forduljanak az osztályfőnökhöz vagy az intézmény vezetőjéhez!

Amennyiben zaklatás, fenyegetés történik, forduljanak a rendőrséghez!

112 SOS

Egy hónap – egy téma
a biztonságos internethasználatért
2017. június

29000/10652-11/2017.ált.

BIZTONSÁGBAN UTAZÁS KÖZBEN

A nyári szabadság alatti utazások során magunk és családtagjaink biztonsága mellett mobileszközeink biztonságára és a biztonságos internethasználatra is figyelmet kell fordítani. Gondoskodni kell a mobileszközök (notebook, tablet, okostelefon) fizikai biztonságáról a lopás vagy elvesztés megelőzése érdekékében, illetve a rajtuk tárolt adatok védelméről, az illetéktelen hozzáférés megakadályozásáról egy mégis bekövetkezett lopás vagy elvesztés esetére.
A munkahelyi vagy otthoni internetelérés – megfelelő beállítások esetén – biztonságosnak tekinthető, ez azonban nem mondható el az utazás során leggyakrabban használt ingyenes WIFI-hozzáférésekről vagy a nyilvános számítógépekről.

FELKÉSZÜLÉS AZ UTAZÁSRA

Az indulás előtti teendők során a biztosítás megkötése mellett a mobileszközeinket is fel kell készíteni az utazásra:

- Mentsük le és töröljük az eszközökről azokat a fájlokat, információkat, amikre az utazás során nem lesz szükségünk! Így az eszköz elvesztése, ellopása esetén más nem férhet hozzájuk, számunkra azonban továbbra is elérhetőek maradnak.
- Védjük az eszközöket megfelelő jelszóval vagy képernyőzárral.
- Lehetőség szerint állítsunk be teljes tárhelytitkosítást.
- Frissítsük a készülékeinken a programokat, alkalmazásokat, köztük a vírusvédelmi szoftverünket.
- Készítsünk biztonsági mentést minden olyan eszközről, amit magunkkal viszünk az utazásra.
- Kapcsoljuk be a helymeghatározást az eszközön.

MOBILESZKÖZÖK FIZIKAI BIZTONSÁGA

- Csomagoláskor a laptopot és a tabletet ne tegyük külső, könnyen elérhető rekeszbe!
- Repülőn lehetőség szerint a kézipoggyászban vigyük magunkkal a mobileszközeinket!
- Repülőn, vonaton vagy buszon utazva figyeljünk az eszközeinkre, különösen az átszállásoknál!
- Lehetőleg ne használjuk a laptopot nyilvános helyeken! Kerüljük el, hogy felhívjuk a tolvajok figyelmét!
- Ne hagyjuk az eszközöket látható helyen, például gépkocsi utasterében!
- Szállodában javasolt a szobában található széfben tárolni az értékeket, így a szobában hagyott mobileszközöket is!
- Ne hagyjuk őrizetlenül a mobiltelefont az étkezésekkor az asztalon!
- A strandon se hagyjuk őrizetlenül a mobiltelefont! Használjuk az értékmegőrzőt!

INGYENES WIFI-HASZNÁLAT

Az ingyenes WIFI a szállodákban, repülőtereken, éttermekben nyújt internetelérést. Nem tudjuk azonban, hogy ki üzemelteti, és ki kapcsolódik hozzá, így azt sem, hogy az ingyenes WIFI-hálózaton keresztül küldött és fogadott adatokat (például felhasználónevek és jelszavak) ki láthatja még. A WIFI-hotspot és az eszközünk közötti kapcsolat nem titkosított, így akár az is lehallgatható.

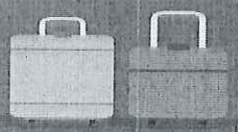
- Ingyenes WIFI esetén használjunk titkosított adatátvitelt.
- Ha böngésző címsorában **egy lakat** és a **https://** szöveg jelenik meg a honlap címe előtt, akkor a honlappal való kapcsolat titkosított és biztonságos.
- Ha lehetőségünk van, használjunk Virtuális Magánhálózatot (VPN-t)! Ennek segítségével a WIFI-n keresztül küldött és fogadott minden információ titkosítva lesz. VPN-t létrehozhatunk akár az otthoni routerünk segítségével is.
- Kerüljük a pénzügyek intézését az ingyenes WIFI hálózatokon. Ha utazás közben szükséges ilyen ügyek intézése, használjunk inkább mobilinternet-szolgáltatást.

NYILVÁNOS SZÁMÍTÓGÉPEK

A nyilvános számítógépek esetében nem lehet tudni, hogy nem fertőzött-e, vagy nem gyűjt-e adatokat.

- Csak és kizárólag publikus információk böngészésére használjuk: időjárás, menetrend, térkép, látnivalók keresése.
- Soha ne lépjünk be róla levelezésünkbe, közösségi fiókunkba vagy banki oldalunkra.

Egy hónap – egy téma a biztonságos internethasználat



Június – biztonságban utazás közben

A nyári szabadság alatti utazások során magunk és családtagjaink biztonsága mellett mobileszközeink biztonságára és a biztonságos internethasználatra is figyelmet kell fordítani.

FELKÉSZÜLÉS AZ UTAZÁSRA

Mentsük le és töröljük az eszközökről azokat a fájlokat, információkat, amikre az utazás során nem lesz szükségünk!

Védjük az eszközöket megfelelő jelszóval vagy képernyőzárral.

Lehetőség szerint állítsunk be teljes tárhelyitkosítást.

Készítsünk biztonsági mentést minden olyan eszközről, amit magunkkal viszünk az utazásra.

MOBILESZKÖZÖK FIZIKAI BIZTONSÁGA

Repülőn lehetőség szerint a kézipoggyászban vigyük magunkkal a mobileszközeinket!

Repülőn, vonaton vagy buszon utazva figyeljünk az eszközeinkre, különösen az átszállásoknál!

Ne hagyjuk az eszközöket látható helyen, például gépkocsi utasterében!

A strandon se hagyjuk őrizetlenül a mobiltelefont! Használjuk az értékmegőrzőt!

Lehetőleg ne használjuk a laptopot nyilvános helyeken! Kerüljük el, hogy felhívjuk a tolvajok figyelmét!

INGYENES WIFI-HASZNÁLAT

Ingyenes WIFI esetén használjunk titkosított adatátvitelt.

Ha lehetőségünk van, használjunk Virtuális Magánhálózatot (VPN-t)! Ennek segítségével a WIFI-n keresztül küldött és fogadott minden információ titkosítva lesz.

Lehetőleg ne használjuk a laptopot nyilvános helyeken! Kerüljük el, hogy felhívjuk a tolvajok figyelmét!

Kerüljük a pénzügyek intézését az ingyenes WIFI hálózatokon.

NYILVÁNOS SZÁMÍTÓGÉPEK

Csak és kizárólag publikus információk böngészésére használjuk: időjárás, menetrend, térkép, látnivalók keresése.

Soha ne lépjünk be róla levelezésünkbe, közösségi fiókunkba vagy banki oldalunkra