

Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

- Háttér
- Oktatás/ Kommunikáció
- Biztonsági Technológia
- Példamutatás

A mai online gyerekek biztonsága

Háttér

Megdöbbenő módon növekszik a gyerekek online tevékenységeinek és kapcsolattartási lehetőségeinek száma. A közösségi média új applikációitól kezdve a játékokon keresztül egészen a Chromebookot kiosztó iskolákig bezárólag, meghatározó a gyerekek szociális élete és jövője szempontjából, hogy mennyire képesek kihasználni a technológia adta lehetőségeket. Szülőként pedig biztosak akarunk lenni abban, hogy a gyermekeink mindezt biztonságos módon teszik. Ugyanakkor ez kihívást is jelenthet a legtöbbször számára, hiszen mi nem ilyen technikai környezetben nőttünk fel. Segítségképpen áttekintjük azokat a főbb lépéseket, amelyek képessé teszik a mai gyerekeket arra, hogy a technológiát biztonságosan és biztonsággal használják.

A szerzőről

Adrien de Beaupre minősített SANS oktató, SANS kurzus szerző, valamint független sérülékenységvizsgálóként dolgozik a gyönyörű Ottawában (Ontario, Kanada). Amikor éppen nem „kockul”, akkor a családjával vagy az edzőteremben tölti idejét. Twitter: [@adriendb](https://twitter.com/adriendb)

Oktatás/ Kommunikáció

Az első lépés, amit tehetünk, az a kommunikáció, győződjünk meg arról, hogy nem csak mi szólunk a gyerekekhez, hanem ők is beszélgetnek velünk. A szülők túl gyakran vesznek el a technológia rejtelmében, arra keresve a választ, hogy mely applikációk jók vagy rosszak, illetve, hogy melyek a legjobb gyermekbiztonsági szoftverek. Ennek ellenére ez nem egy technológiai, hanem egy viselkedésbeli és értékválasztási kérdés. Azt várjuk a gyerekektől, hogy ugyanúgy viselkedjenek az online világban, ahogy azt a valóságban is tennék. Egy jó kiinduló helyzet, ha szabályokat és elvárásokat tartalmazó listát készítünk a gyerekekkel közösen arra vonatkozóan, hogyan is kellene használniuk a technológiát. Az alábbiakat vegyük figyelembe (tartsuk szem előtt, hogy ezek a szabályok gyermekeink növekedésével folyamatosan változhatnak).

- Mikor és mennyi időt tölthetnek/nem tölthetnek online
- Kérdezzük meg gyermekeinket, hogy kik az online barátaik vagy követőik, és hogyan ismerkedtek meg velük. Valójában is ismerik-e azokat az embereket, akikkel online kapcsolatban vannak?
- Beszéljük meg a gyerekeinkkel, hogy milyen típusú weboldalakat látogathatnak, vagy nem látogathatnak, illetve mely játékok megfelelőek, vagy nem megfelelőek és miért.
- Milyen információkat és kivel oszthatnak meg. A gyerekekben gyakran nem tudatosul, hogy amit posztolnak az nyilvános és maradandó. Továbbá azt hihetik, hogy egy titkot kizárólag egy emberrel oszthatnak meg, holott az a titok könnyen megosztható az egész világgal.
- Kinek jelentsek az olyan problémákat, mint amikor valaki online zaklató vagy ijesztő.

A mai online gyerekek biztonsága

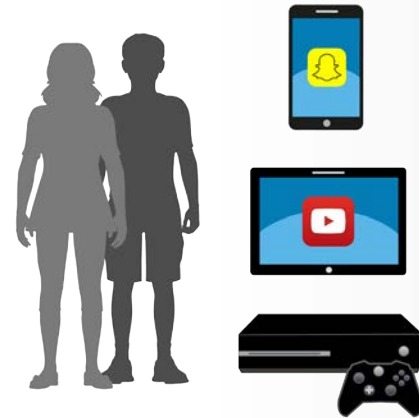
- Kezeljenek online úgy másokat, ahogy azt ők is elvárják másoktól.
- Online nem létezik anonimitás, az emberek tudomást szerezhetnek arról, hogy kik is vagyunk valójában.
- Az emberek nem mindig azok, akinek kiadják magukat az interneten.

Az idősebb gyerekek esetében lehetőség van arra, hogy ezeket a szabályokat a tanulási eredményeikhez, házimunka elvégzéséhez, vagy ahhoz kössük, hogy miként bánnak másokkal. Minél jobb a viselkedésük a való világban, annál jobban tudnak online is viselkedni. Miután meghatároztuk a szabályokat, tegyük ki az otthoni számítógép közelében, vagy a gyerekek szobájának ajtajára. Még jobb, ha átnéztjük és aláíratjuk velük a dokumentumot, amely így kifejezi mindenki teljes egyetértését. Minél előbb kommunikáljuk az elvárásainkat a gyerekeink felé, annál jobb. Nem biztos benne, hogyan kezdje a beszélgetést, különösen az idősebb gyerekekkel? Kérdezzük meg tőlük, milyen alkalmazásokat használnak és azok hogyan működnek. Helyezzük a gyerekeket tanári szerepkörbe és mutassuk meg velük, hogy mit csinálnak online.

Technológia

Az oktatáson kívül vannak olyan technológiák, amelyeket ellenőrzésre használhatunk és segítenek megvédeni gyerekeinket. Meglátásunk szerint a technikai megoldások legjobban a fiatalabb gyerekek esetében működnek, főképp úgy, hogy megvédik őket a nem megfelelő vagy káros tartalmakhoz való véletlenszerű hozzáféréstől. Azonban ahogy a gyerekek egyre idősebbek lesznek, a technikai kontrollok már nem működnek olyan jól. Az idősebb gyerekeknek nem csak Internethez való szélesebb körű hozzáférésre van szükségük, hanem gyakran már olyan eszközöket használnak – mint például az iskola által kiadott eszközök, játékkonzolok, vagy a barátoknál, rokonoknál lévő számítógépek -, amelyek felett nincs kontrollunk, vagy nem tudjuk azokat ellenőrizni. Ezért is olyan fontos az oktatás szerepe.

Egy másik módszer, ha kifejezetten a gyerekeink számára tartunk fenn egy külön számítógépet. Így nem tudják véletlenszerűen megfertőzni azt a számítógépet, amit olyan szenzitív tevékenységekre használhatunk, mint pl. az online bankolás vagy adóügyintézés. Továbbá tartsuk a gyerekek gépét nyílt, forgalmas helyen, így ellenőrizni tudjuk, hogy mit csinálnak. Csak azért, mert azt mondják, hogy a házi feladatukat készítik, még nem jelenti azt, hogy tényleg a házi feladaton dolgoznak. Végül győződjünk meg róla, hogy a számítógép védett, rendszeres a biztonsági mentések rajta és a gyerekeinknek nincs adminisztrátori joga felette. A mobil eszközök estében fontoljuk meg, hogy legyen egy központi hely a házban a telefóntöltésre. Mielőtt a gyerekeink elmennek este aludni, helyeztessünk minden mobilt a töltőpontra, így nem éreznek készletetést annak használatára alvás helyett.



A legfontosabb dolog online gyerekeink védelme érdekében, hogy felkészítsük őket azokra a veszélyekre, amelyekkel szembe kell nézniük és meggyőződjünk arról, hogy nem csak mi szólunk hozzájuk, hanem ők is beszélgetnek velünk.

A mai online gyerekek biztonsága

Példamutatás

Ne feledkezzünk meg arról, hogy szülőként nekünk is jó példát kell mutatnunk. Ez azt jelenti, hogy amikor a gyerekeink beszélnek hozzánk, akkor tegyük le a digitális eszközeinket és nézzünk a szemükbe. Figyeljünk oda, hogy ne használjunk digitális eszközöket az ebédlő asztalnál és sose írjunk üzenetet vezetés közben. Végül, amikor a gyerekek hibáznak, kezeljük a hibáikat úgy, amiből tanulhatnak ahelyett, hogy azonnal fegyelmeznénk őket. A „Miért?”-re minden alkalommal adjunk választ, és emlékeztessük őket, hogy mi csak megpróbáljuk megvédeni őket az olyan veszélyektől, amiket ők még nem láthatnak. Tudassuk velük, hogy hozzánk fordulhatnak, ha valamilyen kellemetlen online dolgot tapasztalnak, esetleg még egy képernyőképet is készíthetünk a gyerekekkel, amit meg tudnak velünk osztani. Biztosítsuk őket arról, hogy akkor is nyugodtan fordulhatnak hozzánk, ha rájönnek, hogy valami helytelen dolgot csináltak. A nyitott és aktív kommunikáció a legjobb módja annak, hogy elősegítsük gyermekeink biztonságát napjaink digitális világában.

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a <http://www.govcert.hu/> és a <http://neih.gov.hu> oldalon olvasható.

Hivatkozások

RSAC Kiberbiztonság: Gyermek:	https://www.rsaconference.com/safety
NCSA:	https://staysafeonline.org/stay-safe-online/for-parents
FOSI:	https://www.fosi.org/good-digital-parenting
Az Egyesült Királyság Nemzeti Bűnügyi Ügynöksége:	https://www.thinkuknow.co.uk

Az OUCH! a Sans Securing The Human részleg által közzétett és a [Creative Commons BY-NC-ND 4.0 licenz](https://creativecommons.org/licenses/by-nc-nd/4.0/) alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra.

A Fordításért vagy további információért lépjen kapcsolatba velünk a ouch@securingthehuman.org címen.

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

Fordította: Tikos Anita



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus