Gyermekek védelme online térben

Fontos szempontok szülők számára

Piarista Rend Magyar Tartománya
Budapest
2020

Ezzel a dokumentummal[1] az a célunk, hogy felhívjuk a szülők figyelmét arra, hogy kövessék nyomon gyermekeik online tevékenységét, segítsenek eligazodni nekik az internet világában. Tudjuk, hogy ez nem egyszerű, hiszen a technológia nagyon gyorsan változik, és felnőttként is épp elég követni az irányzatok közül a valóban hasznosakat, de a felelős cselekvés arra szólít minket, hogy legalább a szükséges mértékig elmélyedjünk ezekben a kérdésekben.

A gyerekek jól eligazodnak az online lehetőségek között, megtalálják a keresők segítségével a válaszokat a kérdéseikre, rengeteg online játékkal játszanak, e-maileznek, chatelnek, különböző üzenetküldő alkalmazásokat használnak. Ezek a tevékenységek azonban nem teljesen tudatosak, inkább mintákat követnek. Így fontos előmozdítanunk, hogy felelősséggel tudják kiválasztani és kezelni az alkalmazásokat. Tisztában kell lenniük azzal, mi az, amit megnézhetnek, használhatnak az interneten. Magabiztosan mozognak az online térben, viszont a kíváncsiságuk és felelősségtudatuk hiánya könnyen veszélybe sodorhatja őket.

Az alábbiakban néhány szemponttal szeretnénk segíteni ezt a folyamatot:

- A digitális élet legyen része a mindennapok beszélgetéseinek. Az elmúlt időszak távtanulásos helyzetében értelmét vesztette a „mi volt ma az edzésen és az iskolában” kérdés, helyette tájékozódjunk arról, mi történt aznap a virtuális térben. A gyerekek legyenek tisztában döntéseik következményeivel,

[1] A dokumentum eredeti változata az ESET informatikai biztonsággal foglalkozó vállalat honlapján jelent meg 2020 tavaszán. (https://www.eset.com/hu/hirek/hogyan-legyenek-a-gyerekek-es-a-tanarok-biztonsagban-a-digitalis-oktatas-ideje-alatt-2020/)
Ezt a dokumentumot alapul véve alakítottuk ki a jelenlegi változatot.

és azzal, hogy baj esetén mindig fordulhatnak szüleikhez.

- A gyermekek sokszor tájékozottabbak technikai szempontból az online szolgáltatások világában, mint a szülők, de ez nem jelenti azt, hogy átlátják a folyamatokat, amelyek velük történnek. Szükséges, hogy segítsük őket tanácsokkal, tapasztalatunkkal, és szükség esetén megvédjük őket a digitális világ veszélyeitől.
- Bármilyen oldalon történő regisztráció előtt a gyerekek egyeztessenek szüleikkel. Tudniuk kell, hol milyen adatot adhatnak meg, hogy mindig a lehető legkevesebb információt adják meg és a felhasználónévből ne legyenek beazonosíthatók. A regisztráció kapcsán beszélgessünk az adatlopásokról, az adatok értékéről, azok megóvásáról.
- Az ingyenes telefonos alkalmazásokban sokszor fizetős modulokat rejtenek el, így a gyermekek „véletlen" módon tudnak vásárlásokat generálni. Beszélgessünk a gyermekekkel arról, hogy ha valamit nem értenek ilyen helyzetben, akkor kérdezzenek. Mi pedig körültekintően járjunk el bankkártyaadataink megadását illetően.
- A közösségi média felületein jól beállíthatók, hogy ki és milyen tartalmat lásson a megosztásokból, de külön odafigyelés nélkül könnyen beleeshetünk abba a hibába, hogy olyan tartalmat osztunk meg másokkal, amelyet csak bizonyos csoporttal szerettünk volna. Érdemes a beállításokat rendszeresen áttekintenünk, ellenőriznünk. Ha gyermekünk már elég idős ahhoz, hogy ezeken a felületeken felhasználói fiókkal rendelkezzen, akkor beszélgessünk vele erről, nézzük meg közösen, mit és hogyan oszt meg másokkal.

- Az online térben történő zaklatásról már mindannyian hallottunk. Sokszor távolinak tűnik ez a problémakör, de ne feledjük, hogy éppen ezt a képzetet használják ki azok, akik a gyermekeket ezen a módon bántják. Fontos látnunk, hogy nem csak szexuális témában lehet szó online zaklatásról, ezért érdemes a témával kapcsolatban részletesen tájékozódni.

  Jó szívvel ajánljuk az UNICEF #nemvagyegyedül kampányának oldalát.[2]

  Tudnunk kell azt is, hogy a Piarista Rend Magyar Tartománya elkötelezetten dolgozik azon, hogy minden piarista iskola biztonságos iskola legyen. Bármilyen zaklatás, bántalmazás esetén segítséget lehet kérni, és bejelentést lehet és kell tenni a *Biztonságos Iskola Tartományi Tanácsánál* (BITT) (https://bitt.piarista.hu/), és segítséget lehet kérni a BITT helyi felelősénél.

- Rengeteg jelszót kell készíteni – legyünk kreatívak! A tapasztalat azt mutatja, többek közt az évi Worst Password-lista is, hogy az egyszerű jelszavak komoly kockázatot jelentenek. Ha ezt még súlyosbítjuk azzal, hogy egy jelszót több felületen is használunk, azzal további kellemetlenségeknek tesszük ki magunkat. Jó ötlet itt is erős, hosszú és egyedi jelszót, vagy jelmondatot választani, és ezeken a helyeken is rendszeres időközönként cserélni őket, ha történik valami, ha nem. A jelszó erősségét értékelő weblapokkal tesztelhetjük is, mennyi idő alatt lehetne feltörni őket, illetve az is jó gondolat, ha szimpla jelszó helyett inkább jelmondatokban gondolkodunk. Mindemellett nagyon hasznos, ha a kétfaktoros azonosítási lehetőségeket is kihasználjuk.

[2] https://unicef.hu/nemvagyegyedul-2020

- Az online térben való biztonság szempontjából ne csak a személyi számítógépekre gondoljuk. Jussanak eszünkbe a mobiltelefonok, tabletek, játékkonzolok, okostévék is. Ellenőrizzük a letöltött programokat, appokat: biztos jót tölt le a gyerek, ez kelle az adott feladat elvégzéséhez? Megbízható az adott platform? Az appok tartalmai szülői visszajelzések alapján jól ellenőrizhetők a Commonsensemedia[3] oldalán, ahol most a digitális oktatás miatt külön menüpont foglalkozik az oktatóprogramok megbízhatóságával. A telepítés során nézzük át azt is, milyen engedélyeket kér az alkalmazás. Egy videochat alkalmazás jogosan kérhet hozzáférést a kameránkhoz, de egy kvízjátékot valószínűleg felesleges felhatalmaznunk erre.
- A regisztráció során figyeljünk az SSL titkosított kapcsolat meglétére (HTTPS), mert csak ebben az esetben utaznak a megadott bizalmas személyes adatok titkosítva. Ha ez hiányzik, akkor bárki által olvasható, lehallgatható sima szövegként fognak szerepelni a jelszavaink, adataink.
- Ha videokonferenciás kapcsolatban kell lennünk, akkor használat után ne felejtsük el kikapcsolni-letakarni a kamerát, hogy illetéktelenek nehogy figyelhessenek bennünket, lakásunkat. Érdemes olyan biztonsági szoftvert beszereznünk, amely webkamera védelemmel is el van látva, és értesít bennünket, ha illetéktelenek próbálnak meg kapcsolódni a kameránkhoz.
- A nyílt wifi-hálózatokkal kapcsolatban hasznos, ha elmondjuk, hogy sose intézzen ügyeket, ne olvasson e-maileket nyílt hálózatokon, ne adjon meg jelszavakat, felhasználóneveket nem biztonságos háló-

[3] https://www.commonsensemedia.org/

zatra kapcsolódva. Ha átmenetileg rövid időre mégis erre kényszerülünk, akkor kizárólag VPN (Virtual Private Network) kapcsolat használatával tegyük.

- Legyenek a gépen megfelelő szűrőprogramok! Ezek segítségével megfelelően szűrhetők az interneten elérhető tartalmak, így megelőzhetőek a pedofil jellegű zaklatások, és az, hogy gyermekünk erőszakos tartalmakkal találkozzon. Mielőtt használni kezdünk egy szűrőprogramot, beszélgessünk el gyermekünkkel, és magyarázzuk el neki, hogy ez nem ellene irányuló kémkedés, hanem az ő érdekeit tartjuk szem előtt.
- A naprakész vírusirtó és a biztonságtudatos hozzáállás mellett az informatikai higiénia elengedhetetlen része az is, hogy az operációs rendszerek és az alkalmazói szoftverek rendszeresen karban legyenek tartva, frissítve legyenek a hibajavító foltokkal, új verziókkal. A nem javított biztonsági rések ugyanis lehetőséget biztosítanak arra, hogy a kártékony kódok a sebezhetőségeket kihasználva megfertőzhessék számítógépünket. Bármilyen operációs rendszerrel dolgozunk, használjunk vírusvédelmi alkalmazást mind az asztali, mind a mobileszközeinken.

Budapest, 2020. szeptember 1.

Jelen dokumentum közzétételét *Szilvásy László* tartományfőnök engedélyezte.