Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

Az internetes biztonság oktatása gyermekeknek

Háttér

Megdöbbentő módon növekszik azon lehetőségek száma, amelyeken keresztül a fiatalok online tölthetik az idejüket, illetve kapcsolatot tarthatnak egymással. Új közösségi hálózatok bukkannak fel a semmiből, és soha nem látott mennyiségű játék kapcsolódik az Internetre. Ezeken túl, pedig számos iskola beépíti a mindennapjaiba a Google Drive-hoz hasonló szolgáltatásokat, valamint egyre több házi feladatot kell részben vagy teljesen online megoldani és beadni. A gyermekek gyakorlatilag úgy nőnek fel, hogy mindig online vannak. Bár ennek számos előnye is van, nem szabad megfeledkezni a lehetőségekben rejlő kockázatokról sem. Ebben a hírlevélben három olyan területre fogunk koncentrálni, ahol veszélyek leselkednek a gyermekekre, illetve arra, hogy mit tehetünk a védelmük érdekében.

A szerzőről

Bob Rudis a Verizon biztonsági szakértője a 2015 Data Breach Investigations Report szerzője, és négy csodálatos gyermek apukája. Bob számos Fortune 100-as listás cégnél készített elő és vezetett be hatékony biztonság-tudatossági programokat. A Tumblr-en **@hrbmstr** néven található meg.

Kockázatok

1. **Magatartás, viselkedés**: amikor a gyermekek online közösségekben vagy virtuális világokban beszélgetnek másokkal, akkor úgy is viselkedhetnek, ahogy a valóságban sohasem tennék. A fizikai jelenlét hiánya az anonimitás erős érzetét kelti, különösen a gyermekben. Emiatt gyakran engednek a kísértésnek, és olyan módon fejezik ki magukat, amivel megbánthatnak más gyermekeket. Ezt nevezzük internetes bántalmazásnak (cyberbullying). De az is előfordulhat, hogy a mi gyermekünk lesz áldozata mások bántalmazásának, akiknek kimondott célja az, hogy idegeneknek fájdalmat okozzanak.

2. **Kapcsolat**: a gyermekek manapság szinte folyamatosan kommunikálnak egymással szöveges üzenetekben, online közösségekben, vagy akár virtuális világokban való játékok közben. A fizikai jelenlét hiánya miatt a gyermekek gyakran elfeledkeznek arról, hogy a beszélgető partner nem biztos, hogy az, akinek mondja magát, vagy úgy viszonyulnak hozzájuk, mint ahogy azt feltételezik. Ragadozók barangolnak ezeken a virtuális utcákon, és bármit felhasználnak annak érdekében, hogy kapcsolatba kerüljenek a potenciális áldozatokkal, például úgy, hogy saját magukat is gyermeknek adják ki.

3. **Tartalom**: a gyermekekben nagy a kísértés arra, hogy bármit közzétegyenek és mindenkivel megosszanak saját magukról vagy a családjukról készült fotókat, videókat, szöveges üzeneteket, stb. Ez egy valós és komoly veszély, mert a gyerekek nem fogják fel a tetteik következményét. Azt sem ismerik fel, hogy mennyire komoly a személyiség ellopásának esélye, vagy éppen egy káros szoftver fertőzés esélye, amikor mások arra kérik őket, hogy töltsenek

Az internetes biztonság oktatása gyermekeknek

ki valamilyen tesztet vagy kattintsanak az általuk küldött hivatkozásra. Ezeken kívül pedig olyan korban élünk, amiben nincs „Visszavonás” gomb, ha valamit kiposztolunk az Internetre, vagy megosztottunk másokkal. A gyermekek azt hiszik, hogy a Facebook-ra, az Instagram-ra, Snapchat-re vagy más hasonló szolgáltatásra feltöltött tartalmak feledésbe merülnek, és nem látják még át, hogy ezek a későbbiekben kellemetlenségeket okozhatnak nekik vagy a családjuknak.

a gyerekek védelmének kulcsa az, hogy felvilágosítsuk őket a rájuk leselkedő veszélyekről, valamint kétoldalú párbeszédet folytatunk velük ezekről a helyzetekről.

A gyermekek oktatása

A gyermekek védelmében tehető legfontosabb dolog az, hogy beszélünk velük. Tisztában kell lennünk azzal, hogy mit művelnek az online térben, fel kell hívni a figyelmüket a manapság gyakori veszélyekre, és arra, hogy mit tehetnek a saját védelmük érdekében.

1. **Biztonság otthon**: bár egyre nagyobb a szerepe a mobilos internethasználatnak, mégis az otthon az, ahol a biztonság, a megfelelő online viselkedés elsajátítása kezdődik. Minél fiatalabb korukban kezdünk velük erről kölcsönös párbeszédet kezdeni, annál jobb. Rendszeresen beszélgessünk el velük az online biztonsági problémákról, akár meg is mutathatjuk nekik a lehetséges következményeket. Ha nem tudjuk, hogy mit csinál a gyerek, akkor egyszerűen kérdezzük meg. Játsszuk el a tanácstalan szülőt, és kérjük meg, hogy mutassa meg a legújabb dolgokat, és azt, hogyan használja azokat, mivel nagyon szeretnek elbüszkélkedni azzal, amit tudnak, és ilyenkor könnyen megnyílnak. Például ha a gyerek fent van az Ask.fm-en, akkor kérjük meg, hogy mutassa meg, hogyan lehet azt használni, segítsen regisztrálni egy felhasználói fiókot, majd iratkozzunk fel (kövessük) a csatornájára. Ezzel pedig nem csak azt érjük el, hogy mindig tudjuk, mit művel az Ask.fm-en, hanem így megkönnyítettük azt is, hogy kommunikáljanak velünk. Ezen túl pedig mivel minden internetes tevékenység egy helyben zajlik, könnyen tudunk időkorlátokat felállítani. Azzal, hogy a számítógép otthon központi helyen van, a gyerekek sokkal kevésbé hajlanak arra, hogy veszélyes dolgokat műveljenek. Érdemes megfontolni egy közös mobil töltő eszközt, így mindig lehet ellenőrizni, hogy a telefont nem viszi ágyba a gyermek lefekvéskor.

2. **Biztonság máshol**: ha a gyermekek elmennek hazulról, nagyobb kockázatnak vannak kitéve. Magyarázzuk el nekik, hogy az általunk felállított szabályok mindenhol érvényesek, és beszéljünk a bevezetett korlátokról azokkal a háziakkal, ahova a gyerek látogatóba megy, és akiket megbízunk a felügyeletükkel. Ha a gyerekeknek van mobiljuk, akkor ellenőrizzük, hogyan használják (sávszélesség és időkorlátok), mivel így hamar kiderül, hogy az esetlegesen lazább szabályokat hajlamosak-e átlépni, ha idegen helyen vannak. Nyilván nem tudjuk az összes szabály betartását kikényszeríteni, de legalább a figyelmezető szavaink mindig ott lesznek velük, ha a mobil készüléket használják.

Az internetes biztonság oktatása gyermekeknek

3. **Biztonság számokban**: nem vagyunk egyedül ebben a történetben, és felvehetjük a kapcsolatot más szülőkkel, testvérekkel, tanárokkal és barátokkal, akik segíthetnek abban, hogy fél szemüket mindig a gyerekeken tartják, hogy megakadályozzák az esetleges káros tevékenységüket. Próbáljunk meg a közösségünket rávenni arra, hogy figyeljenek oda a gyerekekre, akik segíthetnek visszaterelni a helyes útra őket adott esetben.

Végezetül pedig, ha a gyerekek elkövetnek valami hibát, akkor ezt a tanulási folyamat részének fogjuk fel, és ne akarjuk azonnal büntetni őket. Minden ilyen esetben magyarázzuk el a „miért”-et, és emlékeztessük őket arra, hogy csak meg akarjuk óvni őket olyan veszélyektől, amiket ők még nem ismernek fel. Tudassuk velük, hogy bármikor és bármivel kapcsolatban fordulhatnak hozzánk, ha olyat tapasztalnak, ami rossz érzéssel tölti el őket, és ilyenkor akár még egy képernyőképet is készíthetnek a helyzetről. Fontos, hogy tisztában legyenek azzal is, hogy akkor is fordulhatnak hozzánk, ha csak valami helytelent tettek. A valódi, nyílt, élőbeszédes kommunikáció a legjobb módszer arra, hogy megvédjük a gyerekeinket a napjaink digitális világában létező veszélyektől.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További

Hivatkozások

Safer Internet Magyarország:	https://saferinternet.hu/korosztaly/szulok/
Ajánlás szűrőszoftverekkel kapcsolatban:	http://nmhh.hu/dokumentum/162986/szuroszoftver_ajanlas.pdf
Biztonságosinternet tippek:	http://biztonsagosinternet.hu./tippek

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó

