Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Безопасността на днешните онлайн деца

Обстановка

Броят на начините по които днешните деца могат да получат достъп до онлайн пространството и да контактуват с други хора е умопомрачителен. От нови приложения за социални медии и игри, до училища, които издават книги в Chromebooks, социалният живот и бъдещето на децата зависят от това да могат да използват технологиите пълноценно. Като родители, ние искаме да сме уверени, че те правят това безопасно и сигурно. Това може да бъде предизвикателство обаче, тъй като много от нас не са израснали в подобна техническа среда. За да ви помогнем, тук ние сме разработили ключовите стъпки в подкрепа на това днешните деца да могат да използват технологиите пълноценно по безопасен и сигурен начин.

Гост-редактор

Адриен дьо Бопре (Adrien de Beaupre) е сертифициран инструктор на SANS, курсов одитор на SANS, и работи като независим специалист по тестване на сигурността в красивата Отава, Онтарио, Канада. Когато не се занимава с компютри, можете да го намерите в залата за джудо. Twitter: **@adriendb**

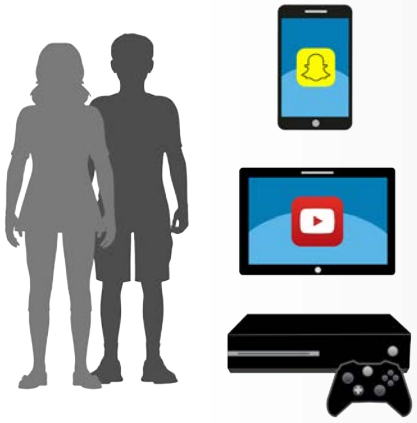
Образоване / Комуникация

Стъпка номер едно, която можете да предприемете е комуникацията – да правите всичко възможно да говорите с децата си и да сте уверени, че и те говорят с вас. Твърде често, родителите се оплитат в технологии и задават въпроси като това какви приложения са добри или лоши или какъв е най-добрият софтуер за сигурност за деца. В основата си, това предизвикателство не е технологично, това е предизвикателство на поведението и ценностите. Искаме децата да се държат онлайн така, както биха се държали в реалния свят. Добро начало е създаването на списък с правила или очаквания от децата ви за това как трябва те да използват технологиите. Ето няколко неща, които да обмислите (помнете, че тези правила ще се променят с порастването на децата).

- Време в което те могат или не могат да са онлайн, както и за колко дълго.
- Попитайте децата си кои са техните онлайн приятели или последователи и как са станали приятели. Познават ли всъщност хората с които са свързани онлайн?
- Говорете за видовете уебсайтове, които трябва или не трябва да посещават или игрите, които са или не са подходящи и защо.
- Каква информация могат да споделят и с кого. Децата често не осъзнават, че онова, което публикуват е общодостъпно и остава за постоянно. В допълнение към това, те може да си мислят, че споделят тайна само с един човек, но тази тайна лесно може да бъде споделена със света.
- На кого трябва да докладват за проблеми, като например ако някой ги тормози или се държи странно.

Безопасността на днешните онлайн деца

- Да се отнасят с хората онлайн така, както биха искали да се отнасят с тях самите.
- Да са наясно, че няма анонимност онлайн, хората могат да открият кой си.
- Те трябва да знаят, че онлайн хората може да не са тези, които казват, че са.



Ключът за предпазване на децата онлайн е да ги образоваме относно опасностите пред които са изправени и да се уверим, че не само ние говорим на тях, но и те споделят с нас.

За по-големите деца, една от възможностите е тези правила да се обвържат с академичните им оценки, с домашните им задължения или с това как се отнасят с другите. Колкото по-добро е поведението им в реалния свят, толкова повече време могат да прекарат онлайн. Щом веднъж решите какви ще са тези правила, поставете ги до семейния компютър или на вратата на стаята на детето. Или още по-добре, дайте им документа да го прегледат и подпишат, така че всички да са напълно съгласни. Колкото по-рано започнете да говорите с децата си за своите очаквания, толкова по-добре. Не сте сигурни как да започнете разговора, особено с по-големи деца? Попитайте ги какви приложения използват и как работят те. Поставете детето си в ролята на учител и ги оставете да ви покажат какво правят онлайн.

Технология на сигурността

В допълнение на образованието, има технологии, които можете да използвате, за да наблюдавате децата си, технологии, които да ви помогнат да ги предпазите. Ние смятаме, че техническите решения работят най-добре при по-малки деца, като най-конкретно ги предпазват от случайно попадане на неподходящо или вредно съдържание. Техническият контрол, обаче, не работи толкова добре с порастването на децата. По-големите деца не само имат нужда от повече достъп до Интернет, а и често използват устройства, които не контролирате или не можете да следите, като тези давани от училище, конзолите за игри или компютрите в дома на роднини или приятели. Именно затова образованието е толкова важно.

Друга стъпка е да имате отделен компютър само за децата. По този начин те не могат случайно да заразят компютъра, който използвате за важни операции, като онлайн банкиране или данъци. В допълнение на това, поставете компютъра им на видно място, откъдето се минава често, за да можете да наблюдавате какво правят. Ако казват, че си правят домашното, това не значи, че задължително наистина си правят домашното. И накрая, уверете се, че компютърът е обезопасен, че рутинно архивирате информацията от него и че децата ви нямат администраторски права в него. За мобилни устройства, обмислете поставянето на централна станция за зареждане някъде в къщата. Преди децата ви да си легнат вечер, накарайте ги да поставят мобилните си устройства на станцията за зареждане, така че да не се изкушават да ги използват във време в което трябва да спят.

Безопасността на днешните онлайн деца

Водене чрез пример

Не забравяйте, че трябва и да даваме добър пример като родители. Това означава, че когато децата ви ви говорят трябва да оставите дигиталното устройство и да ги погледнете в очите. Обмислете това да не използвате дигитални устройства на масата за хранене и никога не пишете съобщения, докато шофирате. И накрая, когато децата правят грешки, гледайте на всяка от тях като на възможност за учене, вместо да прилагате веднага дисциплиниращи мерки. Обяснявайте "защо" всеки път и им припомняйте, че просто се опитвате да ги предпазите от опасностите, които те все още не могат да видят. Кажете им, че могат да дойдат при вас ако и когато преживеят нещо неудобно онлайн, може би дори им кажете да направят снимка на екрана, която след това да ви покажат. Уверете се, че се чувстват свободни да се обърнат към вас, когато установят, че те самите са направили нещо неправилно. Поддържането на отворена и активна комуникация е най-добрият начин да помогнете на децата да останат в безопасност в днешния дигитален свят.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

RSAC CyberSafety: Kids:	https://www.rsaconference.com/safety
NCSA:	https://staysafeonline.org/stay-safe-online/for-parents
FOSI:	https://www.fosi.org/good-digital-parenting
UK's National Crime Agency:	https://www.thinkuknow.co.uk

Редакторски колектив: Бил Уайман, Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли
Превод: Николай Дачев и Радослава Несторова

