Ежемесячный информационный бюллетень по безопасности

Интернет-безопасность для детей

Исходная информация

Жизнь детей в сети важна больше, чем когда-либо, от общения с друзьями и общения с семьей до онлайн-обучения и образования. Как родители, мы хотим убедиться, что они делают это безопасно и надежно. Однако это сложно, поскольку многие из нас никогда не росли в подобной онлайн-среде, как эта. Ниже мы расскажем, как помочь детям максимально безопасно и надежно использовать онлайн-технологии.

Образование/Общение

Прежде всего, убедитесь, что вы способствуете хорошему открытому общению со своими детьми. Слишком часто родители увлекаются технологиями, необходимыми для блокировки контента, или тем, какие мобильные приложения хороши или плохи. Ни одна технология родительского контроля не является идеальной, и некоторые из них обеспокоены конфиденциальностью из-за данных, которые они собирают. В конечном итоге это проблема не технологий, а проблема поведения и ценностей. Научите своих детей вести себя в Интернете, как в реальном мире. Хорошее место для начала - составить список ожиданий ваших детей. Вот некоторые из них, которые следует учитывать (эти правила должны развиваться по мере взросления детей):

- Время, когда они могут или не могут выходить в Интернет и как долго.
- Типы веб-сайтов и / или игр, к которым они могут получить доступ, и почему они подходят или не подходят.
- Какой информацией они могут поделиться и с кем. Дети часто не осознают, что то, что они публикуют, является постоянным и публичным, или что их друзья могут поделиться их секретом со всем миром.
- Кому им следует сообщать о проблемах, например о странных всплывающих окнах, страшных веб-сайтах или о том, что кто-то в сети ведет себя задиристо или хулиганит.
- Относитесь к другим в сети так, как вы бы хотели, чтобы относились к вам.
- Люди в сети могут не быть теми, кем они себя называют, и не вся информация является точной или правдивой.
- Что и кем можно приобрести в Интернете, включая внутриигровые покупки.

Подумайте о том, чтобы связать эти правила к их школьным оценкам, выполнению домашних обязанностей или их отношению к другим. Как только вы определитесь с правилами, разместите их в доме. Еще лучше, пусть дети прочитают и подпишут документ, таким образом, они покажут свое согласие. Чем раньше вы начнете говорить с детьми о своих ожиданиях, тем лучше.

© SANS Institute 2020

Не знаете, с чего начать разговор? Спросите их, какие приложения они используют и как они работают. Поставьте своего ребенка на роль учителя и попросите его показать вам, что он делает в сети. Открытое и активное общение - лучший способ помочь детям оставаться в безопасности в современном цифровом мире.

Для мобильных устройств, где-нибудь в вашем доме подумайте о центральной зарядной станции. Перед тем, как ваши дети ложатся спать, поместите все мобильные устройства на зарядную станцию, чтобы у детей не возникало соблазна использовать их, когда они должны спать.

Технологии безопасности и родительский контроль

Существуют технологии безопасности и родительский контроль, которые вы можете использовать для наблюдения за своими детьми и их защиты. Обычно они предоставляют возможности для принудительного применения ограничений или часов использования, а также защиты содержимого. Эти решения, как правило, лучше всего подходят для детей младшего возраста. Дети постарше не только нуждаются в большем доступе к Интернету, но и часто используют устройства, которые вы не контролируете или не можете контролировать, например, используемые в школе, игровые консоли или устройства в доме друга или родственника. Вот почему так важно общаться с детьми о своих ожиданиях и опасностях, существующих в Интернете.

Подавать пример

Подавайте хороший пример как родители или опекуны. Когда дети разговаривают с вами, положите собственное цифровое устройство и смотрите им в глаза. Не используйте цифровые устройства за обеденным столом и не пишите текстовые сообщения во время вождения. Наконец, когда дети совершают ошибки, относитесь к каждой из них как к опыту, на котором можно учиться, вместо немедленных дисциплинарных мер. Убедитесь, что им комфортно приближаться к вам, когда они испытывают что-то неудобное в сети или осознают, что сами сделали что-то не так.

Приглашенный редактор

Крис Пизор - главный инструктор SANS и руководитель учебной программы в кибер-обучении ВВС США. Когда он не работает, его можно встретить с семьей или занятием по деревообработке. Twitter: @chris_pizor

Ресурсы

FOSI: https://www.fosi.org/good-digital-parenting
Видео SANS «Безопасность ваших детей»: https://www.sans.org/security-awareness-training/secure-your-kids
Национальный альянс по кибербезопасности: https://staysafeonline.org/get-involved/at-home/raising-digital-citizens/
NetSmarts: https://www.missingkids.org/netsmartz/home
OpenDNS: https://www.opendns.com/

Переведено для сообщества: Роман Поляков

OUCH! публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0. Вы можете поделиться или распространить этот бюллетень, если вы не продаете или не изменяете его. Редакция журнала: Уолт Скривенс, Фил Хоффман, Алан Ваггонер, Шерил Конли