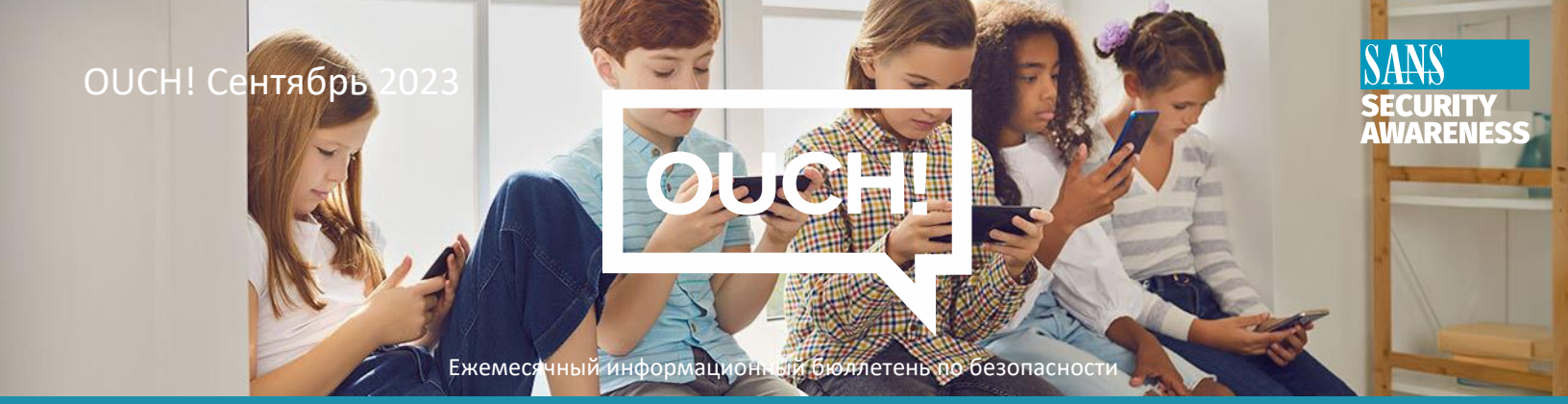

Ежемесячный информационный бюллетень по безопасности

Интернет-безопасность для детей

Исходная информация

Жизнь наших детей сегодня больше, чем когда-либо, связана с Интернетом, от общения с друзьями и игр до онлайн-обучения и образования. Итак, как мы можем помочь нашим детям максимально безопасно и надежно использовать онлайн-технологии?

Образование и общение

Прежде всего, убедитесь, что вы способствуете хорошему открытому общению со своими детьми. Слишком часто родители увлекаются блокировкой контента, или тем, какие мобильные приложения хороши или плохи. В конечном счете, обеспечение безопасности детей зависит не столько от технологий, сколько от поведения и ценностей. 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. Например, вы можете убедиться, что дети выполнили все домашние задания или работу по дому, прежде чем играть в онлайн или общаться с друзьями в социальных сетях, и ограничить количество времени, которое они проводят в сети каждый день.
- Определите типы веб-сайтов, мобильных приложений и игр, к которым они могут получить доступ в Интернете, и почему они подходят или нет.
- Определите, какой информацией они могут делиться и с кем. Дети часто не осознают, что то, что они публикуют в Интернете, является публичным, постоянным и доступным для всех. Кроме того, все, чем они делятся в частном порядке со своими друзьями, может делиться с другими без их ведома.
- Определите, 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. Крайне важно, чтобы дети чувствовали себя в безопасности, разговаривая со взрослым, которому доверяют.
- Как и в реальном мире, учите детей относиться к другим в Интернете так, как они хотели бы, чтобы относились к ним самим, с уважением и достоинством.
- Убедитесь, что дети понимают, что люди в сети могут быть не теми, за кого себя выдают, и что не вся информация является точной или правдивой.
- Определите, что и кто может купить в Интернете, включая внутриигровые покупки.

Со временем, чем лучше они будут себя вести и чем больше доверия они завоюют, тем больше гибкости вы, возможно, захотите им предоставить. 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. 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.

Подумайте о том, чтобы дать им несколько сценариев «Что, если…», чтобы закрепить положительное цифровое поведение, которое вы обсудили или согласовали. 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 лягут спать, выделите определенное время, когда все мобильные устройства будут помещены на зарядную станцию, чтобы у ваших детей не возникло 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. 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. Кроме того, дети постарше часто могут обойти чисто технологические попытки контроля над ними. Вот почему, в конечном счете, общение, ценности и доверие с детьми так важны.

Подавать пример

Не забывайте подавать хороший пример в качестве родителей или опекунов. 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, а не просто наказывайте их. Убедитесь, что они чувствуют себя в безопасности, обращаясь к вам, когда испытывают дискомфорт или понимают, что совершили ошибку в Интернете.

Приглашенный редактор

Дайана Келли — член совета директоров WiCyS и директор по информационной безопасности Protect AI. Она является инструктором учебного курса LinkedIn: Риски безопасности в AI (искусственный интеллект) и ML (машинное обучение) и соавтор книги «Практическая архитектура кибербезопасности».

Ресурсы

Безопасная игра онлайн: https://www.sans.org/newsletters/ouch/securely-gaming-online/
Конфиденциальность: защита вашего цифрового следа: https://www.sans.org/newsletters/ouch/privacy/
Защита ваших мобильных устройств: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Дипфейки: https://www.sans.org/newsletters/ouch/learn-a-new-survival-skill-spotting-deepfakes/

Роман Полаков