**5 главных опасностей соцсетей. Как уберечь детей?**

**И что делать, если ребенок обходит программы родительского контроля?**

*Ребенок завел Instagram, TikTok, YouTube. Знаем ли мы, что именно он смотрит, кто ему пишет, о чем он разговаривает? Но ведь все его друзья по соцсетям — такие же дети, значит все в порядке! В какой момент родители должны насторожиться и чему научить ребенка? Объясняет Андрей Сиденко, руководитель направления «Лаборатории Касперского» по детской безопасности в интернете. Полная версия прямого эфира — в видео.*

**1. Ребенок опубликовал в соцсетях телефон и адрес**

Когда дети только начинают использовать гаджеты, то часто не понимают, какой информацией можно делиться, а какой — нет.

Часто выкладывают личные данные. Например, место жительства или номер телефона, имена и контакты родителей, места, в которых вы часто бываете, любая информация, на первый взгляд незначительная, может быть использована злоумышленниками.

Социальные сети предлагают пользователям оставлять большое количество информации о себе: свои увлечения, комментарии, геопозиции и многое другое. Добавив другого пользователя в друзья, ребенок дает ему доступ к этой информации.

10% детей сталкивались с мошенничеством с использованием поддельных сайтов и писем, по данным «Лаборатории Касперского». Фишинговые сайты — это ресурсы, которые имитируют социальные сети или игровые порталы. Ребенку трудно понять, что сайт — подделка, визуально он похож на настоящий. Он вводит свой логин и пароль, и все личные данные, которые находятся у пользователя в аккаунте соцсети, попадают к онлайн-мошенникам через такие сайты.

**Что делать?**

Научить ребенка оберегать личные данные. Мы ведь учим их с малых лет, что нельзя разговаривать с незнакомцами на улицах. Если кто-то подойдет и начинает спрашивать у тебя номер телефона или где ты живешь, то говорить нельзя. В интернете — то же самое.

**2. Дом или личные вещи попали на фото**

Дети публикуют в социальных сетях фотографии и видеоролики, которые сделали дома или в своем дворе. Это может быть опасно.

**Что делать?**

Поговорить с ребенком о том, какие фотографии нельзя размещать. Примеры:

— виден монитор компьютера, на котором можно прочитать переписку с кем-то, о которой через несколько дней все узнают;

— логин и пароль, на бумажке приклеенные у компьютера;

— по фото из двора можно узнать домашний адрес (видна табличка с номером дома и улицей);

— в кадре — обстановка квартиры и дорогие вещи.

Также нельзя размещать фотографии, на которые попадают другие люди. Правило хорошего тона — спросить у человека разрешения. Например, люди встретились где-то на улице, сделали селфи, потому что давно не виделись. Прежде чем публиковать кадр, нужно спросить: «Можно я это фото у себя где-то размещу?»

**3. Переслал снимок другу — его опубликует кто угодно**

Объясните детям, что ни под каким предлогом не нужно отправлять свои личные фотографии даже хорошо знакомым людям. Это может быть все что угодно — начиная от комичных ситуаций и заканчивая кадрами, предназначенными только для семьи или узкого круга друзей.

Если пользователь отправляет кому-то фото через интернет, мессенджер или почту, то оно ему уже не принадлежит. Отношения с человеком, который получил снимок, хорошие. Но через некоторое время они могут испортиться. И в его силах будет использовать кадры для шантажа. К тому же человека, которому ребенок отправил фото, могут взломать. И вместе с учетными записями к злоумышленнику попадут все фото и переписка.

**Что делать?**

Научить ребенка, что делиться в соцсетях можно только теми фото, которые ты готов показать вообще всем.

Или, например, напечатать на футболке и прийти в ней в класс. Это касается и выражений из личной переписки — она тоже может стать достоянием общественности, есть такая опасность.

Еще можно рассказать про «правило мамы» — готовы ли вы перед тем, как что-то опубликуете, показать это родителям? Как вы думаете, что они на это скажут? Если есть какие-то сомнения, лучше хорошо подумать, стоит ли это вообще публиковать.

**4. Ребенка травят в интернете**

Кибербуллинг — это травля в интернете. Пользователь подвержен ей 24 часа в сутки, 7 дней в неделю. Нет никакой привязки к локации. Часто бывает, что нет привязки к какой-то группе людей. Это может возникнуть совершенно стихийно.



Незнакомые люди могут стать хейтерами — писать ребенку что-то плохое в комментариях, оскорблять и угрожать, мало, что зная о нем самом или о ситуации, в которой он оказался. Их цель — выплеснуть эмоции. И это все сказывается на пользователе.

Из-за сетевой травли дети испытывают стресс, бессонницу, у них ухудшается общее самочувствие и настроение, снижается социальная активность и академические показатели в школе, согласно данным опроса «Лаборатории Касперского». Многие до сих пор считают, что кибербуллинг живет только в интернете. Но это не так — из-за последствий проблема переходит в реальный мир.

**Что делать?**

Научить ребенка, чтобы он сообщал вам о негативе в соцсетях. А также обсудить с ним алгоритм действий в случае кибербуллинга:

Во-первых, ни в коем случае ничего не комментировать в ответ.

Во-вторых, не отвечать на вопросы хейтеров.

В-третьих, заблокировать человека, если он начинает грубить или использовать какие-то нецензурные выражения.

Важно! Если хейтеры применяют угрозы жизни и здоровью, нужно обращаться в полицию. Заявление вы можете подкрепить скриншотами, даже сохраненными страницами, где ребенку или вам явно угрожают.

**5. Незнакомец добавил ребенка в «друзья»**

Ребенок получает сообщение: «Привет! Я Маша. Я учусь в параллельном классе. Ты меня, наверное, не знаешь, но я часто тебя видела на переменках. Давай поболтаем». Как проверить, точно ли это школьница или взрослый, который под нее маскируется?

Чаще всего дети на такое могут ответить. Они в лучшем случае скажут: «Да, привет. И что?» Или зададут любой вопрос, который уже более-менее будет связан со школой. Если это действительно Маша, то у них быстро найдутся общие темы для разговора. Дети одинакового возраста из одной школы действительно могут познакомиться и подружиться, в этом нет ничего плохого.

Возьмем ситуацию, если взрослый добавляет к себе ребенка и начинает общаться. В таких ситуациях чаще всего дети понимают — что-то пошло не так. Но иногда они могут поддерживать такое общение.

С незнакомцами, которые добавляются через социальные сети, лучше не знакомиться, не открывать им все возможные данные о себе, зачастую даже не добавлять в «друзья».

Потому что в этих социальных сетях пользователи оставляют кусочек своей жизни, цифровой след — в каких местах они бывают или куда ездят отдыхать, какие комментарии им оставляют и прочее. Когда вы доверяете эту информацию совершенно незнакомому человеку, это опасно.

**Что делать?**

Важно, чтобы ребенок мог прийти к родителям, если чувствует, что что-то не то в этой переписке или в тех вопросах, которые ему задает совершенно незнакомый ему человек. Чтобы спросил маму и папу, когда не знает, как поступить. Это такой уровень доверия, который, конечно же, должен быть в семье.



В программе родительского контроля есть функция, которая позволяет родителям знать о том, кто пишет ребенку. Он видит, что это аккаунт человека, который идентифицирует себя как взрослый, с фотографиями и прочим. И он почему-то начинает писать моему ребенку.

Стоит проверить, что это за человек. Одно дело, когда это руководитель кружка по спорту или моделированию, который напоминает вашему ребенку о расписании занятий или задании — это нормальная ситуация. Другое дело, когда ребенок этого человека не знает, а он пытается как-то втереться в доверие.

Нужно еще раз напомнить о том, что личные данные неприкосновенны, их нужно беречь.

**Стоит ли проверять соцсети ребенка?**

Читать переписку точно не нужно. Во-первых, это нарушение личных границ. Во-вторых, ребенок, зная о том, что его переписку будут просматривать, может быть не до конца откровенным, соответственно, это еще больше запутает родителя и ухудшит отношения в семье.

Лучше использовать гибкие программы родительского контроля. Они могут оградить детей от нежелательного контента.

Например, ребенок переходит в поисковик, ищет какие-то сайты, которые ему интересны. Если они попадают в категорию, которую в силу возраста ему смотреть еще рано — насилие, материалы для взрослых, нецензурные выражения, азартные игры, алкоголь и так далее — ребенок туда просто не зайдет. Программа даже не покажет ему такую возможность.



Родитель в этот момент получает уведомление. Он может смотреть отчеты, не забирая телефон. Алгоритм фиксирует переходы по сайтам и поисковые запросы. Если ребенка интересует какая-то тема, то родители получат об этом информацию, смогут поговорить об этом с ним.

Но не стоит бить тревогу каждый раз, когда ребенок пытается найти что-то неподходящее. Часто дети ищут информацию, потому что интересуются окружающим миром. Если вы видите, что ребенок ищет что-то запрещенное очень настойчиво — тогда появляется повод поговорить, а также подробно настроить категории ресурсов, к которым будет доступ с устройства ребенка.

Программа также позволяет контролировать поисковые запросы не только на сайтах, но и на YouTube. Нежелательные ролики будут блокироваться.

**Что делать, если дети обходят «Родительский контроль»?**

Иногда дети обходят родительский контроль, подбирают проводки, снимают все пароли с блокировки wi-fi. Что делать родителям?

**Во-первых**, перед тем, как давать устройство ребенку, нужно ему объяснить правила безопасности и самостоятельно настроить гаджет. Поставить программу родительского контроля, сделать так, чтобы установка всех программ была невозможна без вашего согласия. Дать ребенку доступ, но не сообщать пароли. Если он знает административный пароль от телефона для установки приложений, то сможет и удалить то приложение, которое ему не нравится.

**Во-вторых**, не нужно устанавливать приложения для родительского контроля втайне от ребенка.

**Нужно объяснить, что вы устанавливаете программу, которая не контролирует, а позволяет изучать интернет безопасно для него самого.**

Чтобы он случайно не перешел к какому-нибудь видео для взрослых или не попал на фишинговый сайт. По нашим исследованиям, очень много детей переходят на такие ресурсы совершенно случайно. Кликнули на баннер, хотели футбол посмотреть, а там не футбол.

В-третьих, нужно договариваться. Например, есть функция «геопозиция» — она позволяет видеть, где находится ваш ребенок в данный момент. Устанавливается безопасный периметр — если ребенок выходит за него, родитель сразу получает уведомление. С подростками могут быть на этой почве конфликты. Попробуйте предложить, что взамен вы можете дать ребенку свою геопозицию, доступ к ней через другие сервисы. Он тоже будет знать, где находитесь вы в данный момент. Это поддерживает доверие. Вы делитесь геопозициями ради безопасности всех членов семьи.

Источник: <https://www.pravmir.ru/5-glavnyh-opasnostej-soczsetej-kak-uberech-detej/>