Как защитить ребёнка от киберагрессии, сомнительных знакомств, интернет-мошенничества и нежелательного контента

Создайте отдельную учётную запись и ограничьте права пользователя. Пусть у ребёнка не будет возможности удалять и устанавливать программы без вашего ведома. Заходить в учётную запись родителей он тоже не должен.

Активируйте функцию родительского контроля и включите безопасный поиск в браузере. Можно составить список разрешённых сайтов или заблокировать нежелательные. Лучше не допускать ребёнка к интернет-аукционам, платёжным системам и онлайн-банкингу.

Установите специальный детский поисковик, например «Гогуль» или«Спутник.дети». Популярность этих ресурсов, несмотря на их безопасность и ориентированность именно на детскую аудиторию, сегодня крайне низкая.

Ими пользуются лишь 2% опрошенных. Самыми востребованными браузерами среди детей являются Google Chrome (42%), «Яндекс.Браузер» (19%) и Safari (17%).

Поговорите с ребёнком и объясните ему, что далеко не всему и не всем в Сети можно доверять. Нельзя публиковать онлайн домашний адрес, слишком много рассказывать о себе и своей семье, хвастаться дорогими гаджетами и игрушками.

ВАЖНО! Оба этих способа имеют один недостаток — не всегда можно найти актуальную и важную информацию по своему запросу, поэтому не должно быть категорического запрета на пользование обычными поисковыми системами. В этой ситуации важен постоянный контроль. Например, множество антивирусов сегодня имеют функцию родительского контроля, позволяющую наблюдать за действиями в Сети**.**

Предупредите, что за всё сказанное и сделанное в Интернете придётся отвечать. Все действия можно отследить, поэтому не стоит совершать необдуманных поступков. Постарайтесь установить доверительные отношения, чтобы ребёнок не боялся делиться с вами своими сомнениями. Скажите, что, если он увидит что-то непонятное или неприятное, столкнётся с агрессией или повышенным вниманием со стороны незнакомых, пусть приходит к вам за советом.

Поговорите об интересах и о том, какие сервисы и сайты можно посещать, а какие не стоит. Расскажите, что нельзя скачивать файлы с подозрительных сайтов, из писем и сообщений неизвестных отправителей.

Научите использовать настройки конфиденциальности и посоветуйте закрыть профили в социальных сетях, пусть они будут только для друзей. Не надо добавлять во френды всех подряд. Лучше всего, если это будут лично знакомые или хотя бы друзья друзей.

Научите не реагировать на киберагрессию. Спокойно и доходчиво объясните, что хамство и троллинг в Интернете — признак скверного воспитания и неуверенности в себе. Если кто-то будет писать ему оскорбительные сообщения или угрожать, пусть расскажет об этом вам, а вот оппонента следует игнорировать. Отсутствие ответа будет лучшим наказанием для интернет-агрессора, и он скоро потеряет интерес.

ВАЖНО! Самый лучший способ — просто заблокировать обидчика (внести его в чёрный список) самостоятельно или с помощью модератора — пользователя форума или сайта, который следит за соблюдением правил ресурса, имеет право редактировать и удалять сообщения других пользователей и вносить их в чёрный список (банить).

Предупредите об опасностях. Объясните, почему ни в коем случае нельзя общаться с посторонними взрослыми людьми, особенно если они просят прислать фотографии или предлагают встретиться. Сразу же сообщать родителям, если такое произойдёт.

Расскажите о мошенниках. Объясните ребёнку, что администрация сервиса никогда не станет требовать конфиденциальную информацию: полные данные счетов, пароли или ПИН-коды. Расскажите об основных видах мошенничества и научите отличать поддельные сайты.

Научите правилам безопасности в Интернете, расскажите, что нельзя скачивать файлы с подозрительных сайтов, открывать письма и сообщения от неизвестных отправителей. Попросите никогда не отключать антивирусные программы. Научите его выходить из своих аккаунтов, если он пользовался чужим устройством.

Выбирайте смартфон, который не привязан к сим-карте одного оператора. Не полагайтесь только на сенсорный экран. Лучше выбрать телефон, где функции приёма и сброса звонков и вызова меню продублированы кнопками.

Если он захочет что-то купить онлайн, пусть предварительно посоветуется с вами.

Защитите смартфон ребёнка, сделав следующее: установите на устройство пароль и попросите ребёнка никому не сообщать его, даже лучшему другу;

установите специальное приложение, которое поможет контролировать устройство удалённо, даже если его потеряют или украдут;

объясните, что скачивать приложения и игры можно только в официальных магазинах приложений: App Store, Google Play и Windows Market;

подключите аккаунт ребёнка к своей банковской карте и настройте предварительное одобрение на покупку контента.

Установите полезные приложения. Загрузите в смартфон ребёнка карты, чтобы он мог определить своё местоположение, если потеряется. Научите прокладывать маршрут и ориентироваться. Убедитесь, что он точно помнит домашний адрес. Установите специальное приложение, которое поможет определять местоположение устройства. Поставьте несколько мессенджеров и научитесь передавать с их помощью фото и данные о геопозиции.