Для родителей «Как сделать Интернет безопасным»

Сегодня обсудим такие вопросы, как:
- овершеринг (излишняя открытость в соцсетях),
- переписка с незнакомцами;
- какие ошибки совершают дети в Интернете;
- стоит ли проверять соцсети ребенка и читать его переписку?
- запретить покупать в интернете или научить, как делать это безопасно?
- что нужно рассказать о приватности и "взрослом" контенте?

Топ типичных ошибок, которые дети постоянно совершают в интернете: они публикуют много личной информации, доверяют незнакомцам в соцсетях, чрезмерно увлекаются онлайн-играми, пренебрегают правилами кибергигиены.

Что нужно объяснить ребенку, когда родители покупают ему смартфон, и как правильно контролировать его отношения с гаджетами:

Правило первое. С какого возраста можно давать детям гаджеты? Ребенка нужно приучать к ним с трех-четырех лет, но под присмотром взрослых. "Можно показывать мультики на планшете или телефоне, давать играть в развивающие игры. Но если вы оставляете ребенка наедине с устройством, установите детский лаунчер — эта программа не даст зайти в настройки, удалить или установить приложения, а запускать сможет только программы, которые разрешили родители". В шесть-семь лет у ребенка уже должен быть свой гаджет: смартфоны есть у большинства сверстников, учителя создают странички для класса во "ВКонтакте", общие чаты в мессенджерах, куда выкладывают домашние задания, фотографии со школьных мероприятий. Стоит помочь ребенку завести собственную почту и заполнить страничку в соцсети.

Правило второе. Расскажите про кибергигиену. Дети пользуются сервисами и приложениями активнее, чем многие взрослые, но они слабы в понимании правил кибербезопасности. Как часто менять пароли? Где их хранить? Что не так с вашим роутером? Правила кибергигиены. Школьники ставят элементарные пароли, устанавливают приложения из неофициальных источников и не обращают внимания на то, какие данные разрешают им собирать, скачивают фильмы и музыку с сомнительных ресурсов, могут перейти по сомнительной ссылке от знакомого в мессенджере или скачать зараженный файл. "Объясните ребенку элементарные правила кибергигиены. Придумывать для аккаунтов сложные пароли и периодически менять их, не делиться большим количеством информации о себе, скачивать фильмы и программы только на известных ресурсах. Расскажите ребенку, с какими угрозами он может столкнуться, если не будет вести себя аккуратно".

Правило третье. Объясните, что гаджеты — это не вся жизнь. Школьники много времени проводят в гаджетах, четверть родителей, опрошенных

исследователями, говорят, что дети пользуются ими "все свободное время". Каждый пятый родитель отмечает, что у его ребенка есть нехватка физической активности и/или ухудшение зрения. Обычно взрослые перестают контролировать то, сколько времени дети используют гаджеты, когда им исполняется 13–15 лет, а это неправильно. У детей, независимо от возраста, должны быть правила использования гаджетов. Можно определить ограничения по времени или месту — запретить, например, пользоваться смартфоном во время еды, разрешить играть в компьютерные игры только час или два в день, не сидеть с гаджетом после 22:00. Объясните, что чрезмерное использование гаджетов вредит здоровью. Ребенок должен понимать, что не стоит увлекаться соцсетями, а лучше отдавать предпочтение живому общению".

Правило четвертое. Научите покупать в интернете. Большинство родителей (57%) считают, что совершать покупки в интернете можно только по достижении 18 лет, по данным исследования QIWI и НАФИ "Дети и технологии". Взрослые обычно не объясняют детям, как правильно пользоваться финансовыми сервисами. Но реальность такова, что большинство подростков (70%) покупают в интернет-магазинах или оплачивают какие-либо товары и услуги онлайн. У 42% детей есть личная банковская карта, не привязанная к счету родителей. Подростки, которые покупают товары в интернете, сталкиваются с традиционными киберугрозами. Могут ввести данные банковской карты на подозрительном сайте. Или заказать в иностранном интернет-магазине товары, запрещенные к ввозу в Россию. К ним относятся, кроме некоторых лекарственных препаратов, еще и с виду безобидные устройства для негласного получения информации вроде флешек с функцией диктофона, очков со встроенной видеокамерой.

Правило пятое. Расскажите о приватности. Еще одна из стандартных ошибок детей — овершеринг — излишняя открытость в соцсетях. Дети охотно выкладывают море фотографий, ставят геометки, указывают в открытом доступе свой номер телефона или номер школы. Этой информацией могут воспользоваться мошенники. Не страшно, если ребенок выложит фото из зоопарка и сделает отметку, но постоянно знать, что и где он делает, должны только родители. По фотографиям из квартиры злоумышленники могут понять уровень благосостояния семьи, а по геотегам из отпуска — узнать, когда никого нет дома.

Правило шестое. Объясните, как вести себя с незнакомцами. Дети зачастую не воспринимают интернет как пространство, в котором также есть опасности. Они спокойно добавляют в друзья в соцсетях незнакомцев и готовы встретиться с ними в реальной жизни. По данным соцопросов ", 70% детей в возрасте от 7 до 18 лет получают приглашения дружить от незнакомых людей. И 18% школьников получают приглашения от незнакомых взрослых. Каждый десятый школьник имел опыт встречи с людьми, с которыми познакомился в соцсетях. "Детям чаще рассказывают про опасности реального мира: "никуда не ходи с незнакомыми людьми,

даже если они говорят, что знают родителей". Важно рассказывать, что это правило действует и в интернете. Здесь представиться другим человеком проще. Вдобавок дети доверчивы — ребята, которые не сталкивались с обманом, могут поверить мошенникам, присылающим сообщения, например, об огромных выигрышах".

Правило седьмое. Научите, как противостоять кибербуллингу. Особенность кибербуллинга (оскорбления, угрозы в интернете) в том, что в отличие от буллинга в школе или во дворе он не прекращается, когда ребенок приходит домой. Иногда обидчиками становятся не сверстники, а взрослые люди, с которыми дети знакомятся в Сети. Чаще с кибербуллингом сталкиваются подростки в возрасте 13–15 лет. При этом, по данным нашего опроса, 23% родителей вообще не заходят на страницу своего ребенка в соцсетях. А это значит, они могут и не подозревать о проблеме. Этот же опрос показывает, что каждый третий ребенок сталкивался с кибербуллингом, а именно: становился жертвой сам, видел, как становились жертвами другие дети, сам участвовал в травле или же слышал о таких случаях. Расскажите ребенку, как действовать в такой ситуации. Добавить обидчиков в блэк-лист, пожаловаться администраторам соцсети, рассказать родителям, не отвечать на травлю.

Правило восьмое. Не читайте переписку. Контролируйте иначе. Треть родителей замечает что-то настораживающее в контенте, который их ребенок просматривает или слушает, по данным соцопросов. На первом месте видео — они либо настораживают, либо не нравятся 22% родителей. Далее идут компьютерные игры — их отмечает каждый десятый родитель. Такой контент ребенок может не искать намеренно, а перейти на взрослый сайт, просто кликнув на баннер или на ссылку, присланную кем-либо в личных сообщениях. Как интернет узнает ваши отпечатки пальцев. Что не так с хранением персональных данных. Когда ребенок начинает осваивать цифровой мир, стоит установить на его устройства программы родительского контроля, которые заблокируют доступ к нежелательному контенту. Но устанавливать их следует сразу, как только малыш начнет самостоятельно выходить в интернет, — позже им это может восприниматься как ущемление свободы. Подростку нужно больше свободы, с точки зрения программ родительского контроля нужно оставлять только уведомления: "Ты заходишь на сайт со взрослым содержимым, ты точно этого хочешь?" Нельзя читать личные сообщения, это как прослушивать телефон, но лучше быть в курсе, если ребенок регулярно получает доступ к запрещенной информации. Причем запрещенной не по мнению родителя, а по закону или по общепринятым нормам — наркотики, не соответствующий возрасту контент. Важно научить ребенка самостоятельно осознавать, что опасно, а что нет.