

Цифровая гигиена. Как обезопасить ребенка в интернете

Эксперт по информационной безопасности и отец двух сыновей Лев Матвеев рассказывает, как научить детей разумно вести себя в сети.

Общие правила Деньги Общение Информация



Фото: depositphotos

Сфера, в которой я работаю, предполагает настороженное отношение к реальности. Когда знаешь, как много вокруг угроз, самое логичное — огородить свою жизнь частоколом. А жизнь близких — тройным. Но у меня в приоритете растить сыновей открытыми миру людьми с предпринимательским взглядом на жизнь. Да и будем честны: у детей понимание угроз современного мира выше, чем было у нас в их

возрасте. Поэтому все, что мы можем сделать, — это вовремя их сориентировать. Моим сыновьям 11 и 6, и мой личный воспитательный минимум для них такой.

Как не подцепить заразу

Если ребенок осознает риск, что любимый гаджет может выйти из строя из-за вируса, он очень быстро приучится пользоваться антивирусом и не ходить на все сайты подряд. Но лучше сразу снабдить чадо списком надежных ресурсов, где тот сможет найти фильмы, музыку, игры, видео.

По мере взросления в прежних границах интернета подрастающее поколение не удержишь. Придется объяснять, как отличать настоящий сайт от ненастоящего, что такое фишинг и социальная инженерия. Это сложнее, тем более, что методы злоумышленников становятся изощреннее, с ними не любой взрослый справится. Но привить привычку осознанного веб-серфинга будет очень хорошим заделом на будущее. А если уж ребенок заинтересовался кибербезопасностью, он и сам вас всему научит.

Чек-лист:

- показать ребенку, где в интернете найти фильмы, игры, музыку;
- рассказать про антивирусы и убедиться, что программа работает на устройстве ребенка;
- рассказать, что бывают фальшивые сайты, где мошенники распространяют вирусы или пытаются узнать личную информацию.



Обращение с деньгами

Я поощряю траты старшего сына на образовательные сервисы, но предоставлять полную свободу здесь мне кажется неправильным. Поэтому мы завели семейный аккаунт Apple (аналогичный сервис есть и в Google), в котором при попытке ребенка что-то оплатить, родитель получает оповещение. Он может согласиться на покупку или отказать в ней. Это воспитывает сознательное отношение к интернет-тратам

и избавляет от неприятных ситуаций, когда какой-то сервис или приложение решает списывать деньги за продление подписки, покупку игровых денег или новых «жизней».

Конечно, вечером после работы я нахожу время, чтобы объяснить, почему отказал в покупке, если такая ситуация происходит. Ребенок услышит мои аргументы, я — его.

Маленькие дети не сразу осознают, что деньги на пластиковой карте появляются не просто так, и нужно объяснять, что давать номер кредитки без спроса нельзя. Поэтому общий совет — подстраховаться, завести виртуальную карту, где хранится минимальная сумма денег и которую легко пополнить, если возникает необходимость совершить покупку онлайн.

Чек-лист:

- рассказать, как работает пластиковая карта и почему ее данные нельзя оставлять где попало;
- объяснить и показать, что в интернете платно и как сервисы могут списывать деньги;
- завести семейный доступ в Apple или Google;
- доверять принятию решений о небольших покупках в интернете ребенку, давая обратную связь об их безопасности и целесообразности.



Общение в интернете

Риск прямых материальных потерь объяснить несложно. А вот рассказать сыну или дочери, к чему может привести доверие к людям в интернете без лишнего запугивания — более амбициозная задача. Первое мое желание как любого родителя, который понимает, что в сети ребенок может столкнуться с троллингом, травлей, буллингом, — полностью запретить любые соцсети. Такие рекомендации, кстати, я часто встречаю в памятках для родителей: «запрещайте, требуйте».

Но если сейчас не научить сыновей реагировать на агрессивное обращение (в интернете или в реальной жизни — не суть важно), они будут получать уроки вплоть до взрослого возраста. Я бы объяснял, что в сети даже хорошие люди часто чувствуют себя безнаказанными и могут проявлять свои худшие качества, говорить то, что никогда бы не сказали в глаза.

Важно, чтобы дети понимали, что все правила общения и обращения с информацией должны работать и в интернете. Сеть — это не какой-то другой мир. Мы и сами иногда этого не можем осознать: учим детей не рассказывать незнакомцам о месте жительства, при этом забываем проверить, не выкладывают ли они в интернет фото с геолокацией.

Чек-лист:

- объяснить, что любая информация, загруженная в интернет, может быть доступна и друзьям, и недоброжелателям;
- проверить настройки приватности в соцсетях — кто и что может видеть и на что реагировать;
- объяснить, что в интернете нельзя грубить самому и терпеть грубость в ответ;
- договориться рассказывать родителям о любой ситуации, которая кажется опасной или хотя бы неприятной;
- договориться сообщать родителям, если кто-то из интернет-друзей предлагает встретиться в реальной жизни;
- объяснить, почему нельзя добавлять незнакомцев в друзья.



Обращение с информацией

Ну, и неизбежное: детей всегда будет притягивать запретное. Взрослый контент — не исключение. Сейчас для того, чтобы его получить, вообще не нужно прилагать усилий. И если в подростковом возрасте сопротивляться любопытству ребенка будет бесполезно, техническими средствами можно до поры оттянуть знакомство со взрослой информацией — о наркотиках, жестокости, сексе, оружии и остальном.

Рынок научился хорошо играть на страхах родителей, представляя сотни решений безопасных устройств, сервисов, технологий. Но часть из них создает только иллюзию безопасности. Например, я бы трижды перепроверил информацию о выявленных уязвимостях в смарт-часах, прежде чем покупать их ребенку. Если эти уязвимости существуют, только представьте, какую полную информацию о местоположении ребенка может получить злоумышленник.

Но часть «безопасных» решений реально хороша. Например:

Антивирусы. Множество из них обзавелись родительским контролем. Некоторые производители пошли дальше и выпустили отдельный продукт специально для защиты детей.

Профили с ограниченной функциональностью. Например, при создании аккаунта Google можно указать, насколько сильно поисковик будет фильтровать выдачу.

Сторонние сервисы. С их помощью можно настроить гибкий доступ к интернету, разрешить или запретить сайты. Некоторые интернет-провайдеры сами предлагают подобную услугу в качестве дополнительной опции к основному тарифу.

Контроль на уровне маршрутизатора. Даже у бюджетных моделей есть базовый родительский контроль. Он позволяет следить и ограничивать действия детей в сети, лимитировать время пребывания в интернете, запрещать доступ на сайты.

Несмотря на то, что я из жесткой сферы информационной безопасности, не считаю запреты лучшим способом воспитания. Угрозы меняются слишком быстро, и со своими запретами родитель всегда оказывается в роли догоняющего. Отгремели новости о «синем ките», появились другие — об игре Мото, завтра появится что-то еще. Эту живую детскую энергию остановить нельзя — дети всегда будут любопытными и изыскательными, будут находить вокруг массу хорошего, но столько же плохого. Поэтому лучшее, что можно сделать для безопасности детей — воспитать их сознательное критичное отношение к реальности на личном примере.