1. Добавлять в «друзья» незнакомцев (особенно взрослых)

Первое, что мы говорим детям: никуда не ходи с незнакомыми людьми, даже если они предлагают показать щенка или говорят, что знают родителей. Такое же правило действует в интернете. Только здесь представиться другим человеком проще, чем в обычной жизни. Достаточно поставить на аватарку фотографию кого-то из ваших реальных друзей, чтобы вызвать доверие у ребёнка. «Знакомому» ребёнок с радостью расскажет, в какое время он возвращается домой, сколько зарабатывают родители (если он знает), начнёт присылать свои фотографии и даже может согласиться на встречу. По статистике, каждый десятый школьник встречался с людьми, с которыми знакомился в соцсетях.

Что делать. Видеть угрозу в каждой новой заявке в друзья точно не стоит. Ребёнок мог познакомиться с кем-то в школе, на занятиях в кружке или вообще во дворе. И устраивать допрос с пристрастием из-за каждого «френда» — не выход. Так вы только подорвёте доверие собственного ребёнка. Но ненавязчиво следить за списком друзей будет не лишним. И реагировать только в том случае, если новый знакомый вызывает обоснованные опасения. Например, приложение Kaspersky Safe Kids присылает отчёты об изменениях в списке друзей ребёнка. Так вы всегда будете в курсе того, кто пытается получить доступ к его странице или завязать общение.

---

2. Ставить геометки

Для того, чтобы рассказать всему миру личную информацию, необязательно переписываться с незнакомцами. Часто дети (и взрослые тоже) рассказывают в соцсетях обо всём, что происходит вокруг. Метки на фотографиях, подробно заполненные профили — мы своими же руками предоставляем о себе все личные данные. Приложение, которое копирует вашу базу контактов и делает её доступной всем желающим, скачало несколько миллионов (!) человек. Если уж взрослые так легко делятся информацией, что говорить о детях. Ребёнок без задней мысли пишет в соцсети: «Ура! Всей семьёй уезжаем на выходные». Друзья пожелают приятного отдыха, а кто-то посторонний сделает вывод, что квартира будет пустовать. Адрес легко вычислить по геометкам с фотографий.

Что делать. Объясните ребёнку, что некоторая информация должна оставаться личной. Нет ничего страшного в том, чтобы выложить фотографию с интересной экскурсии и поставить геометку. Но рассказывать о каждом шаге в интернете, особенно в открытом доступе, не стоит. Знать о том, где находится и чем занимается ребёнок, должны только родители. К слову, в специальном приложении вы можете установить безопасный периметр — когда дети выйдут за его пределы, вы получите уведомление.

---

3. Тратить в интернете слишком много

Раньше дети (то есть уже некоторые взрослые) верили в телевикторины и тратили деньги родителей на дорогие звонки. Теперь современные дети покупают жизни и бонусы в играх и заказывают игрушки на сайтах. Необязательно даже совершать покупку осознанно. Многие приложения так устроены, что для оплаты хватает одного клика. Родители сами помогают детям — дают свой телефон поиграть, сохраняют данные карт в браузерах и не выходят

из профилей в интернет-магазинах. Это позволяет детям оформлять заказы на крупные суммы. Например, совсем недавно мама шестилетней Кейтлин из американского штата Юта не закрыла профиль на «Амазоне», и девочка потратила на игрушки 400 долларов.

Что делать. Если ребёнок время от времени пользуется вашим гаджетом, настройте ограничение встроенных покупок, удалите все данные банковских карт и электронных кошельков. На приложения мобильных банков установите пароль, который знаете только вы. Если вы в целом не против покупок в интернете и просто волнуетесь, что он может потратить слишком много, — заведите отдельный электронный кошелёк. Установите лимит: вот 1000 рублей на месяц, можешь потратить всё за раз, а можешь растянуть удовольствие. Заодно научите ребёнка распоряжаться деньгами.

---

4. Писать в открытом доступе свой номер телефона или данные карты

В интернете легко остаться анонимным, поэтому в сети много мошенников. Одни обманом выманивают у вас пароли и личные данные, другие присылают ссылки с вирусами. Фишинговые атаки, спам, скрытый майнинг — на уловки интернет-мошенников попадают даже взрослые. Дети, которые ещё не сталкивались с обманом, верят в платные опросы и случайные выигрыши, оставляют свой номер телефона или даже данные банковской карты на странных сайтах. Или случайно подключают wap-рассылку — одного клика (иногда даже на кнопку «закрыть») хватит, чтобы со счёта телефона начали списываться деньги.

Что делать. Во-первых, установите антивирус. Хоть этот совет и звучит очевидно, многие до сих пор не готовы платить за программу и рассчитывают лишь на встроенную защиту компьютера. Во-вторых, регулярно напоминайте ребёнку, что нельзя открывать сомнительные сайты, скачивать непонятные файлы и вводить куда бы то ни было номер телефона, пароли и данные карты.

---

5. Смотреть «взрослый» контент

Сайты с порнографией — не самое страшное, что можно увидеть в интернете. Вспомнить хотя бы «группы смерти», из-за которых многие родители стали внимательно следить за поведением детей в интернете. Кроме этого, в сети полно материалов с маркировкой 16+ и 18+ — жестоких игр и видео, доступ к которым никак не ограничен. Скачивать игру или нет, смотреть видео или закрыть его — решает только сам ребёнок. И часто его выбор не совпадает с мнением родителей: «весь класс играет в GTA, значит, и я буду».

Что делать. Сложно контролировать каждый шаг ребёнка в интернете (и не нужно!). В первую очередь, разговаривайте с детьми и ищите компромисс. Не просто запретите играть во что-то или заходить на определённые сайты, а объясните, к чему это может привести. Если уговоры не помогают, ограничьте доступ к нежелательным сайтам с помощью приложения.