Не разговаривать с незнакомцами и переходить дорогу на зеленый — родители с детства учат детей базовым правилам безопасности на улице. А вот про правила в интернете, где мы проводим едва ли не больше времени, часто забывают. Куратор программ по кибербезопасности школы профессий будущего «КрашПро» Алексей Гришин рассказывает, что надо рассказать ребёнку, чтобы он никогда не столкнулся с мошенниками и вирусами в интернете.

1. Пользуйтесь антивирусом и не скачивайте программы с сомнительных сайтов

В интернете очень просто поймать вредоносную программу, которая может воровать ваши данные, начать рассылать спам или вовсе заблокировать доступ к гаджету. Происходит это так: вы случайно открыли ссылку, автоматически начала загрузка неизвестного файла (с вирусом, конечно!) и теперь на мониторе такая картинка:

400 рублей на указанный счет вряд ли помогут разблокировать компьютер. Так что единственный выход — обратиться в сервис. Но если четырем простым советам, то вероятность заразить компьютер или смартфон вирусами близка к нулю.

Что важно рассказать ребёнку:

- При покупке нового телефона, попросите его не экспериментировать с настройками. Или просто ограничьте доступ к консоли настроек, если ребёнок ещё маленький и может не туда нажать. На компьютере лучше включить режим обычного пользователя, а не администратора — тогда ребёнок не сможет случайно скачать (и установить) опасную программу с непроверенного сайта.

- Не забывать про хороший антивирус. Подойдет любая программа с проактивной защитой, которая отслеживает потенциальную угрозу, а не только ищет уже словленные вирусы. Лучше пользоваться платными программами: например, Kaspersky, Norton, McAfee и другие. У большинства есть версии и для десктопа, и для мобильных устройств на Android и iOS.
- Скачивать программы только с официальных сайтов разработчиков. Скачав программу с первого попавшегося ресурса, легко получить вместе с ним вирус. Так что это именно тот случай, когда лучше довериться проверенным сайтам, а не пытаться найти обходные пути.
- Не открывать незнакомые файлы. Открывать все вложения, которые вам прислали неизвестные отправители, — нельзя. А если даже файл прислал знакомый человек, но вы не понимаете, что там внутри, свяжитесь с ним и проверьте, не взломали ли его профиль.

---

2. Жаловаться на пользователей или даже банить их — не стыдно

Травлю в сети важно отличать от простого спора в комментариях. Как правило, она носит постоянный характер: унижают не один раз, а регулярно, придумывая всё новые способы обидеть. Ребёнка могут публично оскорблять, вывешивать отредактированные фотографии, угрожать ему или близким людям. Застраховать ребёнка от кибербуллинга на 100% невозможно: агрессорами часто бывают знакомые ему люди. Например, ученики той же школы или ребята из соседнего двора, с которыми не сложились отношения в реальности. Но правильное поведение поможет избежать нападок и не попасть в поле зрения профессиональных интернет-троллей.

Что важно рассказать ребёнку:

- Все действия в интернете имеют последствия. Возможно, даже более сильные, чем в обычной жизни. Информация в интернете хранится годами и может всплыть на поверхность в любой момент. Не стоит выкладывать сомнительные фото или писать дерзкие посты.
- Не вступать в перепалку, даже если на это провоцируют. Если ребёнку кажется, что кто-то ведёт себя агрессивно, пытается угрожать или высмеивать — нет смысла реагировать и разводить «срач». Лучше сообщить об этом администратору соцсети, затем прекратить общение с обидчиком или сразу заблокировать его.
- Не стесняться рассказать родителям или кому-то из взрослых. Если нападки не случайны, агрессия повторяется, ребёнка пытаются запугать или вынудить сделать что-то, чего он не хочет — объясните, что о таких вещах нужно рассказать старшим родителям. Это не трусость, а благоразумие, и важно принять меры, пока никто не пострадал.

---

3. Не рассказывайте слишком личную информацию о себе (и не ставьте геометки на каждом фото)

Вряд ли вы рассказываете незнакомцам, куда едете в отпуск или где живёт ваша бабушка. А вот в соцсетях часто можно обнаружить даже номер паспорта. Объясните ребенку, что личные страницы стоит сделать приватными, чтобы их видели только друзья. Не нужно добавлять в друзья всех подряд, лучше только тех, кого знаешь лично. Если ребёнок хочет

стать звездой в соцсетях и наращивать количество подписчиков — объясните ему, что подробности личной жизни нужно рассказывать дозировано и не выкладывать информацию, которую могут использовать во вред.

Что важно рассказать ребёнку:

- Не выкладывать личные фотографии в общий доступ, сделать их открытыми только для друзей. Неизвестно, кто наткнется на страницу и как их использует. Нужно отключить геометки на фотографиях, с помощью которых злоумышленники могут определить местонахождение ребёнка.
- Никаких персональных данных в интернете. К этому пункту относятся фото документов, точный адрес проживания, школа и класс. Клички домашних любимцев, девичью фамилию матери и другие данные, которые часто используют в качестве вопросов восстановления паролей, тоже лучше не публиковать в открытом доступе. ФИО, адрес, дату рождения и так далее можно вводить только на государственных сайтах или при покупке билетов.

---

4. Придумайте себе надёжный пароль и опасайтесь фишинга

Даже взрослые часто используют простые комбинации цифр или короткие слова, которые злоумышленники могут легко подобрать и получить доступ к важным данным. Так делать нельзя. В надёжном пароле должно быть от 12 до 18 символов, есть строчные и заглавные буквы, цифры и спецсимволы. Например, qwerfg12 — не очень-то надежный пароль, а вот qaz#FGHiur_FGR — хороший.

Для кражи паролей мошенники часто используют сайты-обманки — по оформлению они похожи на настоящие, но в названии домена отличается одна-две буквы. Например, sperbank.ru вместо настоящего sberbank.ru. Этот метод сбора паролей называют фишингом.

Что важно рассказать ребёнку:

- Пароли нельзя хранить в обычном файле на компьютере или онлайн-сервисах. Тем более их нельзя пересылать друзьям в чатах или по почте. Безопасно их хранить можно с помощью специальных программ, шифрующих и защищающих информацию, например, KeyPass.
- Пароли никому нельзя сообщать. Ни знакомым, ни незнакомцам. Даже если незнакомый человек представляется сотрудником известной компании или кем-нибудь еще.
- Нельзя использовать одинаковые пароли для всех сайтов. Желательно придумать для каждого отдельный (и потом не забыть, да).
- Проверяйте названия сайтов, перед тем, как вводить пароль. Важно убедиться, что вы находитесь на нужном сайте. Внимательность — самая надежная защита от фишинга. В идеале стоит вводить название нужного сайта вручную или заходить на него из закладок. В закладки можно сохранить все ресурсы, которыми ребёнок часто пользуется.
- Нельзя переходить по подозрительным ссылкам, которые получили по почте или в сообщениях. Во всех почтовых системах есть встроенные фильтры спама, которые включаются в настройках, также можно скачать платные фильтры, например, Kaspersky Secure Mail Gateway. Они помогут защитить вас от сомнительных сообщений.