Не бойтесь пускать детей одних на улицу, бойтесь пускать в интернет! Жизнь без Всемирной паутины сейчас сложно представить. Конечно, информационные технологии дают нам большие возможности, но вместе с этим могут прийти и большие проблемы. С каждым днем информации в интернете все больше, становится все труднее отсеивать ненужное. Перед кибермошенниками особенно уязвимы дети, вот почему так важно изучать основы кибербезопасности уже со школьных лет.

**Чем опасен интернет для ребенка?**

**1. Опасные знакомства.** Чем хорош интернет? Здесь легко можно скрыть свою личность. Часто при знакомстве в сетях люди не знают, кто перед ними. С виду симпатичная девушка, на самом деле — человек, состоящий в радикальной группировке и подстрекающий на это детей. И поверьте, такие люди знают подход к детям! Интернет-знакомство может перерасти в реальную встречу, что еще опаснее: в безопасности нельзя быть уверенным на сто процентов.

**2. Азартные игры.** Еще не сформированная детская психика гораздо больше подвержена игровой зависимости. В XXI веке дети практически живут в информационной среде и с удовольствием пробуют все, что предлагает Сеть. Ставки на спорт, онлайн-казино, лотереи — реклама азартных игр сейчас присутствует практически во всех видеороликах, а баннерами пестрит на каждая страница. В погоне за «легкими деньгами» ребенок регистрируется, играет, и в конечном счете проигрывает (а как иначе).

**3. Недетский контент.** Одна из самых важных проблем. Информация нежелательного содержания находится в открытом доступе: как самостоятельно изготовить взрывчатку, создать синтетический наркотик, сайты с порнографическим или экстремистским содержанием. Такой контент можно пытаться контролировать, но, будем честны — попытки окажутся безуспешными. Важно объяснить детям, для чего создаются такие сайты и чем это грозит.

**4. Вирусы, вредоносное ПО.** Посещение подозрительных сайтов или скачивание неизвестных файлов может повлечь за собой установку опасного вируса или вредоносного ПО. Они устанавливаются без согласия пользователя и могут украсть личные данные, удалить их или повлиять на работу аппаратных средств компьютера. К сожалению, рынок вредоносных программ постоянно растет.

Опасность поджидает во время использования интернета не только с ПК, но и со смартфона. Некоторые гаджеты достаточно восприимчивы к вирусам. В девайс вирус может попасть не только при скачивании какой-либо программы. Если вам пришло sms с неизвестного номера с просьбой перейти по ссылке, делать этого не нужно — ссылка может быть вирусной.

**Основы кибербезопасности: чему учить детей**

**1. Не разглашать тайны.** Нельзя раздавать свои персональные данные всем подряд (Ф.И.О, адрес, номера документов). Делать это можно только на официальных государственных сайтах с защищенным соединением (слева от адреса сайта будет значок навесного замка́).

**2. Замечать поддельные сайты.** Фишинг — способ выманивания у человека данных (логина, пароля). Фарминг — процедура скрытного перенаправления жертвы на ложный IP-адрес. Перед тем как перейти по ссылке сайта, изучите ее: часто адрес поддельного сайта похож на настоящий (например, vk-vk.com, вместо vk.com). Если ввести данные на таком сайте, они становятся известны злоумышленнику.

**3. Распознавать злоумышленников.** Беспокоиться о безопасности можно в следующих случаях:

* в реальной жизни ребенок не знаком с этим человеком;
* собеседник в разы старше ребенка;
* очень мало друзей в соцсети, зарегистрирован недавно;
* собеседник настоятельно требует фото, какие-либо данные и др.

**4. Придумывать разные пароли.** Использовать один пароль для всех сайтов — не самое разумное решение. Они должны быть уникальны к каждому сайту. Не используйте в качестве пароля дату рождения, имя любимой кошки, свою фамилию. Добавьте цифр и спецсимволов. Все пароли желательно записывать в блокнот (а лучше держать в голове). Воспользуйтесь менеджером паролей — это программное обеспечение, которое помогает пользователю работать с паролями и PIN-кодами от нескольких аккаунтов.

**5. Грань между реальностью и виртуальностью.** Ее практически нет. Не делайте в виртуальном мире того, что вы бы не стали делать в реальном. Запреты и жесткий контроль не помогут оградить детей от всех опасностей в интернете. Необходимо вместе с ребенком изучать основы киберграмотности, чтобы он сам понимал, какие риски могут иметь посещение подозрительных сайтов или общение с незнакомцами.