Ребенок может обхитрить кибермошенника. Но для этого он должен знать как минимум 10 правил о том, что можно и чего нельзя делать, когда ты онлайн.

1. Если ваш компьютер “говорит”, что сайт небезопасный, послушайте его. Иногда может появиться всплывающее окно с предупреждением, а порой в строке браузера отображается знак “красный замок”. Это значит, что сайт, на который вы переходите, сомнительный. Лучше закрыть окно.
2. Иногда в сети лучше промолчать. Не стоит писать пост о том, что вы одни дома, рассказывать, чем занимаются родители. Ни в коем случае не объявляйте всему миру, что дом останется без хозяина на две недели. Никогда не знаете, кто может воспользоваться этой информацией.
3. Следите за личной информацией, которая попадает в сеть. Лучше выложить селфи с друзьями со вчерашней прогулки, чем фото своего дома, дачи, характеризующие уровень достатка. Также избегайте провокационных фотографий. Такой контент притягивает неадекватных граждан.
4. Встречайтесь с реальными друзьями. Если пришло сообщение от виртуального друга, которого вы знаете только по переписке, лучше отказать во встрече. “Развиртуализация” бывает крайне опасна.
5. У каждого аккаунта должен быть свой пароль. Чтобы не получилось так, что добыв логин и пароль от вашей страницы в соцсети, мошенники получили доступ в мобильный банк. А такие истории не редкость.
6. Придумайте сложный пароль. Не нужно использовать слова из словаря, сочетание “имя+мобильный телефон”. Транслитерация — тоже не лучший вариант. Вводите буквы, цифры, символы. Пусть лучше это будет больше похоже на сумбур, чем “12345”. Но даже самый сложный пароль надо менять хотя бы раз в полгода. А хранить их можно в фотографиях или заметках среди длинного текста.
7. Обновляйте приложения и программное обеспечение. Как только система предлагает вам установить обновление, делайте это. Причем самые уязвимые для вирусов — это приложения Office и Adobe, не забывайте про них.
8. Не все ссылки ведут туда, куда нужно. Часто на почту приходят письма с просьбами перейти по той или иной ссылке. А там “зловред” — атакующее программное обеспечение. Он незаметно для пользователя “угоняет” логины и пароли, номера платежных карт, которые когда-либо вводили в браузере, сканы документов и паспортов и превращает гаджет в один из узлов ботсети. Не стоит переходить по таким ссылкам, особенно если они в письме от незнакомых вам отправителей.
9. Между LTE и публичным wi-fi выбирайте LTE. Не стоит подключаться к публичным wi-fi в кафе, транспорте, музеях. Вы можете попасть в сеть мошенника, который будет пропускать весь ваш трафик через свою систему и собирать логины, пароли, номера кредитных карт, личную информацию.
10. Не платите в играх. Когда онлайн игра просит оплатить дополнительные кристаллы, жизни, броню “живыми” деньгами, не делайте этого. Не стоит вводить данные своей карты, иначе вы рискуете стать жертвой обманщиков, которые решили сыграть на вашем азарте.

Десять правил безопасности в Интернете для подростков:

1.Не сообщай никому адрес или номер телефона. Ты не знаешь, кто «прячется» за монитором.
2. Не посылай свою фотографию кому-то, кого ты не знаешь и, тем более, интимную.
3. Храни пароли к электронной почте и входам на другие ресурсы в тайне, не передавай их даже близким друзьям.
4. Никогда не отвечай на грубые или вульгарные электронные письма и сообщения. Просто проигнорируй их, пометь как спам, заблокируй отправителя.

5. Не договаривайся о встрече онлайн, не сказав об этом кому-то (родителям, старшему брату, друзьям). В идеале желательно пойти на встречу, взяв с собой кого-то еще.
6. Если на каком-либо сайте тебе попадется фотография, видео или электронное письмо, которое тебя смутит или шокирует, покинь этот веб-сайт.
7. Доверься взрослым, если что-то тебя смущает или пугает.
8. Не давай вирусам шанс. Не открывай вложения к сообщению, пришедшему с неизвестного адреса.
9. Не верь каждой информации, которую получаешь в Интернете.
10. Если ты не хочешь с кем-то общаться, несмотря на доброжелательные сообщения или комментарии - не общайся.

Литература для родителей

Ефимова, Л.Л. «Информационная безопасность детей»
Цветкова М.С., Якушина Е.В. «Информационная безопасность/Правила безопасного Интернета». Пособие для 2-4 классов
Цветкова М.С., Якушина Е.В. «Информационная безопасность/Безопасное поведение в сети Интернет». Пособие для 5-6 классов
Цветкова М.С., Хлобыстова И.Ю. «Информационная безопасность/Кибербезопасность». Пособие для 7-9 классов
Министерство образования и науки РФ ФГБНУ «Центр защиты прав и интересов детей». Памятка для родителей «Родителям о психологической безопасности детей и подростков». Москва, 2018
Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ