

Кибератаки. Как защитить компьютер



- 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 привлекает 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.

Дети — одна из главных целевых аудиторий мошенников в виртуальном мире. Они доверчивы и менее внимательны. Но когда они знают правила игры, могут себя обезопасить.