7. URL социальной сети

Сегодня в Интернет существуют десятки клонов сайтов Вконтакте, Facebook и другие. Внешне они выглядят точно так же, как и оригинальные ресурсы, а отличаются лишь названием домена, например, «vkonakte.ru» вместо «vkontakte.ru», «faceboook.com» вместо «facebook.com». Эти фишинговые сайты просят ввода логина и пароля, а потом, завладев Вашими данными, перенаправляют на оригинальный сервис.

8. Подозрительные сообщения

Никогда не принимайте и не устанавливайте неизвестные файлы от людей, которых не знаете. Иногда сообщения, отправленные вам якобы вашими друзьями, могут быть отправлены злоумышленниками, которые взломали их аккаунты. Поэтому если сообщение кажется вам подозрительным или содержит подозрительную ссылку, свяжитесь с другом напрямую или по телефону, чтобы убедиться, что сообщение действительно пришло от него.

9. Чужой компьютер

Старайтесь не заходить на свои аккаунты в социальных сетях с чужих компьютеров. Даже если вы доверяете этому человеку, может случиться так, что на его компьютере находится троян, который отправит хакеру данные о вашем аккаунте. Если вы все же используете чужое стройство, убедись, что галочка «запомнить меня» не стоит при вводе логина-пароля.

10. Кибербуллинг

Если вы столкнулись с травлей в социальных сетях, действуйте без промедления. Немедленно сообщите об этом взрослому, которому доверяете. Сделайте скриншоты тех сообщений (или других проявлений травли в сети), которые на ваш взгляд являются кибербуллингом, и заблокируйте тех, кто отправил их вам. Никогда не травите никого в сети или в реальной жизни. Не участвуйте в онлайн-беседах, которые могут закончится травлей.

Всегда, всегда оставайтесь порядочными гражданами цифрового пространства!

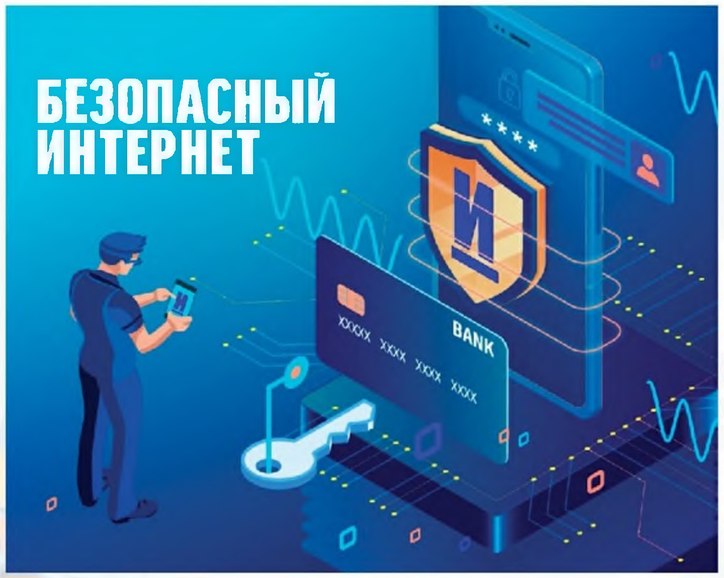
Ссылки на материал:

https://minterese.ru/pravila-bezopasnosti-v-sotsialnyh-setyah/

https://webtous.ru/poleznye-sovety/pravila-bezopasnosti-povedeniya-v-socialnyx-setyax.html

https://vc.ru/social/81702-bezopasnost-v-socialnyh-setyah

ТВОЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ



Следуйте простым 10 правилам и проводите время в социальных сетях не только приятно, но и безопасно!

Михеева Дарья

школа №2

1. Используйте сложные пароли

Надежный пароль должен содержать не менее 8-ми символов и состоять из букв в верхнем и нижнем регистре, цифр, специальных символов.
Не используйте один и тот же пароль на многих ресурсах: пароль должен быть уникальный для каждого сервиса!

2. Лучше иметь 100 рублей, чем 100 друзей

Добавление Вас в друзья дает мошенникам возможность получить доступ к информации, которую Вы скрыли для просмотра незнакомым лицам. Естественно, что появляется возможность писать Вам в личные сообщения, под предлогом какой-то акции, рекламы, либо частной переписки, с целью узнать о Вас больше, либо "подсунуть" вирусную программу для получения Ваших личных данных, с целью мошеннических действий. Внимательно изучайте человека, который предлагает Вам "дружбу", а лучше игнорируйте такие запросы и удаляйте.

3. Двухфакторная авторизация

Этот инструмент даст возможность создать еще один барьер для входа в Ваш аккаунт. Разные социальные сети предоставляют множество типов такой аутентификации, начиная с кодового слова, до пароля, который будет приходить к Вам на личный номер телефона, который привязан к странице, для подтверждения входа. Это сильно усложнит возможность входа в Ваш аккаунт третьим лицам и поможет понизить риск утери важной информации.

4. Банковские данные

Никогда не указывайте номер своей кредитной банковской карты нигде, кроме защищенных платежных систем. Если нужно указать в соцсетях банковские реквизиты, то можно указывать номер карты и ФИО получателя (на которого оформлена карта). Больше никаких данных, а тем более фото карты, размещать нельзя, так как всеми этими данными могут воспользоваться мошенники. Не привязывайте к соцсетям свою основную платёжную банковскую карту.

5. Удаление старых аккаунтов

У основной массы пользователей социальных сетей есть парочка страниц, в той или иной социальной сети, о которых уже давно забыли, но Вы должны помнить, что там находится Ваша личная информация, которую Вы скорее всего не удалили. Если Вы уже не пользуетесь такими страничками, то просто удалите их, чтобы не оставлять Вашу информацию в общем доступе, даже если она устаревшая, как-ни-как это рычаг давления на Вас со стороны мошенников.

6. Минимум личных данных в аккаунте

Обычно злоумышленники взламывают учетные записи на сайтах через ответ на секретный вопрос. Это может быть дата вашего рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице.