БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Социальные сети – пространство для общения, поиска информации, ведения своих блогов и многого другого. Но здесь спрятано и множество рисков: кибербуллинг, мошенничество, груминг и др.

Давайте сформируем перечень советов, которые помогут детям и родителям защитить свои данные в социальных сетях.

СДЕЛАЙТЕ СВОЙ АККАУНТ ПРИВАТНЫМ

Закройте свой аккаунт, чтобы быть уверенным: контент, который вы публикуете, доступен только друзьям и знакомым. По данным исследования «Лаборатории Касперского» «Взрослые и дети в интернете: альтернативные цифровые реальности», 79% детей получают заявки на добавление в друзья от незнакомых людей в социальных сетях, а 23% случаев – это незнакомые взрослые.

Некоторые незнакомцы могут оказаться злоумышленниками. Они могут узнать у вас личную информацию или прислать фишинговые ссылки на сервисы, чтобы украсть личные данные. Логичным следующим шагом будет запрет на отправку сообщений от незнакомых вам людей.

ИСПОЛЬЗУЙТЕ АНТИВИРУСНЫЕ РЕШЕНИЯ НА ВСЕХ СВОИХ УСТРОЙСТВАХ

Технические меры защиты, установленные на ваших устройствах, помогут вам уберечь свои данные от действий зловредного программного обеспечения (вирусов, троянов, шифровальщиков и др.).

Кроме того, стоит позаботиться и о том, чтобы регулярно устанавливать обновления для вашей операционной системы, мобильных приложений и защитных решений. Разработчики программных продуктов периодически находят уязвимости в своем коде и стараются максимально

быстро выпустить обновления. Зачастую этого может оказаться недостаточно, ведь о существовании уязвимости знают не только разработчики, но и злоумышленники, которые могут эти уязвимости эксплуатировать в своих целях. Например, они могут получить доступ к данным, которые хранятся на вашем устройстве (фото, видео, переписка).

Антивирус помогает быстро «отловить» все опасности, которые могут угрожать вашим данным. Например, обнаружить зловредное программное обеспечение, заблокировать переход по фишинговой ссылке или отфильтровать спам-письмо в электронной. Устанавливать защитные решения нужно не только на персональные компьютеры, но и на мобильные устройства.

ИСПОЛЬЗУЙТЕ НАДЕЖНЫЙ ПАРОЛЬ

Правило такое: один сервис, один пароль. Не самой хорошей идеей будет авторизация в социальной сети при помощи аккаунта другой социальной сети, т.к. в случае утечки данных обе учетных записи будут скомпрометированы.

Большое количество паролей запомнить сложно. Чтобы запомнить все коды, можно воспользоваться менеджером паролей. Проверить вашу учетную запись на наличие утечек в сеть можно в сервисе Have I Been Pwnd (HIBP).

НЕ ОТКРЫВАЙТЕ ПОДОЗРИТЕЛЬНЫЕ ССЫЛКИ

Если вы получили сообщение с такой ссылкой, даже от человека из вашего списка контактов, не торопитесь по ней переходить. Сразу обращайте внимание на подозрительные словосочетания в обращении собеседника. Например, обычно ваш друг даже не здоровается, а сразу переходит к сути вопроса. А в этот раз пишет «доброе утро!» и «как дела?». Сообщение от мошенников может начинаться словами «Дорогой друг…» в начале, вместо обращения по имени и др. В этом же сообщении вас могут просить что-то сделать: проголосовать за рисунок, видеофрагмент, оценить работу художника и т.п. Не спешите это делать, свяжитесь со своим другом, например, по телефону и уточните детали. Или задайте вопрос, ответ на который можете знать только вы вдвоем. Часто злоумышленники, получив доступ к аккаунту пользователя, начинают от его имени отправлять сообщения всей книге контактов. В надежде на то, что кто-то им поверит и совершит действия, которые от него требуются.