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.

ДОКСИНГ: ЧТО ЭТО ТАКОЕ И КАК ИЗБЕЖАТЬ?

Наши действия в интернете, например, на платформах социальных сетей или игровых мирах могут привести к нежелательным последствиям уже в реальном мире. Мы создаем профили в соцсетях и других сервисах, оставляем свои данные на разных ресурсах. Часто сами сервисы просят нас рассказать что-то о своей жизни, поделиться эмоциями, указывать места, которые вы часто посещаете, других людей на фотографии и т.д.

Возможность свободно получать информацию практически о любом человеке заинтересовала злоумышленников, которые стали называть **доксерами**. А сам процесс – **доксингом.** Это поиск и преднамеренное раскрытие информации о человеке с целью получения какой-либо выгоды, шантажа или травли.

Самыми распространенными действиями со стороны таких злоумышленников являются раскрытие данных жертвы: адреса проживания, места работы, медицинских диагнозов, переписки с друзьями и другой информации о пользователе. Кроме того, в общий доступ могут попасть детали личной жизни, которые изначально не предназначались для посторонних глаз.

В виртуальном пространстве информация распространяется мгновенно и после первой публикации удалить ее из сети практически невозможно. Это факт усугубляет опасность доксинга, который представляет собой серьезную угрозу для потенциальной жертвы.

Откуда берется информация

В интернете можно найти все, что вы когда-либо загружали или пересылали, существуют даже специальные сервисы, которые архивируют все веб-ресурсы и фиксируют изменения, которые на них происходят. Кроме того, количество утечек данных пользователей за последние пару лет

резко возросло. Как это не страшно признавать, но стопроцентной защиты от доксинга не существует.

Что же это за данные?

В интернете можно найти все, что вы когда-либо загружали или пересылали, существуют даже специальные сервисы, которые архивируют все веб-ресурсы и фиксируют изменения, которые на них происходят. Кроме того, количество утечек данных пользователей за последние пару лет резко возросло. Как это не страшно признавать, но стопроцентной защиты от доксинга не существует.

Давайте попробуем разобраться на конкретном примере, могут ли сами пользователи как-то повлиять на распространение информации о себе в интернете и какую роль они играют в этом процессе.

Разбираем на примере

Разберем ситуацию, как злоумышленники могут воспользоваться информацией, которую вы размещаете у себя на странице.

Например, вы давно собираетесь купить новый велосипед. Выбрали модель, цвет, подобрали все оборудование. Чтобы ваши старания оценили друзья, публикуете фото еще не купленного «железного коня» у себя на странице с подробным описанием того, что на нем будет установлено. Через несколько дней вы получаете сообщение от пользователя, который давно на вас подписан, но вы его лично не знаете. Он сообщает вам, что ваш выбор – просто отменный. И что он/она сам недавно купил/а себе точно такой же велосипед и с радостью сможет поделиться с вами ссылкой на онлайн-магазин, где был сделан заказ.

Это сопровождается красивой легендой о том, откуда такая низкая стоимость. Например, склад закрывается или распродажа «только для своих». После этого вам присылают ссылку: она будет фишинговой, т.е. будет приводить пользователя на поддельный сайт интернет магазина. Ошибки в имени сайта будут допущены специально и никогда не будут идентичными настоящей площадке. Если вы понимаете, что это ненастоящий ресурс, то ни в коем случае не вводите свои данные и тем более не совершайте оплату. Даже если такой «знакомый» вернется спустя некоторое время, чтобы поинтересоваться, как все прошло. Можете просто не обращать внимания на такие сообщения.

Стоит ли говорить, что никакого велосипеда вы не получите, зато злоумышленники получат данные банковской карты. В этой ситуации может быть и другой сюжет, разные действующие лица, но итог будет один. Вас попытаются обмануть, используя за основу ту информацию, которую вы сами размещаете у себя в профиле.

Поэтому всегда проверяйте адреса ресурсов, на которые вы заходите, даже если они как две капли воды похожи на настоящие. Если не уверены, всегда можете открыть поисковую страницу и проверить, как пишется адрес веб-ресурса, который вас интересует.

КИБЕРБУЛЛИНГ

Буллинг – это умышленное агрессивное поведение в отношении жертвы, которое носит систематический характер. С таким поведением по отношению к себе может столкнуться буквально каждый, достаточно чем-то отличаться от других, быть не как все, иметь увлечения, которые многие могут не разделять и др.

Кибербуллинг, в отличии от агрессивного поведения в реальном мире, отличается анонимностью. Согласно опросу «Лаборатории Касперского», чаще всего травлю организовывают люди, с которыми жертва не встречалась в реальной жизни (44%). Но в 22% случаев – знакомые или даже друзья.

Еще одно отличие кибербуллинга от буллинга. Травля не имеет никаких временных рамок, т.е. может происходить в любое время суток, без перерывов на выходные и праздники, так как происходит в онлайн среде. Она может включать в себя размещение неприятных по содержанию постов, получение сообщений через личные сообщения или в мессенджерах, в том числе сопровождаться медиаконтентом (фото или видео). Цель таких сообщений – запугать и унизить жертву, нанести ему серьезный эмоциональный урон.

КАК СНИЗИТЬ РИСКИ КИБЕРБУЛЛИНГА?

1. Не выкладывайте в публичный доступ свои личные данные: адреса, приватные фотографии, номера телефонов, адрес почты и тем более логин/пароль от какого-либо сервиса.

2. Не общайся с незнакомцами в офлайн пространстве. Злоумышленники могут «втираться» в доверие с целью грабежа, насилия или киднеппинга.

3. Используй функцию блокировки от неприятных собеседников в социальных сетях. Кроме того, можно сообщить о травле администраторам.

4. Не отвечайте на негативные сообщения. Часто агрессоры преследуют именно эту цель: вывести на эмоцию и на неприятный разговор.

5. Можно уйти на несколько дней из онлайна, отключив аккаунты в социальных сетях или других сервисах.

Если вы считаете, что проблема выходит из-под контроля, не закрывайтесь в себе. Нет ничего зазорного, если вы решите обратиться к родителям, а вместе с ними к профессионалам, например психологам, которые специализируются на подобных проблемах.

Есть бесплатные и круглосуточные телефонные линии, куда можно позвонить в кризисной ситуации:

- детская телефонная линия – 8-801-100-16-11
- линия в Республиканском центре психологической помощи, работающая в рабочее время (с 9 до 18) – 8-017-300-2321