

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.