В 2023 году в мессенджере Telegram значительно увеличилось число случаев фишинга. Распространенность некоторых популярных мошеннических схем выросла на десятки процентов, а в отдельных случаях – до 5 раз. Сами схемы различаются достаточно сильно: иногда злоумышленники предлагают принять участие в конкурсе или проголосовать в нем, иногда – заманивают фейковой раздачей призов, а иногда – выдают себя за сотрудников банков или правоохранительных органов. Злоумышленники могут присылать просьбы занять денег от имени друзей, в том числе с использованием поддельных голосовых сообщений, а также, представляясь поддержкой Telegram, сообщают о каких-либо проблемах с аккаунтом и необходимости пройти проверку. Также пользователю может прийти сообщение, в котором говорится о том, что его комментарии в тех или иных группах и каналах являются дискредитирующими, и предлагается удалить их по указанной ссылке. Необходимо использовать двухфакторную аутентификацию везде, где только можно, в том числе, и в Telegram, с осторожностью относиться к новым каналам и ботам и верифицировать их подлинность, а также не переходить по подозрительным ссылкам и не вводить какие-либо данные на сторонних сайтах, переход на которые осуществлялся из мессенджера, преступники часто используют взломанные аккаунты.

Для борьбы с фишингом и минимизации возможного вреда необходимо соблюдать следующие правила:

1. Никогда не раскрывайте по телефону личную или мошенническую информацию, если вы не уверены в личности звонящего и причинах, по которым ему нужна ваша информация.

2. Избегайте предоставления личной информации или заполнения информационных форм по электронной почте. Если вы сомневаетесь, позвоните отправителю для подтверждения, даже если электронное письмо отправлено коллегой или кем-то из ваших знакомых.

3. Не нажимайте на ссылки в электронной почте или текстовых сообщениях из неизвестных источников. Эти ссылки могут перенаправить вас на поддельные веб-сайты, которые запрашивают личную информацию на ложных основаниях. Кроме того, на ваше устройство может быть установлено вредоносное ПО, которое ставит под угрозу ваши данные или блокирует ваши файлы.

4. Будьте осторожны в социальных сетях. Открытие вложений, полученных по этим каналам, может привести к заражению вашего компьютера или телефона шпионскими программами или вирусами.

5. Если вы подозреваете, что поделились конфиденциальной информацией с неуполномоченной стороной, немедленно уведомите свой банк или компанию-эмитента кредитной карты, чтобы заблокировать вашу учетную запись и предотвратить злоупотребления.

Заблаговременно сохраните их контактную информацию для таких ситуаций. Сохраняя бдительность, вы можете защитить себя от фишинговых атак. Проявляя инициативу и осторожность, можно предотвратить эти злонамеренные попытки и сохранить цифровую безопасность и конфиденциальность