УДК 343.985.7

А. В. Сычева
доцент кафедры криминалистики
учебно-научного комплекса по предварительному следствию
в органах внутренних дел Волгоградской академии МВД России,
кандидат юридических наук

К ВОПРОСУ О СПОСОБАХ СОВЕРШЕНИЯ МОШЕННИЧЕСТВ ПОСРЕДСТВОМ МЕТОДА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В последнее время проблема борьбы с мошенничеством, совершаемым посредством применения метода социальной инженерии, приобретает все большие масштабы. Четко отслеживая новостные ленты, мошенники быстро реагируют на изменяющуюся ситуацию в стране и придумывают новые способы обмана людей.

Социальная инженерия — это психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации [1].

В последнее время социальная инженерия приобрела прочную связь с киберпреступностью. Киберпреступники (социальные инженеры) в целях незаконного получения доступа к ценным сведениям, обладая хорошими знаниями в области психологии, владея определенными техниками и приемами, стараются обмануть как можно больше граждан.

Мошеннические атаки на граждан могут совершаться различными способами. Рассмотрим некоторые из них.

1. «Кви про кво» (от лат. quid pro quo — «услуга за услугу»). Используя данный метод, мошенник может представиться потенциальной жертве сотрудником службы технической поддержки и предложить исправить возникшие проблемы в системе, которых на самом деле нет. Поверив преступнику, жертва лично передает последнему доступ к важной информации.

Одной из особенностей «кви про кво» является то, что преступники, как правило, действуют быстро и настойчиво, создавая иллюзию выгодности и срочности предложения. Они могут применять такие приемы, как создание срочности, угрозы лишения возможности приобретения товара или услуги, обещая потенциальной жертве получение большой выгоды. Так, Е. посредством сети Интернет оформила путевку в Тайланд онлайн через туристическое агентство. Оператор прислала Е. ссылку для оплаты путевки. Е. перевела

на указанный счет 94 тыс. рублей. После этого сайт указанного туристического агентства оказался заблокированным[1].

2. Действие, отработанное по заранее составленному сценарию, — претекстинг. Для получения необходимых мошеннику сведений он представляется потенциальной жертве родственником, другом, знакомым, коллегой последней. Мошенники могут представиться сотрудниками государственных структур, правоохранительных органов, банковских организаций, то есть лицом, которому по умолчанию жертва должна доверять. Для того, чтобы расположить жертву к себе, установить психологический контакт, мошенники могут назвать фамилию, имя жертвы, номер ее счета в банке и даже действительную услугу, с которой жертва некоторое время назад обращалась в эту организацию. В целях получения интересующей информации преступник выдает себя за известное потенциальной жертве лицо, которому якобы необходима информация жертвы для выполнения важной задачи. Социальные инженеры представляются сотрудниками банков, кредитных сервисов, технической поддержки, другом, знакомым, членом семьи жертвы, т. е. человеком, которому жертва полностью доверяет. В целях завоевания еще большего доверия преступники сообщают потенциальной жертве какую-либо информацию о последней: имя, фамилию, номер банковского счета, реальную проблему, с которой жертва ранее обращалась в эту службу.

3. Троян. Данный способ совершения мошенничества основан на расчете преступников на жадность потенциальных жертв. Жертве приходит сообщение посредством электронной почты, мессенджеров, социальных сетей с радостной информацией о получении легкой прибыли, выигрыша или других легких материальных благ. Перейдя по ссылке, указанной в письме, потенциальная жертва получает вирус, с помощью которого мошенник впоследствии может похитить личные данные жертвы. Для того, чтобы потенциальная жертва обязательно кликнула по нужной ссылке, скачала и запустила вредоносный файл, мошенники используют свои хорошие знания в области психологии, программирования и т. д.

4. Фишинг. Так, посредством электронной почты потенциальной жертве поступает поддельное сообщение от какой-либо известной организации с просьбой перейти по ссылке и авторизоваться. В целях завоевания максимального доверия, мошенники придумывают любые аргументы, для того чтобы жертва точно перешла по указанной ими ссылке (например, просят жертву обновить свой пароль или ввести какую-то информацию (Ф. И. О., номер телефона, банковской карты и т. д.)).

[1] Материалы следственной практики ГСУ ГУ МВД России по Волгоградской области.

5. Обратная социальная инженерия. Данный метод совершения преступления направлен на то, чтобы жертва самостоятельно обратилась к социальному инженеру и передала последнему необходимые ему сведения. Это возможно путем внедрения особого программного обеспечения либо посредством рекламы. Мошенники могут рекламировать свои услуги под видом компьютерных мастеров или других специалистов. Потенциальная жертва обращается к преступнику сама, а мошенник не только работает технически, но и выясняет интересующую его информацию в ходе беседы со своим клиентом.

Говоря о внедрении особого программного обеспечения как способа совершения мошенничества посредством социальной инженерии, необходимо отметить, что преступники, владея навыками программирования, умышленно организуют сбой в системе работы программы, принадлежащей жертве [2, с. 13]. Подобного рода сбой в работе системы, безусловно, требует помощи квалифицированного специалиста. Мошенники создают обстановку таким образом, что тем специалистом, которого вызовет жертва, окажется именно социальный хакер. В ходе настройки программного обеспечения, мошенник производит необходимые для взлома манипуляции. А когда взлом обнаруживается, социальный инженер остается вне подозрения, так как он оказывал помощь жертве.

Таким образом, знание субъектом расследования способов совершения мошенничеств посредством применения метода социальной инженерии может оказать помощь в выдвижении следственных версий, разработке алгоритма действий в целях установления личности преступника и его розыска.

Список основных источников

1. Социальная инженерия [Электронный ресурс] // Википедия. URL: https://ru.wikipedia.org/wiki/Социальная_инженерия (дата обращения: 10.01.2024). Перейти к источнику Вернуться к статье

2. Пупцева А. В., Курин А. А. Методика расследования мошенничества : учеб. пособие. Волгоград : ВА МВД России, 2022. 96 с. Вернуться к статье