КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА СПОСОБОВ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Старостенко Н.И., Старостенко О.А.
Краснодарский университет МВД России, г. Краснодар
email: nstarostenko1996@mail.ru

Аннотация. Данная статья посвящена исследованию способов мошенничества, совершенного с использованием методов социальной инженерии. В статье проводится криминалистический анализ способов совершения мошенничества с использованием методов социальной инженерии, имеющий как теоретическое, так и прикладное значение. Целью исследования является систематизирование и обобщение методов социальной инженерии как способов совершения мошенничества для эффективного раскрытия и расследования преступлений данной категории.

Ключевые слова: Криминалистика, расследование преступлений, мошенничество в сфере информационно-телекоммуникационных технологий, методы социальной инженерии, виды социальной инженерии.

Современное развитие информационных технологий за последние два десятилетия вызывает не только ряд положительных предпосылок для информационного развития общества, но и порождает комплекс отрицательных последствий, выраженных в появление новых видов преступности [1]. В связи с тем, что технологии стали более портативными и мощными, все большее количество информации создается, хранится в общем доступе, в том числе и персональные данные, что позволяет преступникам совершать мошеннические действия, используя личные данные пользователей. Сегодня основной тенденцией развития современной преступности в сфере информационно-телекоммуникационных технологий является совершение мошенничеств с использованием методов социальной инженерии. Их содержание включает в себя деятельность злоумышленника по совершению с корыстной целью деяния, содержащего психологические техники и приемы воздействия, направленные на введение человека в заблуждение и побуждение его выполнять определенные действия для достижения преступного результата в виде предоставления мошеннику персональных данных и (или) конфиденциальных сведений, повлекших причинение имущественного ущерба собственнику. В связи с чем, изучение и анализ методов совершения преступлений данной категории вызывает интерес не только у правоприменителей, но и у ученых.

Отличительной чертой преступлений рассматриваемого вида является обстановка их совершения, образованная электронным устройством, виртуальной средой, а также дистанционностью противоправных действий [2]. Следовательно, мошеннические действия осуществляются в условиях, исключающих вербальный контакт с потерпевшим.

По мнению В.Д. Зеленского и Г.М. Меретукова, «основой механизма мошенничества выступают «действия, слова, те или иные манипуляции преступников, направленные на вхождение в доверие к потерпевшим и вовлечение их в обман» [3]. Злоумышленники при совершении преступлений добиваются получения секретной информации от потерпевших, используя особенности психологии, играя на человеческих слабостях и страхах.

Ведущая роль в криминалистической характеристике рассматриваемого вида мошенничеств принадлежит именно способам совершения преступлений.

Способы совершения преступлений с использованием методов социальной инженерии представляют собой совокупность приемов, являющихся вспомогательными средствами злоумышленника при неправомерном получении доступа к конфиденциальной информации пользователей для достижения корыстных целей с помощью информационных технологий. По своему содержанию техники социальной инженерии многообразны, зачастую их виды дополняются более новыми и современными, в связи с активной деятельностью мошенников и развитием научно-технического прогресса.

Существуют следующие методы социальной инженерии:

1. В зависимости от характера мошеннических действий:

а. Фишинг – (англ. passwordharvestingfishing – ловля паролей) - наиболее распространенная и эффективная техника социальной инженерии, которая представляет собой массовую рассылку писем на электронную почту, либо личных сообщений на номера мобильных телефонов. Зачастую злоумышленник указывает в своем письме (сообщении) ложную ссылку под видом легальной и просит выполнить определенные действия, связанные с передачей конфиденциальной информации.

Фишинг используется злоумышленниками от имени различных известных компаний, банков, сервисов (например, Вконтакте, mail.ru и др.), именно поэтому многие жертвы так легко сообщают им свои персональные данные.

Признаками фишинга являются:

- массовость рассылки писем;
- искажение данных об отправителе;
- отсутствие информации о получателях при отправлении писем;
- использование психологических приемов для побуждения у пользователей желания ввести на поддельной интернет-странице свои логин и пароль;
- письма содержат просьбу перейти по ссылке.

б. Вишинг – (англ. vishing – голосовая запись). Особенность данной техники заключается в том, что преступники включают заблаговременно записанное голосовое сообщение технического специалиста, представителя известной компании (например, сотрудника банка Сбербанк России) при телефонном разговоре с жертвой. В результате мошенники могут получить сведения, содержащие секретный пин-код, номер карты и другую информацию.

Вишинг имеет следующие признаки:

- получение конфиденциальной информации пользователя при помощи средств сотовой связи, а также заранее подготовленной записи официального разговора;
- использование техники для получения доступа к данным банковского счета жертвы;
- стимулирование у пользователя желания к совершению определенных действий с банковской картой;
- нагнетание психологического напряжения для достижения корыстных целей;
- отсутствие конкретных ответов на вопросы, задаваемые жертвой.

в. Претекстинг – это набор действий, проведенный по определенному, заранее подготовленному сценарию (претексту), в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Как правило, целью злоумышленника является выяснение пароля от какого-либо ресурса или иных секретных данных пользователя.

Признаками претекстинга являются:

- собирание информации о потенциальной жертве и её окружении заранее для создания доверительных отношений при общении;
- предварительная подготовка текста диалога с жертвой на основании анализа полученных данных.

г. «Троянский конь» – техника использования любознательности, доверчивости и алчности людей в преступных целях. Злоумышленник отправляет жертве сообщение, содержащее любопытный текст, например, о выигрыше крупной суммы денег. Однако это письмо во вложении содержит вредоносную программу, и при переходе по ссылке или скачивании файла, как правило, происходит списание денежных средств с банковской карты либо заражение персонального компьютера вирусом, избавиться от которого возможно, заплатив денежные средства мошенникам. Данная техника будет оставаться актуальной для преступников, пока пользователи будут охотно переходить по ссылкам, приходящих от своих знакомых или неизвестных отправителей.

Характерными признаками техники «троянский конь» являются:

- использование текста в сообщении, содержание которого вызовет большой интерес любого человека;
- массовость рассылки писем от неизвестных отправителей;
- содержание в прикрепленном к письму файле вирусной программы.

д. Дорожное яблоко – техника социальной инженерии, которая по своим признакам близка к технике троянский конь, однако их отличает способ использования вирусной программы. Главное отличие заключается в том, что этот метод атаки подразумевает применение физических носителей - внешних накопителей памяти, которые злоумышленник преднамеренно оставляет в местах общего доступа, где они могут быть легко найдены заинтересованными лицами. Атака мошенников рассчитана на то, что лицо, обнаружившее накопитель, подсоединит его к компьютеру, тогда произойдет кража персональных данных [4].

2. В зависимости от применяемых информационно-телекоммуникационных средств достижения преступной цели:

а. социальная инженерия с использованием средств сотовой связи;

б. социальная инженерия с использованием сети Интернет;

в. социальная инженерия с использованием ПЭВМ (персонального компьютера);

г. комбинированная социальная инженерия (сочетает в себе два или более названных способов).

3. В зависимости от схемы преступного поведения:

a) «Сотрудник банка» - наиболее популярная схема злоумышленника, когда он представляется специалистом банка или службы безопасности банка и, играя на страхе жертвы потерять деньги, получает данные банковской карты, в том числе и ее секретный пароль.

b) «Представитель пенсионного фонда» - суть данной схемы заключается в убеждении жертвы о возможности получить выплаты, а затем завладеть ее денежными средствами.

c) «Друг или родственник» - данная схема подразумевает действия мошенника, когда он представляется другом, товарищем или родственником с просьбой о неотложной помощи в беде или денежном переводе на лечение.

d) «Бесплатный помощник» - в названной схеме деяния злоумышленника выражены в скрытых мошеннических действиях под видом бесплатной финансовой или правозащитной консультации, а предложенные им услуги оказываются за определенную сумму. Расчет преступника направлен на то, что данные услуги фактически не будут осуществлены, а денежные средства спишутся с банковского счета.

e) «Покупатель по объявлению» - суть данной схемы выражена в том, что мошенник под видом покупателя сообщает жертве о готовности купить у нее тот или иной товар на интернет-сайте «Авито» или «Юла», однако для этого ему

понадобятся данные банковской карты для перевода денежных средств, включая секретный код этой карты или проверочный код из СМС.

f) «Продавец с интернет-сайта» - в названной схеме злоумышленник наоборот размещает заманчивое предложение о продаже какого-либо товара. Зачастую мошенник создает поддельный сайт под видом известного магазина, надеясь заинтересовать жертву выгодным предложением. Такой способ мошенничества подразумевает, что жертва при покупке данного товара переведет преступнику предоплату или полную сумму за этот товар.

Таким образом, представленные методы социальной инженерии свидетельствуют о том, что человек более уязвим, чем система. Ведь человек легко поддается чужому влиянию и психологической манипуляции преступными схемами мошенников. Именно поэтому преступники все чаще используют методы социальной инженерии для получения доступа к интересующей секретной информации пользователей, а также для достижения преступных целей. В связи с чем, представлена обобщенная и систематизированная классификация способов совершения мошеннических действий рассматриваемой категории преступности, анализ и изучение которых представляет большое криминалистическое значение при раскрытии и расследовании преступлений, совершаемых с использованием информационных технологий.

Библиографический список

1. Официальный сайт МВД [электронный ресурс] // режим доступа: https://xn--b1aew.xn--p1ai/reports/item/19412450 (дата обращения 26.10.2020 г.).

2. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Криминологический журнал ОГУЭП. - 2012. - № 3(21). - С. 87-94.

3. Зеленский В.Д., Меретуков Г.М. Криминалистика // Учебник.- Санкт-Петербург: Издательство «Юридический центр», 2015. - С.488.

4. Старостенко Н.И. Криминалистический аспект техник социальной инженерии при совершении преступлений // Вестник Краснодарского университета МВД России. - 2020. - №1 (47). - С. 80-83.

CRIMINALISTIC CHARACTERISTICS OF METHODS OF FRAUD USING METHODS OF SOCIAL ENGINEERING

Starostenko N.I., Starostenko O.A.
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar
email: nstarostenko1996@mail.ru

Abstract. This article is devoted to the study of fraudulent methods committed using social engineering methods. The article provides a forensic analysis of methods of committing fraud using social engineering methods, which has both theoretical and applied significance. The aim of the study is to systematize and generalize the methods of social engineering as ways of committing fraud for effective disclosure and investigation of crimes in this category.

Keywords: Forensic science, crime investigation, fraud in the field of information and telecommunication technologies, methods of social engineering, types of social engineering.