**Социальная инженерия как способ мошенничества**

﻿ Ключевые слова: мошенничество, способ совершения, социальная инженерия, криминалистическая характеристика, данные, конфиденциальная информация, банковская карта, вредоносное программное обеспечение.

Одним из важных элементов криминалистической характеристики мошенничества является способ его совершения. От этого во многом зависит дальнейшее планирование расследования и раскрытие преступления. Недостаточные знания россиян в сфере информационной безопасности позволяет мошенникам ежегодно с успехом использовать при совершении преступления информационные технологии и средства связи в совокупности с приемами социальной инженерии.

Целью является хищение денежных средств с личного счета жертвы или его работодателей путем обмана и злоупотребления доверием. В настоящей статье речь пойдет о современных способах и методах совершения мошенничества с использованием приемов социальной инженерии.

Указанный термин происходит из теории защиты информации и подразумевает «взлом» человеческого сознания в целях побуждения потерпевшего к совершению действий по передаче преступнику конфиденциальной информации или предоставлению доступа к ресурсам ограниченного пользования в обход системы безопасности [1].

При этом главной целью такого метода является побуждение человека к раскрытию конфиденциальной информации для реализации действий, которые в дальнейшем направлены на обход систем безопасности: «Самая эффективная тактика сетевых атак — на нейросеть, уютно расположившуюся между монитором и спинкой офисного кресла» [5].

На сегодняшний день существует множество вариантов, которыми пользуются злоумышленники для выяснения конфиденциальных данных лица, необходимых для хищения безналичных денежных средств, начиная от программ с содержанием специального кода до передачи таких данных самим потерпевшим. К наиболее распространенным способам совершения мошеннических действий в указанной сфере относятся:

-создание сайтов, содержащих ложную информацию позволяющие ввести потерпевшего в заблуждение (и получить личные данные);

-рассылка писем на электронную почту с содержанием вредоносного кода, ссылки;

-незаконное получение регистрационных данных жертвы;

-хищение безналичных денежных средств путем взлома данных, предназначенных для входа в электронные кошельки;

-получение денежных средств через виртуальные интернет магазины либо организации благотворительной акции.

Техники социальных инженеров разнообразны, но их объединяет одно — в основе лежат когнитивные искажения (то есть человеческая глупость и невнимательность) [2].

Помимо этого в последнее время участились случаи мошенничества с помощью социальной инженерии — **метод незаконного получения доступа к определенной информации, не используя технические оборудования и средства.** Главным образом используются слабости человеческого фактора, и заключается в манипулировании поведением человека. Мошенники с помощью социальных и психологических навыков заставляют лицо предпринять какие-либо действия, достаточных для хищения его денежных средств или «овладения личных данных»

К способам совершения мошенничества с помощью социальной инженерии относятся:

1. **фальшивые смс-рассылки**. Обычно в таком сообщении содержится информация о блокировке банковской карты и указанием номера менеджера банка, с которым необходимо связаться. При перезвоне на указанный номер, мошенники представляются сотрудниками банка и уведомляют лицо о том, что с его счета была осуществлена подозрительная попытка перевода денежных средств. Для того, чтобы убедиться в обратном, предлагается проверить свои персональные данные, данные банковской карты и посетить ближайший банкомат для совершения определенных операций для разблокировки карты.
2. **Взлом данных для входа на популярный социальный Интернет-ресурс**. Мошенники, изучая переписку с определенными контактами, делают им рассылку от имени владельца с просьбой занять определенную сумму денег.
3. **Фишинг** (англ. phishing, от fishing — рыбная ловля, выуживание). Данный способ заключается в рассылке сообщений, подделанных по официальное письмо банка или платежной системы, и содержит ссылку на фальшивую web-страницу. Такая страница содержит логотип организации и специальную форму с вводом персональных данных от адреса проживания до пин-кода банковской карты.
4. **Квипрокво** (от лат. Quid pro quo — «то за это»). Мошенники звонят по случайному номеру телефона компании и представляются сотрудниками технической поддержки. Целью является ввод определенных команд самим потерпевшим, позволяющих запустит вредоносное программное обеспечение.
5. **Претекстинг** (от англ. pretexting — предлог) — это действие, отлаженное по заранее составленному сценарию (претексту). Такой способ мошенничества применяется обычно по телефону. Такая техника включает в себя подготовку и предварительное исследование жертвы. Узнаются ее ИНН, дата рождения, номер паспорта, последние цифры счета.
6. **Троянские вирусы**. Троян, также называемый вирусом троянского коня, тип вредоносного компьютерного программного обеспечения (вредоносного ПО), замаскированного под законные или полезные программы или файлы. После установки в компьютерную систему пользователя троян предоставляет разработчику вредоносного ПО удаленный доступ к главному компьютеру, подвергая главный компьютер различным деструктивным или нежелательным действиям [7].

При совершении мошенничества с использованием любого из перечисленных выше методов социальной инженерии злоумышленники стараются придать совершаемым действиям легальный характер.

Можно выделить несколько этапов такого мошенничества:

-Подготовка. На этом этапе мошенник определяет и исследует жертвы, осуществляет сбор информации и выбирает способ атаки. Осуществление действий, сопряженных с обманом либо злоупотреблением доверием. Обычно на этом этапе мошенник беседует с жертвой либо посылает сообщение, содержащее ложную информацию.

-Получение конфиденциальной информации. После того, как мошенник завоевал доверие собеседника, он получается доступ к важной информации.

-Завершение контакта. Прекращение общения осуществляется осторожно, чтобы жертва не догадалась о совершении преступления.

-Хищение средства с использованием полученных данных. С помощью платежных систем и данных потерпевшего мошенники присваивают себе его денежные средства. Личность потерпевшего можно характеризовать как лицо доверчивое, любопытное, зачастую эксплуатируется любезность, лень и даже энтузиазм.

К основным чертам также можно отнести стремление лица сэкономить.

Мошенничество в отношении физических лиц можно **разделить на три группы**.

1) В отношении менее защищенных слоев населения, имеющих низкий уровень финансового достатка и киберграмотности (пенсионеры, жители небольших городов), эффективным способом являются звонки и смс-сообщения.

2) Для экономически активной части населения, которая пользуется Интернетом, мошенники выбирают спам-рассылки писем, содержащие информацию о мнимым скидках, получении льгот, компенсаций, социальных выплат. Такие сообщения содержат вредоносные программы или ссылки на фишинговые сайты, в результате использования которых происходит заражение устройства и компрометация платежных данных его владельца.

3) К последней группе можно отнести активно пользующихся владельцев современных мобильных устройств с операционными системами Android и IOS. Используя вредоносное программное обеспечение, злоумышленники получают доступ и контроль к установленным на устройстве приложениям, которые содержат конфиденциальные данные, что позволяет им осуществлять финансовые операции включая переводы денежных средств с карт жертвы.

По данным ФинЦЕРТ было выявлено восемь основных причин успешности целевых атак [4]:

-Человеческий фактор: недостаточная грамотность сотрудников, открывающих подозрительные письма, пришедшие извне.

-Отсутствие установленных актуальных обновлений на основные продукты, используемые в кредитных организациях.

-Неустановка обновлений.

-Использование слабых паролей.

-Отсутствие сегментирования сети.

-Отсутствие или неправильная настройка систем управления событиями информационной безопасности.

-Неправильная настройка межсетевого экранирования.

-Устаревшие антивирусные базы или отсутствие антивирусного программного обеспечения вообще.

Таким образом, варианты мошенничества с использованием социальной инженерии весьма разнообразны. Такой метод манипуляции действиями человека заключается в использовании слабостей человеческого фактора. Высокая распространенность данного вида мошенничества подтверждает, что современное информирование — это ключевой защитный механизм, который необходим для пользователей средств современной коммуникации.

Социальная инженерия нематериальна, ее невозможно устранить физически. **Самый действенный способ не стать жертвой мошенничества — это не терять бдительности и не позволять мошеннику себя провести.** Помимо этого, защитить конфиденциальную информацию помогает **использование современного антивирусного решения.**

**Литература:**

Бахтеев Д. В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц // Российское право: образование, практика, наука. — 2016. — № 3. — С. 24–26.

Бирюков М. Социальная инженерия или как не стать обманутым // Международный журнал прикладных наук и технологий «Integral». — 2018. — № 2. — С. 22–24.

Кузнецов М. В. Социальная инженерия и социальные хакеры / Кузнецов М. В., Симдянов И. В. // СПб.: БХВ-Петербург. — 2007. — С. 368. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности банка россии. // cbr: — URL: https://www.cbr.ru/Content/Document/File/50959/survey\_0917\_0818.pdf (дата обращения: 05.10.2020).

Социальная инженерия. История из практики именитых пентестеров [Электронный ресурс] // xakep: — URL: https://xakep.ru/2015/06/23/pentesting-197/ (дата обращения: 05.10.2020).

Спам и фишинг во II квартале 2020 года. [Электронный ресурс] // KasperskyLab: — URL: https://securelist.ru/spam-and-phishing-in-q2–2020/97655/ (дата обращения: 05.10.2020).

Троян. [Электронный ресурс]// britannica: — URL: https://www.britannica.com/technology/trojan-computing (дата обращения: 05.10.2020).

Шумский, И. Н. Социальная инженерия как искусство взлома человека // Международный студенческий научный вестник. — 2018. — № 1.

Сивчук, Е. С. Социальная инженерия как способ мошенничества / Е. С. Сивчук. — Текст : непосредственный // Молодой ученый. — 2020. — № 41 (331). — С. 128-130. — URL: https://moluch.ru/archive/331/73995/ (дата обращения: 07.12.2023).