Информация

О видах преступлений (мошенничеств), совершаемых с использованием информационно-телекоммуникационных технологий, и способах защиты от них

Прежде чем рассмотреть одни из наиболее популярных способов мошенничеств, гражданам для защиты своих сбережений необходимо иметь представление о работе тех инструментов, которые используют мошенники, для реализации своей преступной деятельности, так как большинство потерпевших говорит о том, что решение о переводе денег принималось ими из-за «городского номера», с которого звонили, из-за ксерокопии паспорта, которую предоставлял преступник, из-за осведомленности преступников об установочных данных потерпевшего и др.

1) ip – телефония. Часто одной из причин доверия потерпевших мошенникам становится наличие в сообщении «городского» номера телефона, то есть, предполагается, что данный номер телефона имеет конкретную привязку к адресу и лицу. Однако, чтобы получить в пользование номер телефона вида 8800, 8495, 8812, 8499 и любые другие, достаточно зарегистрироваться на соответствующем ресурсе провайдера, выбрать номер и произвести оплату. За отдельную плату полученный номер можно менять каждые 5 минут. Принцип работы ip-телефонии состоит в том, что голосовой сигнал преобразуется в цифровой, передается на виртуальный сервер, после чего отправляется другому абоненту и может быть воспроизведен как на мобильном телефоне, так и на компьютере, оборудованном акустическими колонками и наушниками. Дополним, что абонентский номер ip-телефонии может иметь привычный вид мобильного телефона 8960, 8920 и т.д., достаточно лишь того, чтобы емкость данных номеров была свободна и арендована соответствующим провайдером.

2) ЭСП (электронные средства платежа). В настоящее время любой крупный банк имеет поддержку «онлайн банкинга» и для того чтобы иметь банковскую карту необязательно приходить в отделение банка с паспортом. Мошенники на сайте банка открывают счета и выпускают электронные банковские карты, которые имеют такие же возможности, как и обычная банковская карта, за исключением того, что их нет на пластиковом носителе. Кроме этого данная система реализована у любого оператора мобильной связи и если мошенник просит пополнить мобильную связь, необходимо знать, что с любого номера телефона денежные средства можно вывести на банковский счет.

3) Фишинг. Заключается в сборе информации о гражданах. Часто, когда люди перезванивают на указанные в сообщениях номера телефонов, они удивляются тому, что их данные известны. Во многих случаях мошенники реализуют это с помощью рассылок, создания сайтов, которые на первый взгляд кажутся благовидными. В указанных рассылках предлагается регистрироваться, вводить номера телефонов и фамилию имя отчество, а также иную информацию, после чего данная информация собирается и используется для обмана жителей различных субъектов РФ.

4) СМС-шлюз. В сети интернет существуют сервисы, в которые достаточно загрузить список абонентских номеров для рассылки сообщений

подготовленных мошенниками, и указать текст данного сообщения, после чего нажатием одной кнопки, смс-оповещения получают сотни людей, некоторые из которых выполняют требования преступников.

Для того чтобы избежать обмана и защитить свои банковские счета при поступлении данных сообщений необходимо знать несколько простых правил:

- при получении сообщения или звонка о необходимости погасить кредит, отменить операцию списания, осуществить обмен, внимательно просмотрите текст сообщения и с какого номера оно получено. Часто данные номера отличаются, и рассылка осуществляется с мобильных номеров, что является первым «звонком», сообщающим о мошенничестве.

- необходимо знать, что требования оплаты долга, а также проведения каких-либо других расчетов регламентированы законодательством РФ, и актуальные сообщения от банковских и иных организаций могут нести лишь рекомендательный или информационный характер.

- обратитесь на сайт банка, от имени которого Вам поступило сообщение, в большинстве случаев на главной странице банка изображен телефон «горячей линии». Позвоните по указанному номеру, узнайте, являетесь ли Вы клиентом данного банка (случаи, когда человек является клиентом банка и он об этом не знает, являются частыми), после этого уточните есть ли у Вас долговые обязательства перед данным банком, проводились ли какие-либо операции и другую информацию.

- звонить по номеру, указанному в сообщении или по номеру, с которого данное сообщение поступило, не рекомендуется. Мошенники очень хорошо подготовлены и умеют оказывать влияние на эмоциональное состояние собеседника, не стоит относиться к диалогу с ними легкомысленно. Известны случаи, когда граждане заведомо знали, что их хотят обмануть, и имея намерение пошутить над мошенником, вступали в диалог и в результате лишались своих денежных средств.

- при получении ссылки не переходить по ней, даже, если данная ссылка получена от известного контакта, предварительно перезвоните знакомому контакту и уточнить содержимое. В случае, если ссылка получена от неизвестного контакта, удалите данное сообщение. При этом не имеет значения, какой марки и модели Ваш телефон и какое в нем программное обеспечение.

- после получения Вами смс-сообщения, может последовать звонок, в ходе которого звонящий будет убедительно говорить о серьезности содержания сообщения, в этом случае рекомендуется сослаться на занятость и положить трубку, после чего самостоятельно связаться с банком или добавить телефон в «черный список».

В случае, если Вы все же стали жертвой мошенников, незамедлительно обращайтесь в ближайший отдел полиции, так как при раскрытии данного вида преступлений очень важно быстро получить информацию, а в некоторых случаях Ваше обращение может способствовать предотвращению списания и возврату денег на счет.

В различных источниках люди часто слышат о том, что обман по телефону или по интернету - явление в наши дни нередкое и многие удивляются тому, как люди переводят неизвестным людям денежные средства или дают доступ к своим банковским счетам. Также многие из нас думают, что не могут быть обмануты таким способом, однако это является большим заблуждением. Способов обмана существует множество и направлены они изначально на сосредоточение внимания потенциального потерпевшего, путем воздействия на его эмоциональное состояние, для того чтобы человек не думал о своих действиях, а например: о благосостоянии своих близких или о своем материальном благополучии.

Мошенники – это преступники, которые хорошо оснащены технически, имеют несколько заранее подготовленных моделей поведения и общения, также они хорошо чувствуют эмоциональное состояние собеседника. Единственное оружие граждан в этом случае - это знание, в связи с чем необходимо на постоянной основе осуществлять профилактическую деятельность и уделять внимание осведомленности граждан о способах обмана.

Далее мы рассмотрим наиболее популярные на сегодня способы обмана и рекомендации по недопущению хищений денежных средств посредством звонков на мобильный телефон, а также ресурсов сети интернет.

1-й способ заключается в том, что Вам на мобильный телефон поступает звонок или смс-сообщение из банка о том, что по Вашему счету совершена какая-либо операция или счет необходимо разблокировать. При этом с потерпевшим общается лицо, которое представляется должностным лицом банка и используются абонентские номера, начинающиеся на «8-800», но могут использоваться обычные городские и мобильные номера.

При поступлении такого сообщения или звонка рекомендуется в первую очередь не давать какие-либо данные о себе и о своей банковской карте, далее необходимо перезвонить на «горячую линию» своего банка и сообщить о случившемся, если есть сомнения, что Вы сообщили какие-то сведения, то заблокировать свои лицевые счета и уже при личном посещении банка, убедившись, что Вам ничего не угрожает, разблокировать их.

2-й способ заключается в совершении обмана посредством использования ресурсов бесплатных объявлений (Авито, Юла, Из рук в руки, Авто.ру и др.), а также создании фиктивного сайта от имени онлайн магазина. Данный способ реализуется преступниками тремя основными вариантами обмана: 1-й заключается в размещении объявления или сайта онлайн-магазина и требовании предоплаты на указанные реквизиты; 2-й заключается – в размещении информации о трудоустройстве на хорошо оплачиваемую работу (личный водитель, охрана в администрацию и др.) и требовании внести денежные

средства за оформление документов и разрешений, а также внести денежные средства на счет с условием их возврата по чеку; 3-й вариант является самым хитроумным и состоит в том, что преступник выступает в качестве покупателя и изъявляет желание сразу перевести Вам предоплату за тот товар. Преступник сообщает, что ему необходимы дополнительные реквизиты и данные Ваши и банковской карты после чего получает возможность дистанционно управлять Вашим счетом.

По данному способу мошенничеств гражданам необходимо усвоить несколько основных правил:

- для перевода Вам денежных средств достаточно указать только номер банковской карты, никаких других данных Вам сообщать ненужно. Доводы преступника о том, что у него специфичный банк и нужны дополнительные подтверждения и данные, являются вымышленными. Любому банку для обработки информации о переводе достаточно полного номера банковской карты;

- оплата должна производиться только при получении товара, при этом способы доставки должны быть выбраны такие, где у Вас будет возможность понимать, за какой товар переводятся деньги;

- большинство реальных интернет-магазинов не требует предоплату, как обязательное условие доставки, и Вы можете осуществить заказ в пункт выдачи, где осуществить расчет по факту доставки заказанного товара.

- не переводить и не одалживать деньги незнакомым людям (есть потерпевшие, которым психологически сложно отказывать, поэтому рекомендуем говорить, что у них нет денег);

- если Вам поступают сообщения, внимательно читайте их содержание.

3-й способ заключается в рассылке смс - сообщений о блокировке, проведение операции по счету или предложении обмена товарами и далее в тексте указана ссылка для перехода. При переходе по данной ссылке денежные средства будут списываться разными способами через онлайн банкинг или управлением счетом мобильным номером, при этом денежные средства будут списываться как на переводы, так и пополнения различных счетов и осуществление покупок в онлайн - магазинах.

Основной рекомендацией по данному способу необходимо указать то, что при поступлении данных сообщений не переходить по ссылкам, а сразу звонить в банк на «горячую линию» и уточнять информацию о состоянии счета.

Далее мы будем говорить о мошенничествах, в которых чаще всего страдают пенсионеры и люди пожилого возраста, которые в своем возрасте имеют некоторые проблемы со здоровьем, легко подвергаются стрессовому состоянию. Необходимо понимать, что кроме доведения до них информации о

возможных способах обмана и защиты, их близкие должны многократно напоминать им о том, что в случае возникновения угрозы таких ситуаций, сразу нужно позвонить и сообщить о случившемся.

4-й способ заключается в размещении на радио, телевидении, в интернете и других источниках информации об оказании юридических или медицинских услугах, а также помощи экстрасенсов. У потерпевших складывается ложное доверие к информации данного характера, когда она размещена на указанных источниках, после чего они звонят на телефоны, указанные в объявлениях или рекламе. Преступники, почувствовав, что звонящему нужна помощь, начинают требовать денежные средства, при этом, чтобы убедить в своей добросовестности, требуют осуществить переводы на предъявителя, при этом они имеют огромное влияние на психологическое состояние потерпевшего, который может неоднократно переводить крупные суммы денег и начинает осознавать происходящее в тот момент, когда денежных средств больше нет.

Данный вид мошенничеств отличается хорошей готовностью преступников и для того чтобы защитить себя и свои накопления, могу порекомендовать пенсионерам и людям пожилого возраста, прежде чем обращаться за помощью по таким объявлениям, посоветоваться с родными и близкими, рассказать о данном объявлении. При этом не стоит стыдиться сказать о своем желании вылечиться или получить юридическую помощь, так как в результате можно не получить помощь и лишиться всех своих накоплений. Любые услуги оказываются на основании составленного договора об оказании услуг и оплата за них производится на лицевой счет организации.

5-й способ мошенничеств состоит в поступлении звонка о попадании близкого родственника в различные экстренные ситуации (ДТП, привлечение к уголовной ответственности и т.п.)

При поступлении звонка такого характера необходимо постараться сохранить самообладание и попытаться задать несколько вопросов звонящему (полные данные родственника, где он находится, попросить дать с ним поговорить), это необходимо в первую очередь для того чтобы успокоиться самому и начать осознанно мыслить. После этого положить трубку и позвонить близкому родственнику или лицам с ним проживающим и выяснить все ли в порядке. Преступник будет просить не класть трубку, говорить о том, что у Вас мало времени, будет согласен на перевод многократно меньшей суммы озвученной в самом начале диалога, все это должно быть сигналом к тому, что это обман.

6-й способ мошенничеств состоит в создании страниц двойников или взломе страниц в социальных сетях, после чего преступник получает доступ к списку друзей и личной информации потерпевшего и от имени друзей поступают

сообщения о том, что срочно необходимы денежные средства в долг, обычно требуется не очень крупная сумма денег, при этом злоумышленник указывает, что по какой-то причине его телефон недоступен, а реквизитами счета для перевода является либо мобильный номер, либо какое-либо средство электронного платежа, через которое вы не сможете идентифицировать держателя.

Чтобы избежать обмана таким способом, сразу обратите внимание на характер общения данного лица с Вами, возможно он будет отличаться от привычного общения с тем лицом, от имени которого Вам поступают сообщения. Попытайтесь в переписке задать ему вопрос, касающийся обстоятельств, которые постороннему человеку могут быть неизвестны. Позвоните лицу, от имени которого Вам поступают сообщения, несмотря на его протесты, указанные в сообщении, и спросите действительно ли ему необходимы денежные средства.

Анализ совершенных преступлений показал, что основная часть мошенничеств в г. Калуге совершается лицами, проживающими на территории других субъектов РФ, в том числе отбывающими наказание в местах лишения свободы.

УУР УМВД России по Калужской области.