**Памятка**

**об основных способах совершения сотовых мошенничеств с банковскими картами и мерах их предупреждения**

Одна из схем сотового мошенничества выглядит следующим образом. Злоумышленники звонят и представляются специалистами социальных служб или сотрудниками банков. Они обещают различные льготы, социальные выплаты и компенсации. Предлагают оформить кредит с минимальной ставкой или снизить проценты по действующему кредиту. Своими обещаниями они вызывают доверие и усыпляют бдительность. Во время разговора мошенники предлагают «проверить», какая льгота положена и какую сумму можно получить. Для этого абоненту нужно сообщить паспортные данные и информацию по банковской карте, на которую якобы переведут деньги. Дополнительно уточняют, к какому номеру телефона привязана карта.

Через некоторое время у владельца карты пропадает со счета крупная сумма или все деньги. Злоумышленники воспользовались информацией и оплатили дорогостоящую покупку с карты жертвы.

По-прежнему звонят мошенники, которые выдают себя за работников банков. Сначала владелец карты получает сообщение, что с карты списаны деньги. Сообщение не вызывает сомнения, потому что номер злоумышленников напоминает номер банка. Через несколько секунд злоумышленник звонит и выдает себя за работника службы безопасности банка. Мнимый сотрудник говорит, что прямо сейчас кто-то пытается снять деньги с вашей карты, нужно действовать быстро и сработать на опережение. После такого напора злоумышленник просит назвать одноразовый пароль из смс или кодовое слово — они якобы нужны, чтобы отменить операцию. Как только человек сообщает код, мошенник тут же списывает деньги. Отличительная черта мошенников — говорят уверенно, часто повторяют слово «безопасность» и торопят с ответом.

Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер. После чего происходит списание средств.

Имеют место случаи когда мошенник прикидывается сотрудником банка. А чтобы человек не распознал обман, запугивает его — говорит, что по карте произошла подозрительная операция и списались деньги. Затем злоумышленник интересуется, проводился ли платеж в ближайшее время. Чтобы отменить несанкционированное списание, «представитель банка» предлагает открыть резервный счет и перевести на него деньги. Клиента просят пройти «верификацию»: назвать номер банковской карты и срок ее действия после чего неправомерно завладевают его денежными средствами.

Часто мошенники, представляются сотрудниками полиции, прокуратуры, следственного комитета, другими сотрудниками правоохранительных органов, Центробанка, просят перевести денежные средства под каким-либо предлогом.

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

– сотрудники любого банка никогда не просят сообщить данные банковской карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются эти данные;

– не при каких обстоятельствах никому не сообщать данные банковской карты, а так же секретный код на оборотной стороне карты;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бояться прервать разговор, положить трубку;

– внимательно читать СМС сообщения приходящие от банка;

– никогда и никому не сообщать пароли, и секретные коды, которые приходят в СМС сообщении от банка;

– помнить, что только мошенники спрашивают секретные пароли, которые приходят к в СМС сообщении от банка;

– сотрудники банка никогда никого не попросят пройти к банкомату;

– если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

- при любых подозрениях, что в отношении вас возможно совершаются мошеннические действия, сообщить в полицию по телефону 02, или 020 с мобильного телефона, а так же по телефонам дежурной части УМВД России по г. Кургану 45-64-48, 49-57-97.

Прокуратура района разъясняет:

Статья на тему: «Понятие социальной инженерии. Как защитить себя и своих близких от телефонных мошенников?».

Вопросы борьбы с «сотовыми» мошенничествами на сегодняшний день не теряют своей актуальности и даже имеют повышенный общественный резонанс в связи с резким увеличением таких преступлений. $CUT$

В последнее время получило широкое распространение такое понятие, как «социальная инженерия» - это метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам. Хотя

термин социальной инженерии появился не так давно, сам метод получения информации таким способом используется довольно долго

Выбор той или иной техники социальной инженерии зависит не только от уже известного знания об объекте воздействия, но и от непосредственной ситуативной практики взаимодействия с ним.

Различаются такие техники, как:

1. Фишинг - это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям);

2. Телефонный фрикинг - термин, описывающий эксперименты и взлом телефонных систем с помощью звуковых манипуляций с тоновым набором;

3. Претекстинг - это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие;

4. Обратная социальная инженерия - данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью».

5. Троянский конь - это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная программа;

6. Дорожное яблоко - этот метод представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании.

Государством принимаются многочисленные меры по предотвращению таких фактов, раскрытию преступлений и привлечению виновных лиц к уголовной ответственности. Правоохранительными структурами, средствами массовой информации, общественными и иными организациями проводится большая работа, направленная на правовую пропаганду населения в целях предостережения граждан от преступных посягательств данного вида.

Вместе с тем, как показывает правоприменительная практика, случаи завладения телефонными мошенниками денежных средств граждан путем их обмана, продолжают иметь место и эти случаи приобрели массовый характер.

В 2020 и 2021 годах на территории района зарегистрировано более 70 преступлений, совершенных с использованием средств сотовой связи.

Характерной особенностью мошенничеств указанной категории является сам механизм совершения преступления.

Так, злоумышленники, а это, как правило, хорошо организованные и технически обеспеченные группы, посредством сети Интернет устанавливает номерные емкости абонентских номеров различных операторов сотовой связи в регионах не территории России, после чего, используя имеющиеся у него сотовые телефоны, осуществляет рассылку СМС-сообщений на номера ранее незнакомых лиц, у которых планирует похитить денежные средства, либо осуществляют непосредственно звонки на указанные номера телефонов. При этом преступник сообщает ложные, не соответствующие действительности сведения о том, что кредитная либо расчетная карта владельца абонентского номера заблокирована и для ее разблокирования необходимо связаться с сотрудником банка, представителем которого представляется сам злоумышленник.

При этом указывается тот номер телефона, на который, по замыслу мошенника, лицо будет осуществлять звонок. После того, как владелец абонентского номера звонит на указанный номер телефона, злоумышленник, представившись сотрудником банка либо сотрудником вымышленного «отдела безопасности по банковской системе платежей и переводов», вводит его в заблуждение и под предлогом разблокирования карты получает информацию о том, подключена ли к расчетному счету услуга «мобильный банк». В случае подключения такой услуги, мошенник, опять же путем обмана получает конфиденциальную информацию о номере банковской карты, сроке ее действия и CVC-коде (т.е. коде проверки карты), достаточной для управления денежными средствами, находящимися на лицевом счете.

Далее мошенник, либо его соучастник, в осуществление своего преступного умысла подтверждают информацию о том, что банковская карта якобы заблокирована и под предлогом ее разблокирования получают устное согласие от потерпевшего на осуществление операций по карте. И уже после этого преступник или преступники, используя компьютерную технику с поддержкой сети Интернет, похищают денежные средства с банковской карты гражданина посредством безналичного перевода через интернет-сайты различных компаний на счета абонентских номеров операторов сотовой связи, подконтрольных этим лицам, в связи с чем получают возможность распорядиться похищенным (обналичивание, оплата товаров или услуг и т.д.).

В том случае, если услуга «мобильный банк» у гражданина не подключена, то мошенник в ходе телефонного разговора с владельцем банковской карты просит подойти к ближайшему банкомату и осуществить ряд операций. Получив согласие от потерпевшего, злоумышленник сообщает в ходе телефонного разговора алгоритм действий с банковской картой и банкоматом и буквально под диктовку преступника жертва мошенничества переводит денежные средства со своего счета на расчетные счета или абонентские номера, названные мошенником, в результате чего у последнего также появляется возможность распорядиться денежными средствами потерпевшего.

МОЖНО ВЫДЕЛИТЬ ОСНОВНЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА:

***«НЕ ДОПУСТИТЬ НЕЗАКОННОГО СIIИСАНИЯ ВАШИХ ДЕНЕГ»***

Мошенники, представляются сотрудниками безопасности банка, либо единой службы безопасности банков, сообщают, что была попытка незаконного списания средств со счета банковской карты и чтобы остановить эту транзакцию нужно

назвать реквизиты карты (номер, ФИО держателя карты, CVV-код) и данные о сумме на счету карты.

***«ВАША КАРТА ЗАБЛОКИРОВАНА»***

С номеров, которые похожи на сервисный номер Сбербанка (900), например

«9ОО» (используются буквы «О»), 9 0 0 (используются пробелы между цифрами), на Ваш телефон поступает SMS-сообщение с текстом, что банковская карта заблокирована. После чего мошенники пытаются узнать реквизиты карты и пароли доступа в личный кабинет.

***«ДОЛГ ПО КРЕДИТУ»***

Неизвестный представляется сотрудником банка и просит погасить задолженность по кредиту, который Вы не брали и в ходе разговора уточняются данные карты (ПИН-код, CVV—код и срок действия карты).

***«КУПЛЯ-ПРОДАЖА ЧЕРЕЗ ИНТЕРНЕТ»***

Мошенник под видом покупателя сообщает, что желает приобрести товар, но проживает в другом городе и предлагает оплатить товар путем перечисления денежных средств на Вашу карту. Для этого он просит Вас назвать номер карты, владельца карты, срок действия карты, код на обратной стороне, а так же сотовый номер, привязанный к карте, либо по умолчанию использует номер, указанный в объявлении. После получения этих сведений мошенник использует данные о карте для оплаты покупок в сети Интернет.

Другой вариант, когда мошенник, выступающий в роли «покупателя» предлагает Вам пройти к банкомату и, якобы произведя некоторые операции, получить деньги.

Также злоумышленник под видом продавца просит у Вас предоплату за товар, а при получении денег перестает выходить на связь. Либо предлагает пройти по направленной Вам ссылке для авторизации, где необходимо выведение Ваших персональных данных.

***«КОМПЕНСАЦИЯ»***

Неизвестные звонят по телефону, представляясь следователями правоохранительных органов, сотрудниками прокуратуры, и сообщают о возможности возместить стоимость услуг адвоката, а также получить моральную компенсацию за приобретенные фальсифицированные биодобавки или лекарства, а для ее получения необходимо оплатить пошлину.

***«ОШИБОЧНЫЙ ПЕРЕВОД»***

Вам приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок, и Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильные переводом»

либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

***«ПОМОЩЬ ДРУГУ»***

Неизвестные путем взлома аккаунта друга в социальной сети, направляют Вам сообщение с просьбой пополнить счет или в долг перевести на банковскую карту деньги.

***«РОДСТВЕННИК В БЕДЕ»***

Под видом близких родственников мошенники звонят Вам по телефону и сообщают, что задержаны за совершение какого-либо преступления или дорожно-транспортного происшествия с жертвами. Для освобождения от уголовной ответственности просят перечислить денежные средства через банкомат или передать курьеру.

Большую часть пострадавших от данного вида преступных посягательств составляют женщины в возрасте от 35 до 50 лет, работающие в бюджетной сфере, и пенсионеры. С одной стороны, это обусловлено неглубокими познаниями данной категории граждан в сфере обслуживания банковских карт и зачастую они попросту не знают простые правила безопасности при их использовании.

С другой стороны немаловажное значение оказывает психологический фактор, который проявляется в создании у жертвы преступления чувства беспокойства за сохранность денег и необходимости незамедлительного совершения действий, направленных на их сбережение. В печальном итоге, все происходит наоборот.

Расследование уголовных дел данной категории является трудоемким и осложняется, в первую очередь, тем, что следователями по таким делам очень часто направляются поручения о выполнении отдельных следственных действий своим коллегам из других областей, а это, в свою очередь, занимает продолжительное время. Также длительное время исполняются ответы на запросы из сотовых компаний, ряд следственных действий можно провести только с судебного разрешения. Все эти, и другие обстоятельства, приводят к продлению процессуальных сроков предварительного расследования. А если к уголовной ответственности привлекается лицо (или группа лиц), совершивших ряд сотовых мошенничеств в отношении граждан, проживающих в разных субъектах Российской Федерации, следствие по таким уголовным делам может производиться длительное время.

Другой особенностью расследования таких уголовных дел является тщательная подготовка преступников к совершению преступлений, обладание ими специальными познаниями в сфере обслуживания банковских карт, а также активное сокрытие следов преступлений.

Можно отметить следующие обстоятельства, способствующие снижению результативности раскрытия преступлений, связанных с мошенническим хищением денежных средств граждан:

- частая смена телефонов и сим-карт злоумышленниками, что не дает возможности оперативно определить лицо, использующее их при совершении преступлений;

- оформление сотовыми компаниями сим-карт без подтверждения документа, удостоверяющего личность лица, оформляющего договор на оказание ему услуг, а также оформление менеджерами большого числа сим-карт на одного из лиц, ранее приобретавших сим-карты, либо передача их без оформления на кого-либо;

Несмотря на имеющиеся трудности, правоохранительными органами преступления данного вида раскрываются, виновные лица привлекаются к уголовной ответственности и предстают перед судом.

Для того, чтобы уберечь себя и своих близких от телефонных мошенников нужно помнить и соблюдать ряд простых правил:

1. В сообщениях настоящих банков никогда не указывается номер сотового телефона для связи. У каждого банка есть федеральный или городской номер круглосуточной поддержки. Поэтому, при поступлении на телефон СМС-сообщения о блокировке банковской карты не нужно звонить на указанный в сообщении номер, а позвонить на тот номер, который указан на оборотной стороне Вашей карты (звонок бесплатный) и уточнить поступившую информацию. Также можно обратиться в ближайшее отделение банка, обслуживающего Вашу карту.

2. Если Вы все-таки осуществили звонок на указанный в СМС-сообщении номер и Вас убеждают осуществить ряд финансовых операций, ни в коем случае не нужно сообщать любые сведения о Вашей карте (номер, срок действия, CVC-код или ПИН-код), в том числе кодовое слово, а напротив, уточнить, из какого Банка звонят, известны ли этому лицу Ваши анкетные данные (ФИО, дата рождения, место жительства), поскольку у специалистов настоящего банка должна быть эта информация.

3. Запомните, что выяснять по телефону данные банковской карты могут только мошенники. Кредитные организации и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов или 3-х значного кода. Никакие сотрудники государственных правоохранительных органов не могут предлагать Вам перечислить деньги за что-либо или требовать выполнить действия, которые Вам рекомендуют совершить якобы банковские служащие, у них нет таких полномочий.

4. Банки не сохраняют денежные средства на так называемых «специальных» счетах, поэтому любые действия по переводу денег, которые Вас просят совершить на другом конце провода, направлены на их хищение путем мошенничества,

***Поэтому осуществлять переводы денежных средств на какие-либо счета ни в коем случае нельзя!!!***

**Уголовная ответственность за создание фирм-однодневок**

Статьей 173.2 Уголовного кодекса Российской Федерации (далее – УК РФ) предусмотрена ответственность за незаконное использование документов для образования (создания, реорганизации) юридического лица. В ней закреплены два самостоятельных состава преступления. Уголовная ответственность за указанные деяния введена Федеральным законом от 07.12.2011 № 419-ФЗ.

Предоставление документа, удостоверяющего личность, или выдача доверенности, если эти действия совершены для внесения в единый государственный реестр юридических лиц сведений о подставном лице предусматривает ответственность в части 1 указанной статьи. Преступление признается оконченным с момента получения названных документов лицами, которые в последующем будут использовать их для образования юридического лица. Указанное преступление совершается с прямым умыслом, направленно на реализацию специальной цели – внесение в Единый государственный реестр юридических лиц сведений о подставном лице.

За совершение данного преступления предусмотрено наказание в виде штрафа в размере от 100 тыс. до 300 тыс. рублей или в размере заработной платы или иного дохода осужденного за период от 7 месяцев до 1 года, либо обязательных работ на срок от 180 часов до 240 часов, либо исправительных работ на срок до 2 лет.

Частью 2 данной статьи закреплена уголовная ответственность за действия, направленные на образование юридического лица. К ним законодатель отнес приобретение документа, удостоверяющего личность, или использование персональных данных, полученных незаконным путем, если эти деяния совершены для внесения в единый государственный реестр юридических лиц сведений о подставном лице. Под приобретением документа, удостоверяющего личность, понимается его получение на возмездной или безвозмездной основе, присвоение найденного или похищенного документа, удостоверяющего личность, а также завладение им путем обмана или злоупотребления доверием.

К уголовной ответственности привлекается лицо, имеющее намерение образовать юридическое лицо, используя чужие документы. Наступает она независимо от того, зарегистрировано ли юридическое лицо или нет. Виновные лица наказываются штрафом в размере от 300 тыс. до 500 тыс. рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет, либо принудительными работами на срок до 3 лет, либо лишением свободы на тот же срок.

Центральный Банк Российской Федерации разработал информационные материалы, направленные на повышение уровня финансовой киберграмотности населения в целях противодействия мошенничеству и хищениям с использованием методов социальной инженерии. Указанные материалы размещены в открытом доступе в информационно телекоммуникационной сети «Интернет» и доступны для скачивания по ссылке: https://finclass.info/_wt/cybergram.