**ВИДЫ МОШЕННИЧЕСТВ**

**Розыгрыш призов**

В этом случае мошенник звонит на мобильный телефон абонента, представляется ведущим популярной радиостанции, либо, дилером крупной компании, поздравляет его с крупным выигрышем (например, автомобиль «Шевроле-Авео») в лотерее, организованной компанией, или приходит СМС-сообщение с аналогичным текстом. Параллельно информация о результатах розыгрыша размещается на интернет-сайте (сайты-однодневки). Затем потерпевшему сообщают, что для получения приза необходимо заплатить налог на выигрыш (или пошлину за оформление), для этого необходимо перечислить деньги через терминал оплаты на определенный телефонный номер и потом перезвонить. После перевода денег, потерпевший звонит «дилеру» и сообщает о перечислении, мошенник извиняется и говорит, что пока деньги перечислялись, увеличилась процентная ставка налога (госпошлины), либо называется другая причина, и необходимо дополнительно перечислить денежные средства. Схема о необходимости дополнительного перечисления денежных средств может отрабатываться столько раз, сколько потерпевший соглашается платить.

**Случай с родственниками**

Мошенник, используя мобильный телефон, осуществляет перебор номеров по возрастанию или убыванию последних цифр, звонит на телефон (стационарный или мобильный) представляется родственником или знакомым, и взволнованным голосом сообщает о том, что задержан сотрудниками полиции за совершении преступления или правонарушения (ДТП, хранение оружия или наркотиков, нанесения тяжких телесных повреждений), но есть возможность за определенное вознаграждение «решить вопрос». Цена вопроса обычно составляет от 1 до 300 тысяч рублей. Если потерпевший соглашается отдать деньги, то ему называют способ передачи (для передачи денег используются водители такси, банковские переводы и переводы через терминалы оплаты).

**Заказ обеда в кафе (продуктов питания) от имени администрации района**

Потерпевшему (администратору кафе) звонит неизвестный и просит приготовить обед для администрации района на несколько персон, обязательно с дорогим алкоголем (до 9 тысяч рублей). Так как дорогого алкоголя в данном кафе нет, то директор предлагает его купить в магазине, о чем уведомляет заказчика. Заказчик сначала соглашается, а затем просит вместо покупки дорогого алкоголя, перечислить деньги на абонентский номер, так как в данный момент пополнить счет самостоятельно не может, но обещает отдать при расчете за обед. В указанное время на обед никто не приезжает.

**Кроме того практикуются и другие способы мошенничеств с использованием сотовой связи, например:**

**СМС-просьба**

Абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если он недоступен – положи определенную сумму денег. Потом все объясню».

**Платный код**

Поступает звонок от, якобы, сотрудника службы технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или, для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

**Штрафные санкции оператора**

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения), и поэтому ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды.

**«Ошибочный» перевод средств**

Абоненту поступает смс-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина или женщина сообщает, что ошибочно перевели деньги на его счет, и просят вернуть их обратно тем же «Мобильным переводом». Потерпевший переводит деньги, затем обнаруживает, что присланная сумма также была снята (осуществлен возврат денежных средств).

**Скрытая информация о повышенной тарификации СМС-сообщений**

Пользователю предлагается изучить содержание СМС-сообщений и список входящих и исходящих звонков интересующего абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 рублей на указанный короткий номер и вписать в прилагаемую форму номер телефона абонента. После того, как пользователь оправляет СМС, с его счета списывается сумма больше, чем была ранее указана мошенниками – до 500 рублей, а интересующая информация так и не поступает.

**Хищение денежных средств с банковских карт**

**I.** На сотовый телефон абонента приходит SMS сообщение о том, что его банковская карта заблокирована, и ему предлагается позвонить на определенный номер для получения подробной информации. Когда владелец карты звонит по указанному телефону, ему сообщают о том, это служба безопасности банка, и что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем действуют по следующим схемам:

1. Просят сообщить свои данные «оператору» (с указанием номера карты и ПИН-кода), либо заполнить аналогичные «документы» на сайте - для ее перерегистрации. Получив реквизиты пластиковой карты, злоумышленники переводят денежные средства на номер своего телефона при помощи «Личного кабинета» в интернет-банке (если услуга поддерживается банком).

2.Просят подойти к банкомату (для держателей карт «Сбербанка») и набрать специальную команду для выдачи паролей (команду потерпевший набирает под диктовку). После этого на руки потерпевшему выдается чеки с указанием нескольких (до двадцати) паролей. Каждый пароль выдается на определенную банковскую операцию по переводу денежных средств через сервер «Сбербанк» онлайн» (оплата ЖКХ, оплата мобильных телефонов, штрафов ГИБДД и т.д.). Количество выдаваемых паролей зависит от количества доступных (подключенных) банковских услуг. После того, как на руки потерпевшему выдаются чеки с указанными в нем секретными паролями, преступники просят сообщить им определенный пароль (для перевода средств на мобильный телефон), якобы, для активации карты. Зная указанный пароль, при помощи услуги «Сбербанк» онлайн» через интернет денежные средства переводятся на указываемый мобильный телефон (услуга «Автоплатеж»).

**II.** Потерпевший имеет карту с подключенной услугой «Мобильный банк» (операции по банковской карте дублируются SMS-сообщениями на мобильный телефон потерпевшего). Потерпевший дает объявление о продаже дорогой собственности (обычно, машины). Через некоторое время ему звонит неизвестный, говорит, что хочет ее купить, но так как в настоящее время он находится в командировке, то может внести задаток на банковскую карточку (сумма, обычно равна половине стоимости машины, и не менее 200 тысяч рублей), просит сказать номер карты. Через некоторое время, неизвестный перезванивает и говорит, что произвел платеж. Потерпевший проверяет свою карту – денежных средств нет. Перезванивает и сообщает об этом «покупателю». «Покупатель» явно «огорчается» и, якобы, перезванивает в банк, потом объясняет, что для перевода денег необходимо сообщить фамилию имя отчество продавца, потерпевший сообщает. Через некоторое время «покупатель» снова сообщает о переводе средств. Потерпевший проверяет карточку – денег не поступало, перезванивает «покупателю». «Покупатель» опять, якобы, «перезванивает» в банк, потом говорит, что из-за технических причин платеж не прошел, и предлагает перевести деньги банковским переводом, но для этого ему нужны номер и серия паспорта продавца. Зная фамилию, имя и отчество, номер и серию паспорта, злоумышленники звонят в сотовую компанию, в которой зарегистрирован абонентский номер потерпевшего, и просят поставить безусловную переадресацию с номера потерпевшего на свой номер (оператору рассказывается история о том, что телефон оставлен в офисе, офис под охраной, но очень необходимо принять звонок от инвестора/банка/ и т.д.). Затем звонят потерпевшему и говорят, что, якобы, сотрудники банка сообщили, что у потерпевшего были какие-то проблемы с картой, и просит отправить SMS в «Мобильный банк» для получения кода доступа (чтобы проверить, что карта доступна), только после этого банк вернет денежные средства, якобы, переведенные ранее «покупателем», и тот сможет перевести ему деньги банковским переводом. Потерпевший отправляет SMS в банк с командой о выдаче секретного кода, ответная SMS с паролем приходит «покупателю» (благодаря безусловной переадресации). Зная, номер карты и пароль доступа, преступники переводят все деньги с карты через онлайн банк на номер своего мобильного телефона, а затем снимают их (данная услуга предоставляется некоторыми операторами сотовой связи).

**Компенсация за ранее приобретенные лекарственные средства и медицинское оборудование.**

Потерпевшему, ранее заказывавшему по рекламным телефонам БАДы (под видом лекарственных средств), либо, якобы, медицинские приборы, звонит неизвестный и, представившись (должность, фамилия, отчество) сотрудником организации по защите прав потребителей или федеральной службы компенсационных выплат, или же судебным приставом, говорит, что деятельность фирмы, которая поставляла товар, признана незаконной, ее счета арестованы, и теперь всем заказчикам положена компенсация (денежная сумма в десятки раз превышает стоимость заказанных товаров).

Для получения компенсации необходимо перечислить определенную сумму (8-20 тысяч рублей) блиц переводом через банк для оформления страховки (оформления вклада, аренды банковской ячейки), данная сумма, якобы, возвращается потерпевшему потом вместе с компенсационной выплатой. Потерпевшему оставляется контактный телефон, по которому он должен позвонить и сообщить о переводе средств.

После перевода средств потерпевшему опять звонит уже другой сотрудник и говорит, что в связи с тем, что Вас признали малоимущим, размер компенсации увеличили на 100 тысяч, а документы уже готовы на прежнюю сумму, поэтому необходимо перевести определенную сумму (10-40 тысяч рублей) на переоформление документов. После того, как потерпевший выполняет следующий перевод, ему звонит другой «представитель» и говорит, что перевод задержался и необходимо перевести деньги за хранение денежных средств (аренду банковской ячейки, оформление сберкнижки и т.д.).

Звонки с известием о повышении суммы компенсации и требованием перевода денег могут поступать до тех пор, пока у потерпевшего есть деньги, и он ничего не подозревает.

ОМВД России ЗАТО Свободный.