

ПРОКУРАТУРА ПРЕДУПРЕЖДАЕТ

Ежедневно гражданам звонят мошенники, представляясь работниками кредитно-банковских учреждений, сотрудниками правоохранительных органов, работниками организаций из сферы государственных услуг, операторами сотовой связи и т.п., при этом последние вводят граждан в заблуждение под предлогами «якобы» незаконного списания денежных средств, взлома личного кабинета «Госуслуг» или «Сбербанк онлайн», продления или смены номера сотового телефона с целью получения личных данных (паролей, кодов доступа). В результате указанных действий мошенники оформляют от имени граждан удаленно посредством сервисов «Госуслуги» и «Сбербанк онлайн» кредиты, мошенническим способом похищают у граждан денежные средства путем убеждения последних перечисления на подконтрольные преступникам счета.

У преступников есть базы данных номеров абонентов сотовых операторов и базы данных банковских карт. Они знают Ваши фамилию, имя, отчество, номер телефона и что у Вас есть банковская карта в определенном банке. Мошенники умеют хорошо убеждать и обладают навыками психологического воздействия.

ЗАПОМНИТЕ

Никто не имеет права выяснять реквизиты Вашей карты и количество денежных средств на ней. Никакая организация и никакое лицо этого делать не могут. Операторы сотовой связи не вправе прекратить действие договора на оказание услуг связи посредством телефонного звонка. Сотрудники правоохранительных органов не звонят гражданам для оказания помощи в раскрытии преступлений.

Если у Вас спрашивают данные вашей карты или пароль из СМС-сообщения, который Вам направлен для восстановления доступа в сервисы «Госуслуги» или личные кабинеты банка, прекратите разговор, это мошенники, ни в коем случае не передавайте коды доступа.

Банковские работники не звонят гражданам с требованиями перевода денежных средств на безопасный счет, в т.ч. наличных сбережений граждан, находящихся у них на руках.

ЗАПОМНИТЕ

Никакие сотрудники государственных правоохранительных органов не могут и не будут предлагать Вам перечислить деньги за что-либо или куда-либо, у них нет таких полномочий.

ОСНОВНЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

«НЕ ДОПУСТИТЬ СПИСАНИЯ ВАШИХ ДЕНЕГ»

Мошенники, представляются сотрудниками безопасности банка, 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), данные о сумме на счету карты или переслать денежные средства на сохранение на счет мошенников.

«ВАША КАРТА ЗАБЛОКИРОВАНА»

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

Неизвестный от имени сотрудника банка говорит об обращении в банк лица с генеральной доверенностью от Вашего имени за получением кредита, в ходе разговора выясняет данные Вашей карты, счета и коды доступа, после чего получает доступ к банковскому счету и похищает принадлежащие Вам денежные средства.

«КУПЛЯ-ПРОДАЖА ЧЕРЕЗ ИНТЕРНЕТ»

Мошенник под видом покупателя сообщает, что желает приобрести товар, но проживает в другом городе и предлагает сделать предоплату на Вашу карту. Для этого он просит Вас назвать реквизиты карты. После получения этих сведений мошенник использует данные карты для оплаты покупок в сети Интернет.

Кроме того, мошенник может попросить назвать ему коды из СМС с номера 900, для входа в личный кабинет Сбербанк-Онлайн для оформления кредита на Ваше имя и последующего перечисления на свой счет.

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.

Продавец, разместивший объявление на сайтах «Avito.ru», «drom.ru» и др. просит перевести на карту предоплату или всю сумму покупки с целью последующей отправки товара, в том числе посредством услуг транспортных компаний, при этом предоставляет в переписке данные карты, транспортные и иные документы, впоследствии получив деньги прекращает переписку.

Будьте внимательны при переводе денежных средств продавцу за товар! Проверяйте продавца заранее, не высылайте денежные средства за товары, приобретаемые посредством сайтов объявлений, а также через незнакомые приложения и сервисы.

«ПОЛУЧИТЕ ДОПОЛНИТЕЛЬНЫЙ ДОХОД / ЗАБЕРИТЕ ВЫИГРЫШ»

Неизвестные звонят по телефону, предлагают получить дополнительный доход, для этого нужно внести небольшие денежные средства на счет организации, занимающейся брокерской торговлей, фьючерсами и т.п., после внесения денежных средств Вам утверждают о выигрыше и большом доходе, но вывести денежные средства невозможно.

Другой вариант работы организации, занимающейся брокерской торговлей, фьючерсами и т.п.: мошенники посредством использования интерфейса, в котором указан Ваш брокерский счет и результаты торговли с указанием прибыли, как правило в долларах или евро, дают возможность снять небольшую сумму в виде прибыли, после чего уверенный в легальности работы организации потерпевший перечисляет на виртуальный счет крупную сумму денежных средств, которые впоследствии не имеет возможности вернуть. Также мошенники предлагают внести денежные средства для уплаты «налога» и страховки для получения «вывода» денег, но никакие налоги и страховые взносы на самом деле не уплачиваются.

Вам приходит сообщение о выигрыше в лотерею/казино и т.п., для того чтобы получить выигрыш необходимо перейти по ссылке. После чего необходимо ввести данные своей банковской карты, а после чего с Вашей банковской карты происходит списание денежных средств.

При просмотре видеороликов, размещенных на различных сайтах в сети «Интернет», в том числе «YouTube» пользователь просматривает информацию о возможности заработать посредством использования услуг различных организаций, реализации государственных программ, в том числе возможности получения доходов от реализации природных ресурсов (нефти, газа), при этом перейдя по ссылке и предоставив данные своего банковского счета или карты, Вас обманывают и похищают денежные средства.

«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, которые похищают.

«БЛОКИРОВАНИЕ НОМЕРА ТЕЛЕФОНА/ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ ДОГОВОРА НА ОКАЗАНИЕ УСЛУГ СВЯЗИ»

От имени представителя оператора сотовой связи звонят неизвестные, при этом называют Ваши персональные данные и в ходе разговора сообщают об истечении срока действия договора связи и блокировке номера сотового телефона, при этом предлагают восстановить доступ посредством его восстановления и просят назвать код из СМС-сообщения, которые сами в это время направляют жертве. Сообщив мошенникам код из СМС – сообщения, последние получают доступ к сервисам личного кабинета «Госуслуги» и других сервисов, к которым привязан номер сотового телефона, после чего от имени гражданина оформляют кредиты либо похищают находящиеся на счетах денежные средства.

ВАЖНО: если Вы поменяли SIM-карту, то в обязательном порядке обратитесь в банковские учреждения, портал государственных услуг и другие сервисы, в рамках которых Вы использовали для доступа предыдущий номер телефона, и смените номер на новый.

«НЕПОВИНОВЕНИЕ СОТРУДНИКАМ ПОЛИЦИИ/НЕЯВКА ПО ПОВЕСТКЕ»

От правоохранительных органов (МВД, Следственный комитет и т.д.) звонит неизвестный, представляясь сотрудником указанных органов, и выясняет причины неявки к сотруднику по повестке, после угрожает привлечением к ответственности, в ходе разговора выясняет данные Вашего банковского счета и другие данные получает к ним доступ либо под разными предлогами требует от жертвы перечисления денежных средств на подконтрольные ему счета.

Важно вовремя понять, что Вам звонят мошенники и прекратить разговор, что позволит сохранить денежные средства.