На заметку

Мошенники «заработали» на инвестициях



Только за два выходных дня жители Челябинска перечислили преступникам свыше двух с половиной миллионов рублей. В обоих случаях на руку злоумышленникам сработала схема, связанная с инвестициями.

В первом случае в отдел полиции «Металлургический» обратилась 67-летняя местная жительница. Она обогатила киберпреступников на два миллиона рублей.

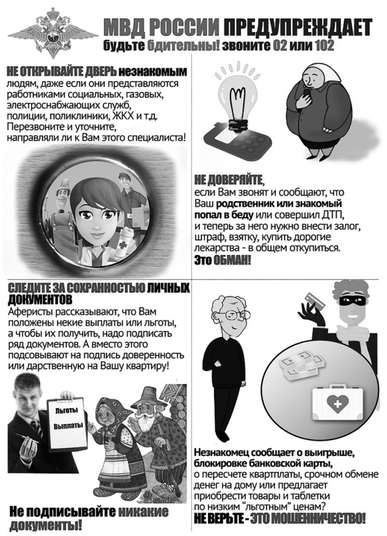
Потерпевшая рассказала, что в мессенджере ей поступил звонок от неизвестного, который представился финансовым аналитиком, занимающимся инвестициями, и предложил заработок путём инвестирования. Далее он пояснил, что для получения заработка необходимо открыть счёт в приложении и перевести 50 тысяч рублей.

Затем мошенники убедили женщину взять кредит в банке, где ей было одобрено свыше 1,8 миллиона рублей. Эти деньги она перевела на указанные ей номера. Женщина увидела, что заработок в приложении вырос, и решила вывести средства, но ей это не удалось. Тогда она поняла, что общалась с мошенниками, и обратилась в полицию.

С аналогичным случаем в отдел полиции «Северо-Западный» обратилась её ровесница – тоже 67-летняя жительница Челябинска. У неё мошенники выманили более 600 тысяч рублей. Ей также в мессенджере поступил звонок от неизвестного абонента с предложением заработка на инвестициях. Под руководством мошенников пенсионерка скачала на мобильный телефон приложение, куда перевела более 600 тысяч рублей. Позже она вывела с платформы четыре тысячи, но оставшуюся сумму вывести так и не удалось. Поняв, что она стала жертвой мошенников, потерпевшая обратилась в полицию.

По данным фактам возбуждены дела по статье 159 Уголовного кодекса РФ – «Мошенничество».

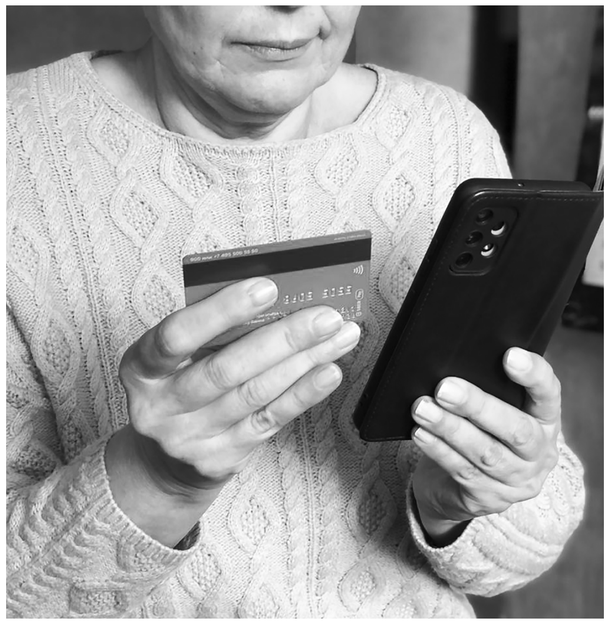
Сотрудники полиции напоминают о необходимости быть бдительными при инвестировании денежных средств. Внимательно изучайте официальную информацию о компании. Следует помнить, что для мошенников характерно обещание высоких процентов и стабильной прибыли новичкам, отсутствие регистрации. Если противоправное деяние всё-таки произошло, незамедлительно обращайтесь в полицию. Это можно сделать по телефонам дежурной части 02/102, либо обратиться в районный отдел полиции по месту совершения правонарушения.



Ой, я вам деньги ошибочно переслала...

Подробно. Мошенники успешно реализуют как старые, так и новые схемы отъёма денег у населения

Чаще всего целью обмана выступают: живые деньги, которые жертва переведет мошеннику, в том числе кредитные; коды доступа к банковским приложениям и коды доступа к госуслугам – для последующей смены пароля и полного присвоения ваших данных.



Нашёлся стаж – получите деньги

Уже нет, наверное, ни одного человека, кто не сталкивался со звонками от «сотового оператора». Развод от лица «оператора» по праву можно считать самым массовым и многовариантным.

Вас убеждают, что у вас истек срок обслуживания номера/СИМ-карты, мол, вам направляли уведомление о продлении и вот-вот отключат номер. Прямо сейчас, в течение 5 минут после разговора. Если задать вопрос о том, почему раньше ничего не продлевалось, то мошенники сочинят красивую историю о том, как «отказала западная программа из-за санкций и теперь всё вручную». Также возможны варианты с «переводом номера к другому оператору». Чтобы прекратить все эти печали нужно всё срочно продлить, сообщив мошеннику код от госуслуг.

Ещё могут «безобидно» попросить уточнить и подтвердить персональные данные. На фоне поправок об ужесточении контроля за продажей СИМ-карт активизировались и жулики, под этим соусом вымогая коды от госуслуг. Легенда почти аналогична продлению: «...вам направляли уведомление, вы его не видели, у вас 10 минут на подтверждение».

Мошенники могут вести с вами беседы о качестве, тарифах и обновлении «до 5G по такой же цене», подключении очень выгодного предложения на домашний или мобильный интернет. Этот обман продвигается под видом «заботы об абоненте». Никакого пугания и давления «прям сейчас», всё кротко и с максимальной вежливостью, от чего в разы опаснее.

Звонки из «социального (пенсионного фонда) и Минтруда» – по этой теме жульё не гнушается звонить всем и вся, при этом не только пенсионерам или лицам предпенсионного возраста. Стаж, надбавки, перерасчёты, индексации – поводов для звонка великое множество. Общее у них лишь то, что для решения обозначенной проблемы нужна электронная запись с кодом от госуслуг.

Могут порадовать, что нашёлся потерянный трудовой стаж, который нужно неприменно по личному заявлению на личном же приёме включить в общий стаж. При этом пенсионерам ещё и предлагают выбрать: забрать недоплаченные деньги единовременно или раскидать на всю пенсию.

На фоне изменения порядка индексации пенсий с 2024 года жулики придумали новый способ обмана: якобы для индексации пенсии нужно явиться в СФР лично и написать заявление. Явка строго по электронной очереди. Звонок поступает исключительно пенсионерам.

Будьте бдительны, услышав, что вами заинтересовались «спецслужбы или полиция». Эти пытаются сходу навести на собеседника жути. В зависимости от «высоты» структуры в избранной легенде будет отличаться и тон общения: чем «серьезнее» орган, тем более дерзко и агрессивно будут вести себя жулики. В их речи может промелькнуть аббревиатура КВК-счёт. Это якобы «код внутреннего клиента». Мошенники будут утверждать, что его хищение влечёт массу проблем и угроз, вплоть до полного захвата «электронной личности» гражданина. Естественно, что никакого такого кода-счёта не существует!

Вас могут оповестить, что взломаны все ваши личные кабинеты во всех банках. Этому будут предшествовать спам-атаки на номер телефона и кучи самых разнообразных СМС-кодов (в основном из МФО), вам будут звонить «сотрудник Центробанка» или иных органов, утверждая, что «всё пропало!». Ещё вас могут грозно припугнуть тем, что вы якобы перевели деньги на финансирование всяких запрещённых и недружественных структур. После клятв и заверений в обратном, радостно сообщат, что вас взломали и нужно срочно «ловить мошенников». А там переводы на безопасный счёт, продажа имущества и прочие радости жизни...

Заплатил налог? Спи спокойно!

В преддверии срока уплаты имущественного налога (1 декабря), да и есть все основания полагать, что и после его истечения, мошенники звонят под видом ФНС. Уточняют, получили ли вы квитанцию, и далее отрабатывают вариант со «сбоем». Нужно получить новые реквизиты или извещение для корректной уплаты.

Пенсионеры легко ведутся на звонки «по поводу полиса ОМС» или из больницы, поэтому мошенники используют сплошной обзвон в надежде, что кто-то да поведётся на обман, связанный с заменой/обновлением полиса ОМС. Вариаций развода несколько. Это и выдача нового пластикового с QR-кодом, и истечение срока, и невозможность автоматического продления из-за санкций. И, конечно же, нужен код от госуслуг. Про то, что полисы давно могут быть электронные, жульё предпочитает не знать.

Не захотите менять полис, вас пригласят на прохождение флюорографии/диспансеризации/медосмотра/получения бесплатных лекарств. Опять же под видом «дежурного врача из поликлиники», регистратуры и так далее, убеждая, что человеку нужно под тем или иным соусом явиться в больницу.

Мошенники могут представляться сотрудниками Почты России или архивного отдела МФЦ и утверждать, что на ваше имя поступило важное письмо. Ещё и обязательное к получению. Отказаться нельзя, иначе статья/штрафы/платное хранение... Другие представятся сотрудниками Энергосбыта и убедят вас, ссылаясь на несуществующие приказы министерств и правительства, что нужно срочно поменять счётчик. Пока что бесплатно, а потом – только за деньги. Если так сложится, что у жертвы уже новый счётчик, и она начнёт задавать логичные вопросы, то будет применена схема «нужно внести в реестр счётчик, иначе вновь замена!».И снова через электронную очередь, госуслуги, коды...



Перед вами могут разыграть комбинацию «неизвестный интернет-заказ». Звонящий представляется курьером или представителем транспортной компании, разыгрывая грусть-печаль по поводу отсутствующего адреса или же просит уточнить имеющийся адрес, называя его с потолка. Далее – синхронизация с госуслугами и всё по стандарту выманивания кода. Если вы где-то оставили негативный отзыв под своими ФИО, будьте готовы к тому, что мошенники «прикинутся магазином» и попытаются вас развести на что-нибудь якобы «приятное».

Прикидываясь менеджерами банков или сотрудниками службы безопасности, мошенники могут как предлагать услуги, так и наводить панику относительно «опасных действий» с вашими счетами, которые вот прямо сейчас нужно предотвратить. Также могут неотличимо от реальных банковских работников предлагать какие-либо выгодные услуги: вклад с повышенным процентом, выгодный кредит, карту с кэшбэком или что-либо ещё. После согласия на оформление или проверку – мошенник будет пытаться получить код доступа или к банковскому приложению, или к госуслугам. На случай категорического отказа также может предложить оформить заявление об отказе и попытаться уже таким образом выведать код доступа от госуслуг.

Бесплатный сыр известно где

Звонок «из суда» – достаточно редкий способ обмана, направленный на тех, кто участвует или недавно участвовал в судебных заседаниях. Мошенники берут данные из картотеки суда и пытаются их соотнести с имеющимися базами. Стороне процесса звонят и начинают что-нибудь предъявлять: неявку в суд, требование получить извещение...

Объектом воздействия мошенников нередко становятся и дети. Как только ребёнок получает условно-бесконтрольный доступ в сеть Интернет – он может стать лакомым кусочком для мошенников. Основная масса атак через детей нацелена на доступ к счетам родителей. Детские карты с парой сотен на обеды жуликам уж точно не нужны. Поводом различные организации, но у мошенников возможны несколько вариантов: начиная от вредоносного программного обеспечения, заканчивая классикой жанра с выяснением информации от жертвы.

Не попадитесь на бесплатные плюшки – компенсации, пособия, доплаты. Достаточно старый, но эпизодически встречающийся способ обмана, когда жертве обещают выплаты за дела давно минувших дней. Это могут быть не только варианты с доплатой за вредные условия и прочее, но и, например, компенсации за вклад времён СССР или специальные надбавки к пенсии. Так же могут фигурировать различные пособия.

В поисках дополнительного заработка людям нередко попадают в неприятные ситуации, оставив заявку не там где надо. Вежливый менеджер тут же поможет с регистрацией, предоставит доступ к «закрытому сайту» или приложению, убедит вложить денежку и даже покажет прибыль. Возможно, дав копеечку в успокоение. А далее... далее всё плохо.

Звонок из ГИБДД, особенно в позднее или слишком раннее время, может выбить из колеи кого угодно. На это и делают расчёт мошенники, вешая лапшу на уши про то ли угнанный, то ли попавший в ДТП ваш автомобиль.

–Займи денег, кинь пару тысяч до получки, надо срочно! – даже голосом друга может прилететь вот такое сообщение. А уж текстовых в социальных сетях великое множество. При этом вариантов развития событий несколько. Либо вы просто лишитесь денег, либо потом может позвонить «страшный следователь» с обвинениями, что вы перевели деньги «куда не надо» и начать красивый прессинг. Где-то рядом находятся и те, кто выпрашивает «голоса» за родственников/детей, участвующих во всевозможных конкурсах. Не ведитесь!

Если на какие-то ситуации вокруг банков, счетов, уголовных дел ещё срабатывает триггер осторожности, то вот на «бытовуху» люди ведутся. Вот на все эти типа «флюорографии», «обновления СНИЛС», «счётчиков» и другие простые и не выглядящие финансово угрожающими ситуации. А вот уже после появится и «следователь», и «безопасный счёт».

ПОМНИТЕ, что код от госуслуг НИКОМУ нельзя сообщать!

Мотайте на ус

«Нагрели» при покупке

В дежурную часть полиции Троицка обратился 25-летний гражданин Республики Казахстан с заявлением о мошенничестве.

Мужчина, работающий специалистом по ремонту дорожно-строительной техники и занимавшийся в данный момент восстановлением фрезерного барабана, столкнулся с необходимостью приобретения большого количества резцов. Для поиска необходимых запчастей он использовал один из популярных онлайн-сервисов объявлений, разместив соответствующее объявление со спецификациями требуемых резцов, указав их размеры, материал и необходимое количество.

На следующий день ему поступил звонок от неизвестного мужчины, который предложил партию из 45 коробок резцов, идеально подходящих под описание, по цене 16 000 рублей за коробку. Общая сумма сделки составляла 720 000 рублей. Продавец утверждал, что весь товар находится на складе в Краснодаре и готов к немедленной отправке. В качестве условия сделки он потребовал предоплаты в полном объёме.

Заявитель, доверился обещаниям неизвестного и перевел на указанный им счёт 725 000 рублей, включая комиссию платёжной системы в размере пяти тысяч рублей.

Однако вместо ожидаемой доставки резцов заявитель столкнулся с игнорированием со стороны продавца. Все попытки связаться с ним по телефону и через онлайн-платформу оказались безрезультатными.

Возбуждено уголовное дело по статье «Мошенничество».

Подарила два миллиона

Такую сумму преступникам перевела 46-летняя жительница соседнего Озёрска.

В полиции она рассказала, что сначала ей позвонила девушка, представившаяся сотрудником оператора сотовой связи, и предложила закрыть абонентский номер, так как им якобы мало пользуются. Озерчанка ответила, что планирует оставить его, но всё равно назвала пришедшие в смс коды от портала госуслуг.

Спустя несколько минут с ней в мессенджере связался лжесотрудник финмониторинга и сообщил, что до этого звонили мошенники и получили доступ в личный кабинет, а теперь оформляют на её имя кредиты.

Чтобы у третьих лиц не получилось осуществить задуманное, телефонный собеседник убедил озерчанку взять кредиты в разных банках, затем скачать приложение по бесконтактным платежам, привязать к нему специально подготовленный счёт, затем внести полученные деньги и личные накопления через банкомат. После всех действий женщина лишилась 1,8 миллиона рублей, из которых только 160 тысяч являются личными накоплениями.

Следственным отделом УМВД России по ЗАТО г. Озёрск возбуждено уголовное дело по статье «Мошенничество».

Полицейским потерпевшая пояснила, что знала о подобных схемах мошенничества, но растерялась из-за страха финансовых потерь.

Сотрудники полиции напоминают, что не стоит разговаривать в мессенджере с неизвестными. Пользуйтесь приложениями, которые уже установлены на вашем телефоне, и помните, что ни в коем случае ни под каким предлогом не следует переводить куда-либо деньги, даже при обещании их защиты или возврата.

