Мошеннические схемы
в отношении граждан

Звонки от мошенников

Оповещение о попавшем в беду родственнике и просьба о помощи

Звонят обычно среди ночи. Полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками, друзьями. Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счет мобильника.

Перевод денег на «безопасный» счет

Звонит «менеджер банка» и сообщает, что ваш счет, на котором лежат деньги, кто-то пытается взломать. Чтобы сохранить средства, нужно срочно перевести их на безопасный счет. Если вы не поверите и положите трубку, спустя несколько минут поступит следующий звонок — якобы из полиции, ФСБ или Центробанка. Новый собеседник сообщает, что только что вы могли стать жертвой мошенников, ведь первый звонок был именно от них. Теперь от вас требуется одно — зайти в личный кабинет интернет-банка или в мобильное приложение, проверить, все ли деньги на месте, и перевести их на другой счет.

Цель мошенников — запутать вас и сделать все, чтобы вы сообщили логин и пароль от учетной записи и назвали секретный одноразовый код из СМС. Под прессингом многие перестают понимать, что происходит, и просто следуют инструкциям. После этого мошенники списывают деньги со счета. Вернуть их очень сложно.

Обвинение в противозаконных действиях

Звонят якобы из полиции и обвиняют, что вы переводите деньги за границу или спонсируете террористов. Естественное желание в такой ситуации — оправдаться и объяснить, что это какая-то ошибка. Но преступники продолжают давить. Если вы кладете трубку, то они перезванивают с других номеров и пытаются убедить, что ситуация крайне серьезная. По словам мошенников, сообщать кому-то о случившемся нельзя: за разглашение секретной информации предусмотрено наказание. Мошенники настаивают, чтобы вы отменили якобы проведенную транзакцию. Для этого нужно сообщить одноразовый пароль из СМС. После этого они получают доступ к счету и списывают деньги.

Звонок по видеосвязи для идентификации «клиентов банка» по биометрии

Мошенник создает в мессенджере фейковый аккаунт, якобы принадлежащий банку. С этого профиля он делает первый звонок, представляясь сотрудником банка, и спрашивает человека, обновлял ли тот мобильное приложение в последнее время.

Если ответ отрицательный, «работник» сообщает, что сейчас позвонит другой специалист банка, который поможет обновить приложение.

Затем мошенник звонит с другого аккаунта или в другом мессенджере, где есть функция трансляции экрана во время видеозвонка. Он объясняет, что звонит по видеосвязи для идентификации клиента по биометрии. Далее просит включить режим демонстрации экрана. По словам мошенника, благодаря этому подключается некая «роботизированная система для диагностики счета». На самом деле трансляция экрана позволяет злоумышленнику увидеть номера карт, суммы на счетах, коды в СМС от банка.

Звонок с требованием заменить полис ОМС

Мошенники представляются сотрудниками страховых медицинских организаций или территориальных фондов ОМС, специалистами департаментов или министерств здравоохранения. Пытаются убедить людей, что срок их медицинского полиса истек. Для продления необходимо скачать специальное приложение Минздрава или перейти по присланной ссылке, иначе будет невозможно получать бесплатную медпомощь. Затем просят назвать код из СМС от портала госуслуг.

Предлагаемое злоумышленниками приложение или ссылка на самом деле является программой, позволяющей получить доступ к устройству и списать средства.

Звонок из «Пенсионного фонда»

Как правило, мошенники звонят людям преклонного возраста и сообщают о необходимости скорректировать начисление пенсии в связи с ошибкой данных. Предлагают приехать в центральный офис пенсионного фонда, предварительно записавшись на конкретную дату и время. Запись якобы производится с помощью электронной очереди на госуслугах. Когда потенциальной жертве приходит СМС, мошенники просят назвать цифры из сообщения. Если человек их сообщает, злоумышленники получают доступ к его личному кабинету.

От имени жертвы мошенники регистрируются на сайтах микрофинансовых организаций через функцию «Войти с помощью госуслуг», оформляют кредиты, быстро обналичивают деньги, а жертве достаются лишь долговые обязательства.

Звонок представителя оператора сотовой связи о продлении истекающего договора

Мошенники выступают в качестве представителя оператора сотовой связи и предлагают «продлить истекающий договор на номер телефона». В начале разговора спрашивают, намеревается ли клиент его продлевать. При этом «засыпают» технической терминологией и мелкими деталями, чтобы усыпить бдительность. К примеру, могут спросить, где было бы удобнее забрать договор.

Далее на номер клиента приходит СМС с кодом, чтобы «подтвердить системе, что пользовательское соглашение продлено на новый срок». А мошенники направляют человеку ссылку якобы для дистанционного подписания, где и нужно ввести пришедший код. По этой ссылке злоумышленники получают доступ в кабинет жертвы на госуслугах. Также просят внести небольшую сумму на счет телефона — рублей 30 с банковской карты. После чего следует хищение всех средств со счета.

Помните, в договорах с сотовыми операторами срока пользования номером нет.

Истек или заканчивается срок сим-карты

Абоненту сотовой связи поступает звонок от «представителя оператора», который сообщает что у сим-карты заканчивается или уже истек срок действия. Для продления просят назвать код из СМС. В противном случае карта заблокируется, номер отберут и восстановить его не получится.

Мошенники вызывают доверие жертвы, называя ее паспортные данные, перечисляя, какие услуги подключены к номеру телефона, обещая скидки на дальнейшую абонентскую плату по тарифу. Затем делают переадресацию звонков и СМС на другой номер или виртуальный дубликат сим-карты. Дальше они могут проникнуть в онлайн-банк жертвы, почту, мессенджеры, соцсети и даже на портал госуслуг.

Мошеннические схемы
в отношении граждан

«АКТИОН» Образование

Сообщения и другие уловки

Просьба обновить электронный журнал или профиль на платформе «Сферум»

Просьба обновить электронный журнал или профиль на платформе «Сферум»

Аферисты от лица «школьной администрации» звонят родителям и просят предупредить ребенка, что ему будут звонить из «школы». Объясняют это необходимостью подтвердить «продолжение обучения во втором полугодии». Затем убеждают ребенка сообщить номер из СМС. Код необходим, чтобы получить доступ к аккаунту на портале госуслуг. С его помощью мошенники могут направить заявки на получение онлайн-микрозаймов и кредитов.

Мошенники используют данные настоящих работников школ, дипфейк-технологии и подменные номера.

В «Сферуме» сообщили, что данные на платформе обновляют автоматически на устройстве пользователя без участия третьих лиц. Для этого не используют коды из СМС, в том числе от госуслуг. Все коммуникации по учебе также ведутся исключительно в «Сферуме», где все пользователи верифицированы.

Имитация голоса родных в аудиосообщениях

Преступники взламывают аккаунты мессенджеров с помощью фейковых голосов. Затем скачивают сохраненные голосовые сообщения и создают новые с нужным контекстом. С помощью нейросетей мошенники генерируют голосовые обращения на основе аудиосообщений владельцев аккаунта.

Аудиосообщение с просьбой одолжить крупную сумму денег отправляют в личные переписки, а также во все чаты, где состоит хозяин украденного аккаунта. Туда же направляется фото банковской карты с именем и фамилией.

Телефонные вирусы

Жертве приходит сообщение о письме. Прочитать его можно, пройдя по ссылке. После этого в смартфон внедряется вирус, и мошенники получают полный контроль над телефоном.

Фишинг через школьный чат

Мошенники взламывают аккаунт одного родителя или учителя, чтобы получить доступ к списку контактов в классном чате. Иногда просто добавляются в чат под видом родителя новенького ученика или педагога. Либо пишут с поддельного профиля директора.

Легенда может быть любая — сбор денег на экскурсию или мероприятие, просьба пройти опрос или заполнить какую-нибудь форму на субсидию. По факту просят прислать деньги на свою карту или кидают фишинговую страницу. Если человек кликнет по ней, под угрозой окажутся его персональные данные, а гаджет может пострадать от вируса.

Обычно эта схема рассчитана на родителей первоклассников, которые еще не успели хорошо познакомиться друг с другом и учителем. Когда связи уже налажены, обман раскрывается довольно быстро. Но вероятность, что кто-то успеет перевести деньги мошенникам или открыть опасную ссылку, все же остается.

Фишинговые письма

Мошенники рассылают по электронной почте письма от имени банка. В письме содержится информация финансового характера. К примеру, что за открытие кредита с вас удержана комиссия или, наоборот, вам начислены дополнительные проценты по вкладу. Для достоверности указывают конкретные цифры – «комиссия за обслуживание кредита составила 8 247 рублей».

Даже если у человека нет никакого кредита или вклада, в большинстве случаев хочется разобраться, в чем дело. Мошенники уверены, что в поисках ответа жертва перейдет по ссылке, размещенной в письме. Но ссылка ведет не на настоящий, а на поддельный (фишинговый) сайт. Сложность в том, что на первый взгляд он практически не отличается от подлинного: то же оформление, расположение разделов, те же цвета и шрифты. В специальной форме потребуется ввести логин и пароль от личного кабинета. После этого преступники считают информацию и получат доступ к финансам.

Сообщение от «руководителя»

Работнику приходит сообщение от «руководителя», который обращается по имени и предупреждает о звонке из контролирующей инстанции. Руководитель настоятельно рекомендует следовать дальнейшим указаниям вышестоящего ведомства. Затем поступает звонок с неизвестного номера, где просят передать конфиденциальную информацию и осуществить финансовые операции.

Позднее становится известно, что руководитель ничего не писал, номер был поддельным, а деньги со счета исчезли.

Похищение денег через неиспользуемые номера телефонов

Пользователи могут менять сотовых операторов и подключать новые сим-карты. При этом старый номер остается привязан к аккаунту: на госуслугах, в интернет-банке или в соцсетях. Преступники сверяют номера, которые есть в открытой продаже, с теми, которые привязаны к каким-либо личным кабинетам. Затем покупают у сотовых операторов те номера, которые давно не используются владельцами, но раньше были привязаны к какому-то цифровому сервису.

С помощью сим-карт злоумышленники входят в личный кабинет банка, госуслуг или другого онлайн-сервиса, ведь на сим-карту приходит одноразовый пароль для входа. Даже если на счете нет денег, мошенники все равно смогут совершить преступление — например, оформить кредит.

Оформление кредитов и микрозаймов через финансовые маркетплейсы

Злоумышленники оформляют заявки на кредиты и микрозаймы на граждан через финансовые маркетплейсы, например «Банки.ру». Доступ к оформлению получают благодаря сотовым номерам жертв.

Изначально злоумышленник, уже имея некоторые важные сведения о жертве, по телефону говорит о поступившем на ее имя письме в МФЦ. Для убедительности называет реальный адрес центра. После этого предлагает направить письмо на почту жертвы по месту ее прописки, а затем сообщает, что через СМС придет номер отправления — на самом деле это код для подтверждения регистрации на «Банки.ру». После получения кода злоумышленник может подать заявку на кредит или микрозайм, общаясь с банком или микрофинансовой организацией от имени жертвы. Для подтверждения личности он, вероятно, будет использовать ранее «утекшие» персданные, включая данные паспорта, номер телефона, электронную почту.

Когда жертва изначально получает подобный телефонный звонок, то может не заподоз-рить мошенничества — преступники пользуются приемами, вызывающими доверие. К примеру, мошенник может знать о ваших родственниках, месте жительства и др.