Обзор наиболее распространенных схем мошенничества, в том числе по телефону

1. Махинации со счетами мобильных телефонов.

Самый распространенный вариант такого мошенничества — сообщение или звонок об ошибочном переводе денег на счет мобильного телефона и просьба вернуть их владельцу. Могут быть даже угрозы обращения в полицию или оператору с требованием блокировки телефона.

2. Сообщения о попавшем в беду родственнике и просьбы о помощи.

Панический звонок о попавшем в беду родственнике обычно случается среди ночи, полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками или просто друзьями. Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счет мобильника.

3. Сообщения о выигрыше в лотерею.

Отличная новость сопровождается требованием перевода на покрытие технических издержек самой лотереи. Здесь расчет на незнание законодательства Российской Федерации, согласно которому все расходы организаторов ложатся на них самих.

4. Телефонные вирусы.

Жертве приходит сообщение о том, что ей пришло сообщение в некий мессенджер, и его можно получить, пройдя по ссылке. После чего в смартфон внедряется вирус, получающий полный контроль над телефоном.

5. Перевод денег на «безопасный» счет.

Ситуация: вам звонит неизвестный человек и представляется менеджером банка. Собеседник сообщает, что ваш счет, на котором лежат деньги, кто-то пытается взломать. Чтобы сохранить средства, нужно срочно перевести их на безопасный счет. Наверняка вы не поверите и положите трубку. Но телефонные мошенники готовы к такому повороту событий. К делу подключаются сообщники. Спустя несколько минут после первого звонка раздается следующий, теперь уже якобы из полиции, ФСБ или Центробанка.

Новый собеседник сообщает, что вы только что чуть не стали жертвой мошенников, ведь первый звонок был именно от преступников. 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-сообщения. Преступники могут «обрабатывать» жертву несколько часов, привлекать новых действующих лиц, угрожать или, наоборот, обещать спасти. Под прессингом многие перестают понимать, что происходит, и начинают просто следовать инструкциям по телефону. Несколько простых действий — и деньги списываются со счета. Вернуть их будет крайне сложно, ведь вы сами сообщили конфиденциальную информацию.

6. Обвинение в противозаконных действиях.

Особенность этой схемы мошенников в том, что вам могут позвонить якобы из полиции и сразу начать обвинять, 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. Злоумышленники настаивают, чтобы вы отменили якобы проведенную транзакцию. Для этого нужно сообщить одноразовый пароль из СМС-сообщения. Дальше мошенничество разворачивается по стандартному сценарию. Если жертва поверила, то преступники за несколько шагов получают доступ к счету и списывают деньги.

7. Фишинговые сайты.

Мошенники рассылают по электронной почте письма от имени банка. В письме содержится информация финансового характера. К примеру, вам могут сообщить, что за открытие кредита с вас удержана комиссия или, наоборот, вам начислены дополнительные проценты по вкладу. Для достоверности указывают конкретные цифры: к примеру, «комиссия за обслуживание кредита составила 8 247 рублей» или «по вкладу начислены дополнительные проценты в размере 24 512 рублей 25 копеек».

Даже если у вас нет никакого кредита или вклада, в большинстве случаев хочется разобраться, в чем дело. На это и расчет. Мошенники уверены, что в поисках ответа вы перейдете 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. От вас требуется одно — ввести в специальной форме логин и пароль от личного кабинета. Как только вы это сделаете, преступники считают информацию и получат доступ к финансам.

8. Сообщение от «руководителя».

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

Позднее становится известно, что ваш руководитель вам не писал и номер был поддельным.

9. Имитация голоса родных в аудиосообщениях.

На первом этапе преступники взламывают аккаунты мессенджеров с помощью фейковых голосов. Затем они скачивают сохраненные голосовые сообщения и создают новые сообщения с нужным контекстом.

Мошенники генерируют с помощью нейросетей 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.

10. Звонок по видеосвязи для идентификации «клиентов банка» по биометрии.

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

Если ответ отрицательный, «работник» сообщает, что необходимо подождать звонка от другого специалиста банка, который поможет обновить приложение.

Затем мошенник звонит с другого аккаунта или в другом мессенджере, где есть функция трансляции экрана во время видеозвонка.

Второй «сотрудник» 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-сообщениях от банка. Эта и другая информация помогает мошеннику заполучить доступ к личному кабинету клиента в приложении на своем устройстве и украсть его деньги.

11. Похищение денег через доверенные номера телефонов.

О каких номерах идет речь? Пользователи могут менять сотовых операторов и подключать новые сим-карты. Часто бывает, что старый номер остается привязан к какому-то аккаунту: на «Госуслугах», в интернет-банке или в соцсетях. Одни пользователи при подключении новой сим-карты переводят на нее все учетные записи. Другие оставляют все как есть: личный кабинет так и остается привязанным к старому номеру. На такие симки и охотятся мошенники в надежде получить доступ к персональным данным.

Как действуют мошенники. Взлом аккаунта выглядит следующим образом:

Преступники сверяют номера, которые есть в открытой продаже, с теми, которые привязаны к каким-либо личным кабинетам. Затем покупают у сотовых операторов те номера телефонов, которые давно не используются владельцами, но раньше были привязаны к какому-то цифровому сервису.

С помощью сим-карт злоумышленники пытаются взломать личный кабинет банка, «Госуслуг» или другого онлайн-сервиса. Если вы не меняли настройки, то аккаунт так и остается привязанным к старому контакту.

Войти в учетную запись не составляет труда: на телефон приходит одноразовый пароль для входа. Поэтому телефонный номер важно беречь: это не просто комбинация цифр для связи, а важный код доступа к личному кабинету, один из этапов авторизации. Получив доступ к личному кабинету, мошенник может совершить от вашего имени любые действия.

Даже если на счете нет денег, и вы давно не пользуетесь услугами этого банка, мошенники все равно смогут совершить преступление — например, оформить кредит. Бывает, что банк выдает кредит на имя клиента, который когда-то оставлял данные и в истории банка числится как подходящий под условия выдачи займа. Тем более что на рынке разрешены программы без подтверждения дохода, если клиент ранее уже предоставлял банку свои данные. Таким образом, вы можете узнать о наличии кредита только спустя несколько месяцев.

12. Звонки с требованием заменить полисы ОМС.

Мошенники представляются сотрудниками страховых медицинских организаций или территориальных фондов ОМС, специалистами департаментов или министерств здравоохранения и в ходе разговора пытаются убедить людей, что срок медицинского полиса их собеседников истек, а для его продления необходимо скачать специальное приложение Минздрава или перейти по присланной ссылке, иначе он не сможет получить бесплатную медпомощь, а затем просят назвать код из СМС-сообщений от портала госуслуг.

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

Основная задача преступников в такой ситуации — получить доступ к личным данным человека и его сбережениям.

Будьте бдительны! Игнорируйте такого рода информацию!

Не отвечайте на вопросы мошенников и прервите звонок. Не устанавливайте никакие приложения, не переходите по ссылкам, не сообщайте злоумышленникам никаких сведений о себе. Сообщите об инциденте в свою страховую медицинскую организацию или в единый контакт-центр своего территориального фонда ОМС.

Специалисты страховых медицинских организаций могут позвонить застрахованному с целью актуализировать данные полиса, однако они никогда не присылают СМС-сообщений с цифровыми кодами, не запрашивают персональные данные и не просят перевести куда-либо деньги.

13. Звонок из «Пенсионного фонда».

Звонки поступают в основном людям преклонного возраста. Как правило, мошенники звонят потенциальной жертве и сообщают о необходимости скорректировать начисление пенсии в связи с ошибкой данных. Человеку предлагается приехать в центральный офис пенсионного фонда, предварительно записавшись на конкретную дату и время. Запись якобы производится с помощью электронной очереди на «Госуслугах». Далее мошенники заходят на портал, потенциальной жертве приходит СМС-сообщение для подтверждения доступа, мошенники просят назвать цифры из сообщения. Если человек их сообщает – злоумышленники получают доступ к личному кабинету жертвы.

Дальше от имени жертвы производится регистрация на сайтах микрофинансовых организаций, используя функцию «Войти с помощью

госуслуг», оформляется кредит, полученные деньги быстро обналичиваются, а жертве достаются лишь долговые обязательства.

14. Звонок представителя оператора сотовой связи о продлении истекающего договора на номер телефона.

Жертве звонят якобы представители операторов сотовой связи и предлагают «продлить истекающий договор на номер телефона». В начале разговора мошенник сообщает, что у клиента якобы заканчивается договор на номер телефона, и спрашивает, намеревается ли он его продлевать. При этом пользователя «засыпают» технической терминологией и мелкими деталями, чтобы усыпить его бдительность. К примеру, у него могут спросить, где было бы удобнее забрать договор.

При утвердительном ответе «менеджер» уточняет, на какой период жертва хотела бы продлить договор, а далее на ее номер приходит СМС с кодом, который нужен чтобы «подтвердить системе, что пользовательское соглашение продлено на новый срок». В основной фазе схемы мошенник направляет человеку ссылку якобы для завершения дистанционного подписания пользовательского соглашения, где нужно ввести пришедший в СМС код.

В первую очередь стоит помнить, что в договорах с сотовыми операторами срока пользования номером нет. Также переходить по ссылке нельзя, так как с ее помощью злоумышленники могут получить доступ в кабинет жертвы на «Госуслугах». Помимо этого, мошенник может попросит внести через «офис» небольшую сумму на счет телефона, рублей 30, и, конечно, с банковской карты. А дальше последует хищение всех средств со счета.

Будьте бдительны и не верьте никаким звонкам и сообщениям о якобы закончившихся договорах с сотовыми операторами!

15. Звонок или сообщение, что истек или заканчивается срок SIM-карты.

Абоненту сотовой связи поступает звонок от якобы представителя оператора, который сообщает что у SIM-карты заканчивается срок действия или он уже истек. Для продления просят назвать код из СМС-сообщения. В противном случае карта заблокируется, номер отберут, и человек уже не сможет ничего восстановить.

Телефоны ценны для многих людей, номера не меняются годами, сформированный пул контактов — это нематериальный актив, важный для жизни. Мошенники в разных случаях пытались вызвать доверие жертвы, называя

их паспортные данные, перечисляя, какие услуги подключены к номеру телефона, обещая скидки на дальнейшую абонентскую плату по тарифу.

Затем мошенники делают переадресацию звонков и СМС-сообщений на другой номер или виртуальный дубликат SIM-карты. Дальше они могут проникнуть в онлайн-банк жертвы, почту, мессенджеры, соцсети и даже на портал госуслуг.

Цель мошенников — либо получить у человека код для входа в его личный кабинет мобильного оператора и установить переадресацию, либо убедить абонента подключить ее самостоятельно.

16. Звонок из банка с просьбой подтвердить оформление кредита.

Ситуация. Звонок из банка с просьбой подтвердить, что вы сейчас оформляете кредит, например на 550 000 рублей. При этом, вы ничего не оформляете в тот момент. Сотрудник банка сообщает, что если это не вы, значит мошенники пытаются взять кредит от вашего имени, поэтому срочно надо принять меры, и присылает вам ссылку на приложение, которое нужно скачать, чтобы защитить ваши данные и остановить мошенников. Жертве не дают подумать, начинают прессинговать о срочности и важности действий, уговаривают выполнять инструкции, чтобы как можно скорее разрулить ситуацию, и жертва скачивает приложение. Затем сотрудник банка просит назвать код из СМС-сообщения и еще какие-то данные, пароли и т.д. Потом сотрудник банка говорит, что, к сожалению, банк успел выдать вам кредит, но благодаря тому, что мы быстро спохватились, мошенникам еще не удалось получить доступ к деньгам. И чтобы точно защитить деньги, вы должны срочно снять их все в банкомате и перевести на безопасный счет в банке-партнере. Мол, так надежнее. А после этого можно будет закрыть тот кредит. Сотрудник говорит, чтобы вы шли к банкомату, а он перезвонит через полчаса. Вы бежит к банкомату, и снимаете все деньги. Сотрудник банка вам перезванивает и говорит, чтобы вы положили деньги в банкомате другого банка, подсказывает адрес куда ехать. Когда вы оказываетесь по нужному адресу, сотрудник банка вам перезванивает и диктует номер безопасного счета, куда нужно перечислить все деньги. Когда деньги поступают на счет мошенников, сотрудник банка сообщает, что теперь все в порядке, и чтобы вы ждали следующего звонка для закрытия кредита. Вы ждете следующего звонка от сотрудника банка, а когда он не выходит на связь обращаетесь в свой банк, и узнаете, что вы только, что оформили предодобренный кредит и сняли все деньги.

Мошенники использовали уловки социальной инженерии, чтобы вас обмануть и заставить выполнять их инструкции. Сначала собрали данные о вас:

ФИО, номер телефона и название банка, где вы обслуживаетесь. Эту информацию злоумышленники, скорее всего, получили в результате утечек персональных данных. Возможно, они также разузнали, что у вас есть предварительно одобренный кредит, и выяснили, на какую сумму. Или назвали размер кредита наугад.

Предодобренный кредит можно оформить удаленно, но для этого мошенникам надо было взломать онлайн-банк жертвы. Они убедили жертву скачать «защитное» приложение, которое на самом деле открыло мошенникам удаленный доступ к его личному кабинету на сайте банка.

Дело оставалось за малым: заставить жертву сообщать им коды для подтверждения операций с кредитом, а затем — убедить перевести все деньги на мошеннический «безопасный счет».

Пока жертва думает, что «спасает» свои деньги, злоумышленники оформляют от его имени кредит. Проблема в том, что фактически все происходит с согласия жертвы: вы сами сообщаете злоумышленникам секретные данные для подтверждения операций.

Когда банк перечислил жертве кредит, жертва снимает эти деньги и опять же сама перекладывает на счет преступников через банкомат. Скорее всего, таким образом преступники хотят «замести следы».

Если бы жертва сделала перевод аферистам прямо со своего счета, то банк легко узнал бы их реквизиты и занес их в черный список — в будущем перечисления им автоматически блокировались бы. А когда человек под диктовку вводит в банкомате номер счета обманщиков, то вряд ли сможет его запомнить и сообщить полиции.

Банки не возвращают деньги в тех случаях, когда люди добровольно переводят мошенникам деньги или передают им данные, которые открывают доступ к счетам.

В любом случае в такой ситуации надо писать заявление кредитору и подавать заявление в полицию. А пока идут разбирательства, придется платить по кредиту, чтобы не испортить кредитную историю.

Если вы получили тревожный звонок от «сотрудника банка», не спешите выполнять его инструкции. Положите трубку и перезвоните в банк сами, набрав номер, который указан на его официальном сайте или на обороте карты.

17. Оформление кредитов и микрозаймов мошенниками через финансовые маркетплейсы.

Злоумышленники оформляют заявки на кредиты и микрозаймы на граждан через финансовые маркетплейсы, например «Банки.ру», с помощью методов убеждения. Доступ к оформлению они 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 называется реальный адрес центра. После этого мошенник предлагает направить письмо на почту жертвы по месту ее прописки, а затем сообщает, что через СМС-сообщение ей придет номер отправления – на самом деле это код для подтверждения регистрации на «Банки.ру».

Один из последних шагов мошенника – регистрация на сайте финансовой платформы, где для нее нужен номер телефона и высылаемый по нему код подтверждения. После получения кода для входа на сайт злоумышленник может подать заявку на получение кредита или микрозайма. В дальнейшем он может общаться с банком или микрофинансовой организацией якобы от имени жертвы, от которой и подается заявление. Для подтверждения личности он, вероятно, будет использовать ранее утекшие в даркнете персональные данные, включая данные паспорта, уже имеющийся номер телефона и полученный социальной инженерией СМС-код подтверждения, и электронную почту.

Когда жертва изначально получает подобный телефонный звонок, она может не подозревать мошенничества, так как преступники пользуются приемами, создающими впечатление доверия. К примеру, мошенник может знать из даркнета о родственниках цели, о месте ее жительства и так далее.

Код из СМС сообщать никому нельзя!

Что делать, если мошенники оформили кредит.

Если вы стали жертвой преступников, действуйте следующим образом:

• Подайте заявление в полицию. Подробно опишите, что произошел взлом аккаунта. Перечислите все, что известно о кредите: когда его оформили, каким банком выдан, на какую сумму, под какой процент, на какой срок.

• Позвоните в банк, сообщите о взломе и объясните, что кредит оформили мошенники. Приложите справку из полиции. Она станет подтверждением, что вы действительно не виноваты и виновных уже ищут.

• Запросите в банке документы, подтверждающие выдачу кредита: заявку, договор, график погашения.

• Позвоните в контакт-центр банка и зарегистрируйте претензию. Опишите, как вы узнали о взломе аккаунта и выдаче кредита. Приложите выписки со всех счетов, принадлежащих вам: по ним будет видно, что деньги не поступали ни на один из счетов.

• Если банк не может помочь, обратитесь с претензией в ЦБ РФ. Возможно, придется разбираться через суд, чтобы вернуть деньги, украденные мошенниками. Сохраняйте все документы, которые могут подтвердить вашу непричастность.

• Для защиты от мошенничества регулярно проверяйте свою кредитную историю на предмет оформленных кредитов и непогашенных задолженностей. Процедуру проводят через БКИ — бюро кредитных историй. Два раза в год проверять финансовое досье можно бесплатно. За дополнительные проверки придется заплатить. Обратите внимание: банки могут отправлять информацию по клиентам в разные БКИ. Поэтому для достоверности заказывайте отчет сразу в нескольких бюро.