Мошеннические схемы

Убеждают взять кредит

Человеку звонит якобы сотрудник бюро кредитных историй и утверждает, что на него или его близких родственников мошенники пытаются оформить кредит. Через короткое время ему снова звонят и уже могут представляться сотрудниками службы безопасности банка, правоохранительных органов или Банка России. Звонящий подтверждает, что на имя гражданина или его близких неизвестные лица действительно оформляют кредит и, чтобы предотвратить его незаконное оформление, необходимо как можно скорее оформить «встречный» кредит самостоятельно онлайн или в офисе банка. Сумма кредита должна совпадать с той суммой, которую оформляют неизвестные лица по его паспортным данным. Для убедительности злоумышленники просят гражданина действовать оперативно и ни в коем случае не рассказывать про оформление кредита и его целях кому-либо, так как проводится секретная операция по вычислению жулика из числа сотрудников банка. Они убеждают жертву, что ее действия позволят раскрыть преступника, а кредитная история останется чистой. Во время разговора звонящие узнают, услугами каких банков пользуется жертва, и, чтобы войти в доверие, интересуются, не теряла ли она документы, удостоверяющие личность, и не передавала ли кому-либо свои паспортные данные.

Предложение пересчитать пенсию из-за неучтенного стажа

Злоумышленники звонят пожилым людям и представляются работниками Социального фонда России (СФР). Они сообщают, что размер текущей пенсии можно существенно увеличить, так как будто бы обнаружен неучтенный трудовой стаж. Тех, кто поверил аферистам, приглашают якобы на консультацию в Многофункциональный центр или отделение СФР для решения вопроса. Причем мошенники называют настоящие адреса центров или отделений, которые находятся в городе, где живет потенциальная жертва. Это усыпляет бдительность человека.

По сценарию злоумышленников, для записи на прием человек должен предоставить данные паспорта, СНИЛС, ИНН и назвать код из SMS -сообщения. На деле перечисленные документы и числовой код из сообщения нужны мошенникам для получения доступа к учетной записи человека на портале Госуслуги. Заполучив доступ к ней, они могут беспрепятственно оформить на жертву кредиты или займы.

Обман военнослужащих и их родных

Злоумышленники обновили свою популярную схему про «безопасный» счет. Теперь они начали использовать ее в отношении военнослужащих либо их близких родственников. Мошенники звонят или пишут своим потенциальным жертвам и сообщают, что единовременная выплата в размере 195 000 рублей, которая причитается военным в соответствии с указом Президента РФ, будет удержана из денежного довольствия.

Причина — дисциплинарное взыскание или нарушение при выполнении служебных обязанностей в зоне проведения специальной военной операции (СВО). Для большей убедительности злоумышленники направляют в мессенджер «копию выписки» якобы из приказа Департамента финансового обеспечения Минобороны России. По сценарию, придуманному мошенниками, военнослужащему или его родным, чтобы

избежать списания денег и сохранить средства, предлагают перевести все накопления с карты на «безопасный» счет, а затем средства обещают вернуть. Однако, получив обманным путем деньги жертвы, телефонные аферисты исчезают.

Кампания по сдаче налоговых деклараций

Схема построена на кампании по сдаче налоговых деклараций и представляет угрозу для большого числа людей и индивидуальных предпринимателей. Злоумышленники направляют на электронную почту письма, в которых выдают себя за сотрудников налоговой службы, с требованием представить декларацию по специальной ссылке. При переходе по ссылке потенциальную жертву просят ввести личные данные и реквизиты банковской карты (ее номер, имя и фамилию владельца карты, трехзначный код на оборотной стороне) якобы для идентификации налогоплательщика. На самом деле с помощью мошеннического ресурса злоумышленники собирают данные банковской карты для хищения денег у человека, а полученные персональные данные могут использовать для новых случаев обмана жертвы.

Хищение средств под предлогом обновления банкнот

Злоумышленники стали спекулировать на обновлении банкноты номиналом 5000 рублей. Мошенники звонят гражданам и сообщают, что необходимо проверить подлинность наличных денег, в том числе новых 5000 рублей. Для этого злоумышленники предлагают человеку установить на мобильном телефоне специальное приложение — «Банкноты Банка России». Однако они дают ссылку на фальшивое приложение, визуально похожее на официальное. После установки такого приложения мошенники получают удаленный доступ к телефону жертвы и, соответственно, к банковским приложениям и счетам. Таким образом, они похищают у человека деньги со всех счетов. Приложение «Банкноты Банка России» действительно существует, но оно содержит информацию об основных защитных признаках всех банкнот Банка России (где именно они расположены и как должны выглядеть) и не определяет подлинность купюр.

Кроме того, аферисты под видом работников социальных служб ходят по квартирам и убеждают жильцов обменивать старые банкноты номиналом 5000 рублей на новые. А на самом деле лжесотрудники подсовывают доверчивым людям фальшивые купюры. Жертвами чаще всего становятся пожилые люди.

Использования ложных аккаунтов руководителей в мессенджерах

Мошенники создают аккаунты в популярных мессенджерах от лица руководителей Банков. Страницы содержат их реальные данные (фамилия, имя, отчество, фото — эти сведения берутся из Интернета) и выглядят максимально достоверно. Используя фальшивые аккаунты якобы служащих Банков, злоумышленники отправляют сообщения руководителям или их заместителям различных крупных компаний или государственных органов. В письмах такие лжесотрудники просят помочь им, например, в задержании аферистов в кредитной организации и предупреждают о скором звонке уполномоченного сотрудника из профильного министерства. Они рекомендуют следовать инструкциям звонящего, а о факте разговора никому не рассказывать. После этого злоумышленники звонят потенциальной жертве и под различными предлогами пытаются получить доступ к банковским данным или убеждают добровольно перевести деньги на подконтрольные мошенникам счета.

Обещание выплаты наличными в Общественной приемной Банка России

Злоумышленники начали использовать новую схему обмана людей, построенную на уловке о «специальном» счете в Центробанке. Они, как и прежде, сообщают человеку, что неизвестные пытаются похитить деньги с его счета, а для спасения средств их надо перевести на «безопасный» счет в Центробанке. Но теперь, по новой легенде, аферисты внушают потенциальной жертве, что сбережения на «спецсчет» переводятся временно, на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в Общественной приемной Банка России в Москве. При этом злоумышленники пугают уголовной ответственностью за разглашение информации следствия. Мошенники действительно от имени потенциальной жертвы записывают человека на личный прием в Общественную приемную Банка России. Делают они это через сайт регулятора, указывая в качестве контактного номера телефон жертвы. Человеку приходит подтверждающее SMS-сообщение с короткого номера Банка России 300. Это позволяет киберпреступникам войти в доверие и убедить собеседника сделать перевод. Только в сентябре 2023 года в Банк России обратилось несколько десятков человек, пострадавших от такой схемы обмана. В некоторых случаях суммы хищения составляют десятки миллионов рублей.

Распространение вирусных шаблонов документов, для похищения средств компаний

Злоумышленники создают сайты, которые имитируют ресурсы государственных ведомств и популярных справочно-правовых систем, чтобы похитить средства компаний. Для эффективного продвижения страниц и привлечения большого числа потенциальных жертв они используют метод SEO-poisoning («отравление» поисковой выдачи). Другими словами, содержание фишинговых ресурсов представлено в таком виде, что в результате поиска мошеннические сайты предлагаются пользователям в числе первых. На них киберпреступники размещают зараженные вирусами шаблоны документов, которые часто ищут в Интернете секретари, бухгалтеры или сотрудники, занимающиеся финансовой, налоговой и другой отчетностью. После скачивания вредоносного документа на рабочем компьютере сотрудника запускается программа удаленного доступа. Она позволяет хакерам дистанционно изменять в договорах с подрядчиками и поставщиками банковские реквизиты получателя средств на свои. Обнаружить вирусное программное обеспечение удается, как правило, не сразу. В некоторых случаях блокируется доступ к рабочим компьютерам, а за разблокировку хакеры вымогают деньги.

Мошенники представляются работодателями

Злоумышленники рассылают по электронной почте, через SMS или мессенджеры сообщения с привлекательными условиями работы: высокой оплатой труда, неполным рабочим днем, легкими задачами. Зачастую это работа на маркетплейсах (продажа товаров и услуг через Интернет). Для уточнения деталей человеку предлагают перейти по ссылке, которая ведет в популярные мессенджеры. Там с потенциальной жертвой вступают в переписку «менеджеры по подбору персонала». Они могут запросить у клиента данные банковской карты, номер мобильного телефона. Затем якобы для регистрации и активации аккаунта для работы на маркетплейсе требуется внести вступительный взнос — например, в размере 500 рублей. Но на самом деле эти деньги оседают в карманах мошенников, а данные банковской карты и номер телефона используются ими для попытки взлома личного кабинета человека на сайте банка и кражи средств с его счета.

Якобы утечка персональных данных

Злоумышленники звонят гражданам и представляются сотрудниками правоохранительных органов. Вначале лжеполицейский сообщает человеку, что по поручению Центрального банка расследует дело о массовой утечке банковских данных, в числе которых могут быть и сведения о гражданине. Под таким предлогом и для возможного привлечения собеседника в качестве пострадавшего мошенник предлагает ему сверить банковские сведения с базой украденных данных. Далее злоумышленник спрашивает у человека, в каком банке он обслуживается, просит данные карты, в том числе трехзначный код на ее оборотной стороне. Чтобы убедить потенциальную жертву в правдоподобности истории, мошенник может направить в мессенджер или на электронную почту фото поддельного документа о проведении оперативно-розыскных мероприятий.

Лжесотрудники банка

Распространённая мошенническая схема, при которой злоумышленники представляются сотрудниками Центрального банка. Вначале мошенники звонят человеку и сообщают о сомнительных операциях, якобы совершаемых по счету или карте, после направляют ему в мессенджер или на электронную почту поддельное удостоверение сотрудника Банка России с логотипом и печатью. Такие документы могут содержать фамилии реальных работников — эти сведения злоумышленники могут брать с сайта регулятора. Высылая фальшивое удостоверение, они надеются убедить человека в правдоподобности своих недобросовестных действий, чтобы в дальнейшем лишить его денег или оформить на него кредит.

Сотрудник оператора мобильной связи

Злоумышленники звонят гражданам под видом сотрудников службы поддержки оператора сотовой связи и сообщают, что номер абонента скоро перестанет действовать. Чтобы избежать отключения номера, человеку предлагают набрать на мобильном телефоне определенную комбинацию цифр. Однако в результате абонент подключает переадресацию звонков и текстовых сообщений, в том числе с SMS-кодами от банка, на номера мошенников. Это позволяет им получить доступ к дистанционному управлению банковским счетом и похитить деньги. Кроме того, мошенники могут сообщить, что гражданину необходимо переоформить договор об оказании услуг связи, поменять тарифный план на более выгодный, отключить платную услугу. Иногда злоумышленники сообщают, что поступила заявка о смене мобильного оператора с сохранением номера. Независимо от причины звонка цель мошенников — либо получить у человека код для входа в его личный кабинет мобильного оператора и установить переадресацию, либо убедить абонента подключить ее самостоятельно.

Обмен кешбэка на рубли

Злоумышленники обзванивают граждан под видом сотрудников банков и сообщают, что накопленный за покупки кешбэк и другие бонусные баллы можно обменять на рубли. Для этого мошенники запрашивают у человека банковские данные и SMS-код, полученный от банка, якобы для подтверждения операции и оплаты комиссии за услугу. Однако на самом деле злоумышленники, заполучив эти сведения, совершают кражу денег со счета.

Помощь в компенсации похищенных денег

Чтобы якобы вернуть пострадавшему похищенные у него деньги, мошенники создают специальные сайты, ссылки на которые направляют по электронной почте, через смс или мессенджеры. Иногда они звонят с предложением оформить компенсацию за похищенные средства. Доверчивых граждан злоумышленники просят заполнить форму с личными и финансовыми данными, чтобы якобы проверить полагающуюся сумму возврата и оформить его. А затем, получив эти данные, похищают у человека деньги.

Проверка счетов на предмет утечек

Злоумышленники предлагают гражданам проверить, не попали ли данные счета или карты в руки третьих лиц. Для этого человеку присылают по электронной почте или иным способом ссылку на сайт, якобы проверяющий утечку банковских сведений. Как только жертва введет на этом сайте свои банковские данные, они оказываются у настоящих мошенников. После этого злоумышленники могут похитить деньги держателя карты или использовать его данные в противоправных целях.

Перевод денег на специальный счет Центрального банка

Злоумышленники часто звонят человеку с сообщением о том, что неизвестные лица пытаются похитить деньги с его счета и для сохранности средства нужно перевести на «специальный» («безопасный») счет в Центробанке. На самом деле счет, реквизиты которого называют злоумышленники, принадлежит им. Мошенники используют в схеме упоминание регулятора, чтобы усыпить бдительность потенциальной жертвы. Иногда, чтобы войти в доверие к человеку, звонящие могут напоминать о правилах безопасности — например, рекомендовать никогда не раскрывать финансовые данные.

Замена полисов ОМС

Мошенническая схема, при которой злоумышленники представляются сотрудниками поликлиники и говорят о необходимости замены полиса ОМС «обязательного медицинского страхования». Причем не просят назвать никаких кодов из SMS, а просят скачать приложение Министерства здравоохранения и заполнить необходимые данные. В результате закачивают в телефон вирусное приложение (троян), который дает возможность украсть ваши личные данные банковских приложений. Будьте внимательны – у всех полисы медицинского страхования бессрочны!

Запись на диспансеризацию

Злоумышленники обзванивают граждан под видом сотрудников поликлиники и предлагают записаться на флюорографию и диспансеризацию. Подбирают дату и время, а затем просят подтвердить запись кодом из SMS, SMS приходит с портала государственных услуг для смены входа в учетную запись, в результате аккаунт портала государственных услуг попадает в полное распоряжение злоумышленников.

Полезные правила безопасности

- Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или SMS-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.
- Если с неизвестного номера звонит сотрудник Центробанка, правоохранительных органов, государственной организации или банка с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Если подозреваете, что вам звонит мошенник, позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.
- Не совершайте каких-либо действий по счету, если вам звонят из Центробанка с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.
- По возможности установите антивирус на все устройства и обновляйте его.
- Совершайте покупки в Интернете только на проверенных сайтах. Заведите специальную карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).
- Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.