МБДОУ «ДЕТСКИЙ САД № 1 «КОЛОКОЛЬЧИК»

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСКИМ ПРАКТИКАМ

Для хищения денег у граждан злоумышленники используют изощренные сценарии обмана, которые регулярно совершенствуют. Схемы финансового мошенничества выглядят очень правдоподобно. Преступники обычно используют обсуждаемые новости или события, запугивают или, наоборот, обещают внезапную выгоду. Банк России выявляет такие схемы и публикует их вместе с рекомендациями, как защититься от мошенников.

МОШЕННИЧЕСКАЯ СХЕМА № 1

Злоумышленники зазывают людей в несуществующую инвестиционную программу цифрового рубля

Признаки мошенничества

Мошенники призывают людей инвестировать в цифровые рубли и получать от этих вложений пассивный доход.

Они создают сайты в фирменных цветах и с логотипом цифрового рубля. Такие интернет - ресурсы аферисты называют инвестиционной программой цифрового рубля Банка России. На сайте посетителя приветствует «личный менеджер», который уговаривает внести сумму на «депозит».

Человека агитируют как можно быстрее присоединиться к якобы существующей программе, пока «порог входа низкий», потому что потом стартовая сумма будет значительно увеличена. Потенциальной жертве предлагают ответить на несколько вопросов и оставить контактные данные. Далее цель «личного менеджера» – заставить человека внести как можно больше денег на подставной площадке.

Что предпринять?

Будьте бдительны: инвестиционных программ цифрового рубля не существует!

Доверяйте только официальным источникам. Вся информация о цифровом рубле опубликована на сайте Банка России.

О запуске цифрового рубля в массовое обращение Банк России сообщит дополнительно.

Цифровой рубль Банка России — это цифровая форма национальной валюты. Она вводится как средство для платежей и переводов. Сейчас операции с цифровыми рублями доступны только участникам пилота — это ограниченный круг клиентов банков, подключенных к платформе цифрового рубля.

МОШЕННИЧЕСКАЯ СХЕМА № 2

Лжесотрудники Банка России предлагают закрыть «международный счет»

Признаки мошенничества

Мошенники стали применять новую схему обмана с упоминанием Банка России. Они направляют потенциальной жертве электронное письмо с логотипом регулятора, в котором указывают фамилию, имя и отчество человека.

В письме злоумышленники сообщают, что у человека якобы есть действующая учетная запись в европейской финансовой организации. Они требуют закрыть «международный счет» с крупной суммой денег и предлагают вывести их с сохранением процентного дохода. Мошенники утверждают, что для этого нужно задействовать свой российский банковский счет, на котором больше всего денег. Чтобы получить более подробные инструкции, человеку следует ответить на письмо или связаться с его отправителями через мессенджеры. В некоторых письмах прилагается фишинговая ссылка на сайт, где предлагается ввести личные данные и банковские реквизиты якобы для идентификации и закрытия счета.

Отказ от закрытия счета, по словам мошенников, грозит значительным штрафом, арестом имущества или принудительным взысканием с заработной платы. В дальнейшем мошенники могут использовать эти сведения для хищения денег или оформления кредитов и займов.

Кроме того, ссылка может содержать вредоносное программное обеспечение, которое автоматически устанавливается на устройство пользователя и предоставляет злоумышленникам удаленный доступ к банковским приложениям.

Что предпринять?

Будьте бдительны и не реагируйте на такие письма: не переходите по ссылкам в сообщении, не предоставляйте личную и финансовую информацию.

При возникновении любых сомнений самостоятельно позвоните в свой банк по номеру, указанному на оборотной стороне карты или на сайте кредитной организации.

По возможности установите антивирусную программу на свои устройства и регулярно обновляйте ее.

Настоящие сотрудники Банка России не звонят людям и не направляют им копии каких-либо документов, не запрашивают персональные и банковские сведения, не предлагают совершить какие-либо операции со счетом.

МОШЕННИЧЕСКАЯ СХЕМА № 3

Мошенники снимают деньги в банкоматах без пластиковых карт людей

Признаки мошенничества

Злоумышленники звонят гражданам, в том числе через мессенджеры, и утверждают, что неизвестные лица пытаются похитить деньги с их счета. Чтобы предотвратить потерю сбережений, мошенники убеждают человека немедленно установить на своем телефоне якобы мобильное приложение Центрального банка (варианты названий могут быть разными). Причем, пока оно устанавливается, запрещают пользоваться устройством.

После этого злоумышленники просят жертву запустить установленное приложение, поднести свою карту к мобильному телефону и ввести подтверждающий СМС-код от банка якобы для авторизации в приложении регулятора и спасения денег на счете. На самом деле загруженная на смартфоне человека программа вредоносная. Она позволяет создать на телефоне мошенников виртуальный образ банковской карты жертвы. В результате злоумышленники с использованием этого виртуального образа могут снимать деньги в банкоматах, поддерживающих бесконтактную технологию: вместо банковской карты они прикладывают свой смартфон.

Что предпринять?

Не скачивайте по просьбе незнакомых лиц никакие мобильные приложения или программы, а также не совершайте по их требованию никаких действий в банковских и иных приложениях.

При возникновении любых сомнений относительно сохранности денег на банковском счете сразу же звоните в свой банк по номеру, указанному на его официальном сайте или оборотной стороне банковской карты.

Не сообщайте посторонним людям личные и финансовые данные, под каким бы предлогом или каким бы способом их ни пытались узнать.

МОШЕННИЧЕСКАЯ СХЕМА № 4

Мошенники обманывают людей под предлогом трудоустройства или стажировки

Признаки мошенничества

Злоумышленники стали чаще размещать в Интернете объявления о привлекательных вакансиях в крупных компаниях, государственных организациях, Банке России. У откликнувшихся соискателей они выманивают персональную и банковскую информацию с помощью анкетирования, а затем приглашают людей на собеседование, чтобы наладить контакт и расположить к себе. Под разными предлогами эти лжеработодатели объясняют, что встретиться лично в офисе невозможно, и проводят собеседование дистанционно. Они втираются в доверие, задавая вопросы о профессиональных навыках кандидата, рассказывают о компании и должностных инструкциях. Однако в итоге мошенники просят кандидата сделать денежные переводы, которые якобы необходимы для подписания трудового договора. Аргументы приводятся разные в зависимости от предлагаемой должности и специфики деятельности организации: оплатить предварительное обучение, медосмотр, внести взносы за спецодежду, подтвердить актуальность банковской карты для зачисления будущей зарплаты, сделать переводы для задержания киберпреступников и другого. Кроме того, в некоторых случаях злоумышленники просят установить на телефон приложение, которое в действительности является вредоносным.

Что предпринять?

Если в процессе обсуждения трудоустройства или стажировки вас просят за что-то заплатить – откажитесь от такого предложения. Помните, что настоящие работодатели не собирают банковские данные, не запрашивают финансовых документов, не просят кандидатов финансово участвовать в каких-либо операциях. Менеджеры по кадрам для переписки с соискателями используют корпоративную электронную почту (после символа @ указывается домен сайта компании). Информацию о вакансиях и стажировках проверяйте на официальном сайте компании или специализированных ресурсах по поиску персонала. Если это Банк России – то в специальном разделе на сайте регулятора.

МОШЕННИЧЕСКАЯ СХЕМА № 6

Мошенники обманывают людей с помощью дипфейков

Признаки мошенничества

В России злоумышленники для хищения денег стали чаще использовать новый инструмент обмана — дипфейк-технологии. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети. В коротком фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. В некоторых случаях мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той сферы деятельности, в которой трудится их потенциальная жертва.

Что предпринять?

Проявляйте осторожность при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи — его аккаунт могли взломать злоумышленники. Иногда для рассылки таких сообщений мошенники создают поддельные страницы с именем и фото человека. Не спешите переводить деньги! Обязательно сначала позвоните тому, от чьего имени поступило сообщение, и перепроверьте информацию. Распознать дипфейк можно по неестественной монотонной речи собеседника, дефектам звука и видео, несвойственной мимике. Если возможности позвонить и убедиться, что человеку действительно нужна помощь, нет, задайте в сообщении личный вопрос, ответ на который знает только ваш знакомый.

МОШЕННИЧЕСКАЯ СХЕМА № 7

Мошенники предлагают пересчитать пенсию из-за неучтенного стажа работы

Признаки мошенничества

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 СМС-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.

Что предпринять?

При поступлении такого телефонного звонка прервите разговор. Настоящие сотрудники государственных служб, в том числе Социального фонда России, не звонят с подобными вопросами. По любым социальным вопросам нужно самостоятельно позвонить в единый контактный центр СФР по телефону 8-800-10-000-01 либо обратиться в ближайшее отделение фонда. Никому и никогда не сообщайте личные данные, реквизиты карт, СМС-код, а также логины и пароли от своих аккаунтов.

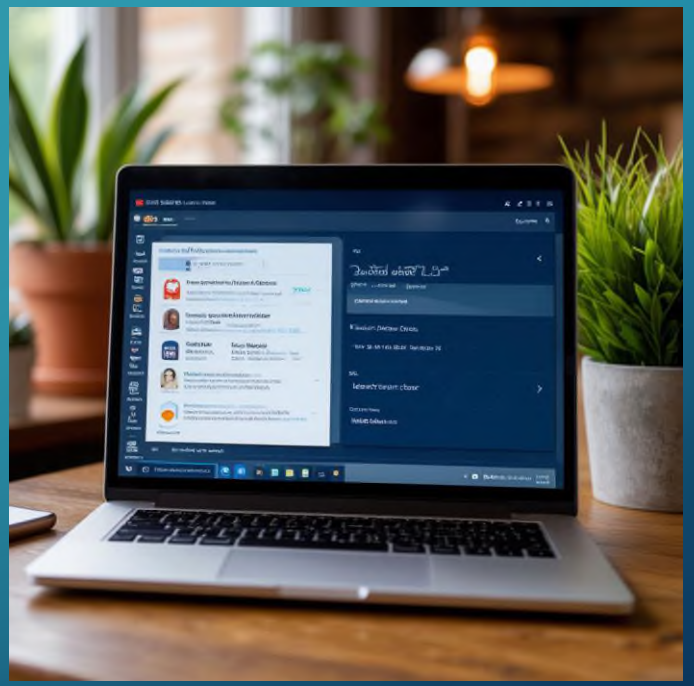
МОШЕННИЧЕСКАЯ СХЕМА № 8

Мошенники стали обманывать военнослужащих и их родных

Признаки мошенничества

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.



Что предпринять?

При поступлении такого телефонного звонка прервите разговор. Если вам пришло подозрительное сообщение или письмо, не реагируйте на них. Следует помнить, что «безопасных» («специальных») счетов не существует. В действительности счет, реквизиты которого называют мошенники, принадлежит им. По любым вопросам, связанным с деньгами, самостоятельно обратитесь в свой банк по номеру телефона, указанному на его официальном сайте или на обороте платежной карты.

МОШЕННИЧЕСКАЯ СХЕМА № 9

Злоумышленники используют кампанию по сдаче налоговых деклараций

Признаки мошенничества

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.

Что предпринять?

Будьте бдительны и не реагируйте на такие письма: не переходите по ссылкам в сообщении и не предоставляйте личную и финансовую информацию. Налоговые органы не рассылают электронные сообщения о задолженности с предложением оплатить ее онлайн. Что касается кампании, которая проходит с 1 января по 2 мая 2024 года, то гражданам нужно самостоятельно подать в налоговый орган декларацию о доходах за прошлый год. Речь идет о доходах в том числе от продажи имущества (квартир и домов, земельных участков, транспортного средства), акций, сдачи в аренду имущества и других. Узнать о неуплаченных налогах, а также способах их оплаты можно с помощью сервиса «Личный кабинет налогоплательщика»

МОШЕННИЧЕСКАЯ СХЕМА № 10

Мошенники похищают деньги и имущество под предлогом обновления банкнот

Признаки мошенничества

Банк России выявил новую схему обмана, которую в последние месяцы начали использовать злоумышленники. Они 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. Есть даже случаи квартирных краж, совершенных под предлогом «обмена денег». Банк России напоминает, что обновленные банкноты — 100 и 5000 рублей — поступают в оборот постепенно. Старые банкноты не нужно специально обменивать на новые. И те и другие будут параллельно находиться в обращении

Что предпринять?

Игнорируйте предложения лиц, которые просят обменять банкноты или проверить их подлинность с помощью приложения.

Не устанавливайте никакие приложения по просьбе незнакомых лиц, а также не переходите по ссылкам, которые поступают от них. Ссылка для установки официального приложения «Банкноты Банка России» размещена на сайте регулятора. Его можно скачать самостоятельно на свой телефон.

По любым банковским вопросам звоните в свой банк по номеру, указанному на его официальном сайте или на оборотной стороне банковской карты.

МОШЕННИЧЕСКАЯ СХЕМА № 11

Использование ложных аккаунтов руководителей Банка России в мессенджерах

Признаки мошенничества

Мошенники создают аккаунты в популярных мессенджерах от лица руководителей Банка России. Страницы содержат их реальные данные (фамилия, имя, отчество, фото — эти сведения берутся из Интернета) и выглядят максимально достоверно. Используя фальшивые аккаунты якобы служащих Банка России, 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.

Такую схему злоумышленники могут применять и в отношении обычных граждан. Например, за счет создания поддельных аккаунтов друзей человека в социальных сетях.

Что предпринять?

Сотрудники регулятора не используют общедоступные мессенджеры или социальные сети для решения служебных вопросов. Обо всех подобных случаях мошенничества необходимо сообщать в правоохранительные органы.

Банк России рекомендует гражданам сохранять бдительность и не сообщать посторонним людям личные и финансовые данные, под каким бы предлогом или каким бы способом их ни пытались узнать. Не нужно совершать какие-либо денежные операции по просьбе незнакомых лиц.

При возникновении любых сомнений относительно сохранности денег на банковском счете необходимо самостоятельно позвонить в свой банк по номеру, указанному на его официальном сайте или на оборотной стороне банковской карты.

МОШЕННИЧЕСКАЯ СХЕМА № 12

Мошенники обещают выплаты наличными в Общественной приемной Банка России

Признаки мошенничества

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 СМС-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.

Что предпринять?

Записаться на личный прием можно через сайт cbr.ru или контактный центр регулятора 8 (800) 300-30-00. Банк России предупреждает: если вы самостоятельно этого не делали, но получили сообщение о записи, это значит, что вашими персональными данными пытаются воспользоваться злоумышленники. Не реагируйте на такое сообщение.

Мошенники широко используют легенду о «безопасном» счете в Центробанке или «спецсчете». Они рассчитывают, что упоминание регулятора финансового рынка усыпит бдительность человека. В действительности такого счета не существует, и по факту жертва переводит деньги злоумышленникам. Сотрудники Центробанка не звонят людям и не направляют никому копии каких-либо документов, не запрашивают персональные и банковские сведения, не предлагают совершить какие-либо операции со счетом.

Если вам позвонили якобы «работники» Банка России, правоохранительных органов или банка и разговор касается ваших финансов, положите трубку. Не раскрывайте никому свои персональные и финансовые данные.

МОШЕННИЧЕСКАЯ СХЕМА № 13

Хакеры распространяют вирусные шаблоны документов, чтобы похитить средства компаний

Признаки мошенничества

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.

Что предпринять?

Соблюдайте осторожность при работе с сайтами, в адресной строке которых отсутствует значок безопасного соединения (замочек). При скачивании документа обращайте внимание на его формат — безопасными, как правило, являются pdf, docx, xlsx, jpg, png.

Чтобы не стать жертвой фишинговых сайтов, необходимо установить на своих устройствах антивирус и регулярно его обновлять. Рекомендуем также настроить запрет на запуск и установку вспомогательных компьютерных программ для удаленного доступа. Обычно официальные сайты государственных органов в популярных поисковых системах маркируются синим кружком с галочкой. Обращайте внимание на адрес веб-ресурса — поддельный может отличаться от официального всего лишь одной буквой.

МОШЕННИЧЕСКАЯ СХЕМА № 14

Мошенники стали приглашать россиян на «личный прием в Центробанк»

Признаки мошенничества

Злоумышленники, которые представляются якобы сотрудниками Банка России, усовершенствовали эту распространенную мошенническую схему. Новая легенда обмана, которую преступники используют по всей стране, выглядит очень правдоподобно. Теперь они не только звонят гражданам от имени Центробанка, но еще и отправляют на электронную почту сообщения с приглашением на личный прием в Банк России. Письма начинаются с обращения по имени и отчеству, в них указывается время приема и настоящий адрес Банка России в регионе проживания потенциальной жертвы.

Чтобы убедить человека, что с ним взаимодействуют настоящие сотрудники Банка России, мошенники используют специальный технический прием — меняют электронный адрес того, кто отправляет сообщение, на вызывающий доверие. В данном случае злоумышленники указывают домен Банка России cbr.ru. Это очень опасная схема действий, и часто из-за доверия к электронному адресу люди попадаются на уловки с подменой.

Персональное приглашение на личный прием — один из поводов вступить в контакт с потенциальной жертвой, вывести ее на доверительный диалог. После отправки письма аферисты могут позвонить получателю и под различными предлогами выманить данные его банковской карты и СМС-код либо побудить перевести деньги на счета злоумышленников.

Что предпринять?

Если вы не записывались на прием в Банк России, но получили подобное приглашение, не реагируйте на него и удалите сообщение. Для уточнения любых вопросов можно позвонить в контактный центр Банка России по бесплатному номеру 8 (800) 300-30-00 (для звонков с мобильного — короткий номер 300).

Банк России по своей инициативе не приглашает граждан на личный прием, его работники не звонят людям и не направляют никому копии каких-либо документов, не запрашивают персональные и банковские сведения, не предлагают совершить какие-либо операции со счетом. Будьте бдительны, мошенники часто представляются сотрудниками Банка России. По любым банковским вопросам самостоятельно позвоните в банк по номеру телефона, указанному на оборотной стороне карты или на сайте кредитной организации.

МОШЕННИЧЕСКАЯ СХЕМА № 15

Злоумышленники стали похищать деньги без данных карты

Признаки мошенничества

Банк России выявил новую мошенническую практику социальной инженерии с применением QR-кода. Некоторые банки внедрили сервис снятия наличных денег с помощью QR-кода. В мобильном приложении клиент может самостоятельно сгенерировать такой код на нужную сумму, поднести его к сканеру в банкомате и снять наличные. Этим стали пользоваться злоумышленники. Они звонят клиентам банков под видом сотрудников кредитной организации, сообщают, что в банк поступил несанкционированный запрос на снятие денег со счета, и просят прислать QR-код, чтобы отменить операцию. Расчет на то, что потенциальная жертва не в курсе особенностей QR-кода и легкомысленно относится к изображению с черно-белыми квадратиками, поэтому легко может им поделиться. Заполучив код, лжесотрудники банков просто снимают деньги в банкоматах со счета обманутого человека.

Что предпринять?

QR-код в этом случае фактически является поручением банку на выдачу денег без ввода ПИН-кода. Никогда не делитесь QR-кодом с незнакомыми людьми, не храните его изображение в мобильных устройствах или в распечатанном виде. Помните, что настоящие сотрудники банков никогда не запрашивают у клиентов QR-код.

МОШЕННИЧЕСКАЯ СХЕМА № 16

Мошенники представляются работодателями

Признаки мошенничества

Злоумышленники рассылают по электронной почте, через СМС 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.

Что предпринять?

Не доверяйте рассылкам с предложением о работе, тем более если вас заставляют оплатить какие-либо услуги, товары, зарезервировать вакансию и провести другие платежи. Такие предложения «гарантированной работы» — популярный прием мошенников.

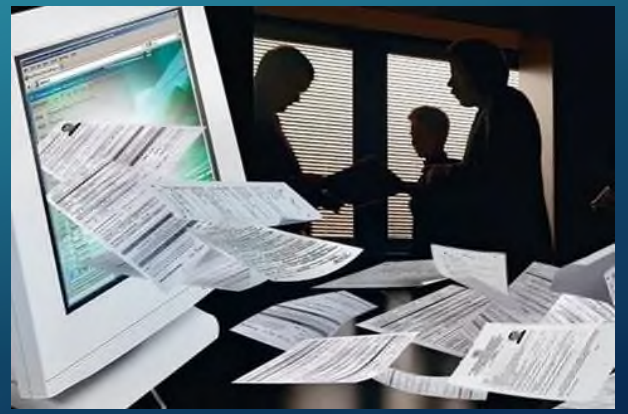
Кроме того, при получении таких предложений о работе не сообщайте свои паспортные данные и финансовые сведения (данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код).

МОШЕННИЧЕСКАЯ СХЕМА № 17

Сообщают клиенту банка об утечке персональных данных

Признаки мошенничества

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.



Что предпринять?

При поступлении такого телефонного звонка прервите разговор.

Банк России напоминает, что ни работники банков, ни сотрудники правоохранительных органов никогда не запрашивают данные банковской карты (ее номер, трехзначный код с оборотной стороны, СМС-код). Эти сведения нужны мошенникам.

Кроме того, ни Банк России, ни представители правоохранительных органов не направляют фото удостоверений или какие-либо другие документы.

МОШЕННИЧЕСКАЯ СХЕМА № 18

Лжесотрудники Банка России

Признаки мошенничества

Банк России отмечает очередную волну широкого распространения мошеннической схемы, 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.

Что предпринять?

Банк России напоминает, что не работает с физическими лицами как с клиентами, не ведет их счета, не звонит им, а его сотрудники не направляют никому копии своих документов. При поступлении телефонного звонка от мошенника немедленно прервите разговор и по возможности заблокируйте его номер. При возникновении любых сомнений относительно сохранности денег на вашем банковском счете самостоятельно позвоните в свой банк по номеру, указанному на его официальном сайте или на оборотной стороне банковской карты.

МОШЕННИЧЕСКАЯ СХЕМА № 19

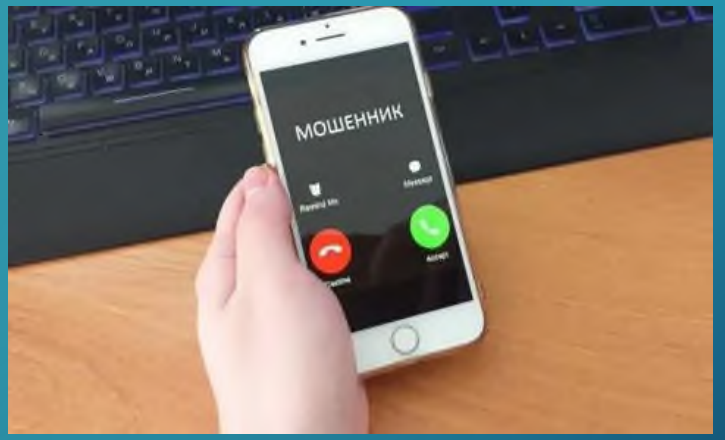
Представляются сотрудниками операторов мобильной связи

Признаки мошенничества

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 СМС-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.



Что предпринять?

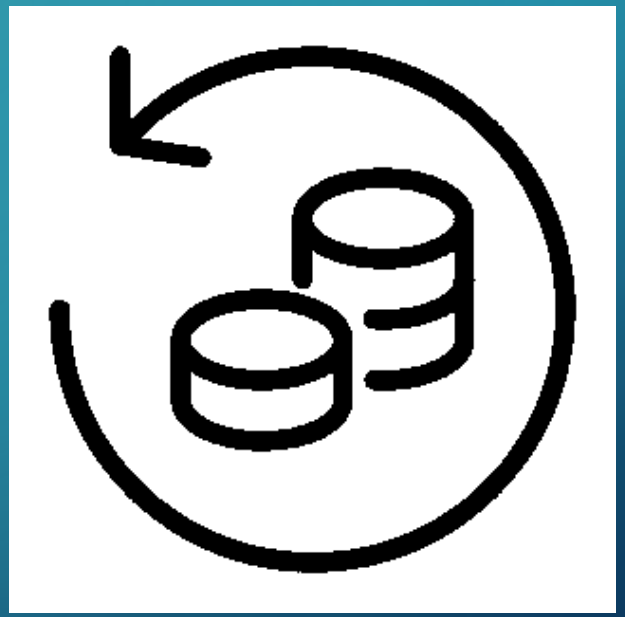
При поступлении такого телефонного звонка прервите разговор. Если вы продолжили общение и вам во время разговора пришел СМС-код от личного кабинета, никому не сообщайте его. Если возникли вопросы, самостоятельно позвоните в службу поддержки мобильного оператора по номеру, который указан на его официальном сайте.

МОШЕННИЧЕСКАЯ СХЕМА № 20

Обмен кешбэка на рубли

Признаки мошенничества

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 СМС-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.



Что предпринять?

При поступлении такого телефонного звонка прервите разговор. Сотрудники банков никогда не запрашивают по телефону финансовые данные, в том числе трехзначный код с оборотной стороны карты или СМС-код.

По любым банковским вопросам, в том числе по кешбэку, самостоятельно позвоните в банк по номеру, указанному на оборотной стороне карты или на сайте кредитной организации.

МОШЕННИЧЕСКАЯ СХЕМА № 21

Обещают помочь с компенсацией похищенных денег

Признаки мошенничества

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. Только за май 2022 года Банк России направил в правоохранительные органы на блокировку данные о 38 интернет-ресурсах с предложением различных компенсаций, а также возврата украденных мошенниками денег.

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.

Что предпринять?

Клиент банка вправе рассчитывать на возврат похищенной суммы лишь в том случае, если он самостоятельно не переводил деньги на мошеннические счета и не раскрывал злоумышленникам свои личные и финансовые данные.

Если деньги списали без вашего согласия, то единственный законный механизм вернуть их следующий: незамедлительно обратитесь в банк, заблокируйте карту и в течение суток после происшествия напишите в отделении банка заявление о несогласии с операцией.

МОШЕННИЧЕСКАЯ СХЕМА № 22

Предлагают проверить данные счета на предмет утечки

Признаки мошенничества

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.

Что предпринять?

Не существует сайтов, на которых можно проверить факт утечки банковских сведений!

Никогда не вводите данные своего счета или карты (номер, срок действия, проверочный код с оборотной стороны карты) и персональные данные (данные паспорта, дату рождения, адрес местожительства и другие) на сомнительных сайтах, не переходите по ссылкам из подозрительных электронных писем или СМС-сообщений.