Противодействие мошенническим практикам

Для хищения денег у граждан злоумышленники используют все более изощренные сценарии. В результате тысячи людей страдают от их действий, теряют деньги, которые в некоторых случаях копили годами. Знания о том, как противостоять мошенничеству, помогут в нужную минуту принять правильное решение. В этом разделе Банк России представляет распространенные схемы финансового мошенничества, которые будут регулярно дополняться, а также рекомендации по защите от них.

Злоумышленники специально оказывают психологическое воздействие на человека таким образом, чтобы он раскрыл личные или финансовые данные, перевел им деньги или даже взял кредит для последующей передачи средств в чужие руки. Мошенники могут звонить жертве, в том числе используя технологию подмены телефонных номеров, направлять электронные письма и сообщения со ссылкой на поддельные (фишинговые) сайты как финансовых организаций, так и любых других компаний и маркетплейсов. Они пытаются вывести человека из спокойного состояния и отключить у него логическое мышление, запугивая, торопя и оказывая давление на жертву или, напротив, стараясь заинтересовать и обрадовать внезапной выгодой. Схемы мошенников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Такое психологическое воздействие представляет собой методы социальной инженерии.

Банк России ведет работу по выявлению таких схем, информирует о случаях финансового мошенничества правоохранительные органы, которые занимаются расследованием хищений денежных средств.

Как не стать жертвой мошенников: общие рекомендации

Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-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).

Если вы стали жертвой финансового мошенничества:
Шаг № 1
Немедленно заблокируйте карту с помощью мобильного приложения или личного кабинета на сайте банка. Заблокировать ее также можно через контакт-центр банка (телефон указан на оборотной стороне карты) или в любом его отделении.
Шаг № 2
В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией. Также обратитесь с заявлением о хищении денег в любое отделение полиции.
ПОМНИТЕ: если вы самостоятельно перевели деньги мошенникам или предоставили им банковские данные, то банк не обязан возвращать похищенную сумму.

Типичные мошеннические схемы
Мошенники похищают деньги и имущество под предлогом обновления банкнот

Признаки мошенничества	**Что предпринять?**
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	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. 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. Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые

доверчивым людям фальшивые купюры. Жертвами чаще всего становятся пожилые люди. Есть даже случаи квартирных краж, совершенных под предлогом «обмена денег».	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.

Использование ложных аккаунтов руководителей Банка России в мессенджерах

Признаки мошенничества	**Что предпринять?**
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	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

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.	на его официальном сайте или на оборотной стороне банковской карты.

Мошенники обещают выплаты наличными в Общественной приемной Банка России

Признаки мошенничества	**Что предпринять?**
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	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

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.	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.

Мошенники стали приглашать россиян на «личный прием в Центробанк»

Признаки мошенничества	**Что предпринять?**
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	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

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.	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.

Злоумышленники стали похищать деньги без данных карты

Признаки мошенничества	**Что предпринять?**
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,	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.

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.	

Мошенники представляются работодателями

Признаки мошенничества	**Что предпринять?**
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	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).

личного кабинета человека на сайте банка и кражи средств с его счета.	

Сообщают клиенту банка об утечке персональных данных

Признаки мошенничества	**Что предпринять?**
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.	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.

Лжесотрудники Банка России

Признаки мошенничества	**Что предпринять?**
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.	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.

Представляются сотрудниками операторов мобильной связи

Признаки мошенничества	**Что предпринять?**
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.	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.

Обмен кешбэка на рубли

Признаки мошенничества	Что предпринять?
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.	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.

Обещают помочь с компенсацией похищенных денег

Признаки мошенничества	Что предпринять?
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.	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

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.	после происшествия напишите в отделении банка заявление о несогласии с операцией.

Предлагают проверить данные счета на предмет утечки

Признаки мошенничества	**Что предпринять?**
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.	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.

Сообщают о дефиците наличных рублей и валюты

Признаки мошенничества	**Что предпринять?**
Злоумышленники используют актуальную повестку для хищения средств у граждан. Например, якобы	При поступлении такого телефонного звонка немедленно прервите разговор.

сотрудники банка звонят и сообщают о дефиците как наличных рублей, так и валюты. Далее предлагают перевести деньги с карты или банковского счета на некий «специальный счет», с которого впоследствии человек сможет беспрепятственно снять средства. Для открытия такого счета злоумышленники запрашивают у гражданина финансовые данные — номер карты, включая трехзначный код на ее обороте, а также подтверждающий СМС-код от банка. Узнав эти сведения, они получают доступ к счету жертвы и переводят средства с него на мошеннические счета.	Сотрудники банков никогда не запрашивают по телефону личные и финансовые данные, в том числе трехзначный код с оборотной стороны карты или СМС-код. Чтобы уточнить интересующие вас вопросы, позвоните в банк по номеру, указанному на оборотной стороне карты или на официальном сайте кредитной организации.

Предлагают перевести деньги на «специальный счет Центрального банка»

Признаки мошенничества	**Что предпринять?**
В последнее время 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.	Банк России не работает с физическими лицами как с клиентами, не ведет их счета и не совершает звонков гражданам. При поступлении такого телефонного звонка немедленно прервите разговор.

Иногда, чтобы войти в доверие к человеку, звонящие могут напоминать о правилах безопасности — например, рекомендовать никогда не раскрывать финансовые данные.	

Убеждают оформить кредит

Признаки мошенничества	**Что предпринять?**
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.	При поступлении такого телефонного звонка немедленно прервите разговор. Ни сотрудники банков, ни бюро кредитных историй не информируют граждан об изменениях в кредитной истории по телефону. Сообщить по телефону или каким-либо другим способом о попытке оформления кредита могут, как правило, только мошенники.

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.	

Источник: https://cbr.ru/information_security/pmp/