ул. Неглинная, 12, Москва, 107016
8 800 300-30-00
www.cbr.ru

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 противодействовать мошенникам, помогут в нужную минуту принять правильное решение. В этом разделе Банк России представляет распространенные мошеннические схемы, которые будут регулярно дополняться, а также рекомендации по защите от них.

Мошенники 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. Они могут неоднократно 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. Злоумышленники всячески пытаются вывести человека из спокойного состояния и отключить у него логическое мышление. Для этого они могут запугивать, торопить и оказывать давление или, напротив, стараться 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 мошеннических схем, информирует о них 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.

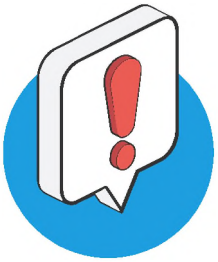
Если с неизвестного номера звонит якобы сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Самостоятельно 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 с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет Центробанка, 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.



Если вы стали жертвой мошенников:

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

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, 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.	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.

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	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

банковской карты и номер телефона используются ими для попытки взлома личного кабинета человека на сайте банка и кражи средств с его счета.	и финансовые сведения (данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код).

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. 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.	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.

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 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.	При поступлении такого телефонного звонка немедленно прервите разговор. 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. Иногда, чтобы войти в доверие к человеку, звонящие могут напоминать о правилах безопасности — например, рекомендовать никогда не раскрывать финансовые данные.	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.

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. 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.	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.