

## 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).

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 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 обратной стороне карты) или в любом его отделении.

#### **Шаг № 2**

В течение суток после получения сообщения о списании средств напишите заявление в отделение 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  
Использование ложных аккаунтов руководителей Банка России в мессенджерах  
Мошенники обещают выплаты наличными в Общественной приемной Банка России  
Хакеры распространяют вирусные шаблоны документов, чтобы похитить средства компаний  
Мошенники стали приглашать россиян на «личный прием в Центробанк»  
Злоумышленники стали похищать деньги без данных карты  
Мошенники представляются работодателями  
Сообщают клиенту банка об утечке персональных данных  
Лжесотрудники Банка России  
Представляются сотрудниками операторов мобильной связи  
Обмен кешбэка на рубли  
Обещают помочь с компенсацией похищенных денег  
Предлагают проверить данные счета на предмет утечки  
Сообщают о дефиците наличных рублей и валюты

Предлагают перевести деньги на «специальный счет Центрального банка»  
Убеждают оформить кредит

Дополнительная информация — в [ответах на часто задаваемые вопросы](#).