**Звонят ли работники Банка России через мессенджеры?**
Сотрудники Банка России, а также государственных и правоохранительных органов никогда не звонят через мессенджеры. Так поступают мошенники, которые представляются в том числе сотрудниками Банка России. Иногда злоумышленники направляют в мессенджер или на электронную почту поддельное удостоверение с логотипом и печатью Банка России. Такие документы иногда содержат имена реальных сотрудников, сведения о которых мошенники могут получить на сайте регулятора или каким-либо другим способом. Высылая фальшивое удостоверение, они рассчитывают добиться доверия, чтобы потом обманом выманить у человека деньги или оформить на него кредит.

Если вам позвонили якобы «работники» Банка России или правоохранительных органов и разговор касается ваших финансов, положите трубку. Никому и никогда не переводите деньги и не сообщайте свои личные и финансовые данные по просьбе незнакомого абонента, кем бы он ни представлялся.

**Звонят из банка и сообщают, что кто-то пытается оформить кредит на мое имя. Что делать?**
Это мошенники, поэтому немедленно прервите разговор, несмотря на угрозы и давление. Чтобы войти в доверие, злоумышленники могут даже обращаться по имени и отчеству. Не поддавайтесь на такие уловки. Не совершайте каких-либо действий по счету, если вам звонят с просьбой или требованием о переводе денег или с предложением об оформлении кредита. Самостоятельно позвоните в банк по номеру телефона, указанному на его официальном сайте или на обратной стороне карты. Также сообщите своим родственникам или людям, которым вы доверяете, о попытке мошенников обмануть вас.

**Мне позвонили из полиции и сообщили, что мои персональные данные были скомпрометированы, а деньги могут быть похищены, и предлагают перевести их на специальный счет в Центробанке. Что делать?**
Это наиболее распространенная мошенническая схема. Не существует «специальных», «безопасных», «защищенных» или каких-то других счетов, на которые граждане должны переводить деньги в адрес Центрального банка. Злоумышленники упоминают якобы специальный счет в Центробанке, чтобы усыпить бдительность человека. На самом деле счет, реквизиты которого называют мошенники, принадлежит им.  Не совершайте никаких действий по своему счету, положите трубку.

Если у вас остались какие-то сомнения, самостоятельно позвоните в банк по номеру телефона, который указан на оборотной стороне карты или на официальном сайте банка.

**Как узнать, почему мои данные оказались в базе данных Банка России «О случаях и попытках осуществления перевода денежных средств без согласия клиента»?**
Банк России ведёт базу данных «О случаях и попытках осуществления перевода денежных средств без согласия клиента». Она формируется на основе сведений, полученных от банков и других операторов платежных систем. Они по закону ( п. 4 ст. 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе») обязаны противодействовать переводам, которые происходят без согласия клиента, как правило, под воздействием злоумышленников. Поэтому информацию обо всех случаях и (или) попытках перевода денежных средств, по которым клиенты заявили свое несогласие с их совершением, банки и другие операторы платежных систем передают в Банк России. Таким образом данные о получателе денег по операциям без согласия клиента попадают в базу данных регулятора.

Для проверки обоснованности включения ваших данных в нее вы можете:

1. Обратиться в обслуживающую вас кредитную организацию.
2. Направить обращение в Банк России через Интернет-приёмную. В обращении обязательно укажите серию и номер паспорта, а также прочие реквизиты, по которым необходимо провести проверку (СНИЛС, номер карты, номер счета, номер телефона).

Рассмотрев обращение, Банк России в течение нескольких дней примет решение о целесообразности исключения ваших данных из базы «О случаях и попытках осуществления перевода денежных средств без согласия клиента».

**Как защититься от кибермошенников?**

Кибермошенники обманывают людей в Интернете или по телефону. У них множество легенд и способов обмануть человека, которые всегда сводятся к одному: у человека пытаются выманить данные карты, пароли или коды из СМС, либо провоцируют самостоятельно перевести деньги. Поэтому важно помнить: никогда не сообщайте данные своей карты, пароли из СМС, не переводите деньги на счет по просьбе неизвестного абонента, кем бы он не представлялся. Также никогда не вводите эти данные на сайтах, на которые вы перешли по ссылке из письма или СМС, а еще лучше вообще не переходите на сайты по ссылкам из подозрительных писем.

**Что делать, если кто-то по ошибке зачислил на мой счет деньги?**

Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем вам звонит человек, который по ошибке зачислил денеги, и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС — не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, прежде чем переводить кому-то деньги, если поступление все-таки было, обратитесь в свой банк и сообщите об этом. Банк должен сам вернуть ошибочно зачисленные деньги.

**Что делать, если приходит сообщение о необходимости подтвердить покупку, которую я не совершал?**

Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас данные, чтобы списать с вашего счета средства или подписать вас на ненужный платный сервис. Если вам придет сообщение о необходимости подтвердить покупку — игнорируйте его.

**Что делать, если мне звонят из МВД, ФСБ или других правоохранительных органов и просят данные карты или перевести деньги?**

Если вам звонят из банка, полиции или другой организации и просят совершить финансовые операции по счету (перевод, зачисление, в т.ч. на «безопасный» счет и т.д.), немедленно прекратите разговор. Если есть сомнения — позвоните в свой банк и узнайте, все ли в порядке с деньгами.

Зачастую при звонке злоумышленники представляются не только «службой безопасности банка», но и «сотрудниками МВД» или других правоохранительных органов, используют разнообразные приемы, сообщают, например, о якобы проводимых в данный момент мероприятиях по поимке преступников. Будьте бдительны и не выполняйте требования позвонившего. Настоящие сотрудники правоохранительных органов или банка никогда не будут запрашивать у вас данные карты или просить перевести деньги.

**Мне на электронную почту пришло письмо от Банка России, в котором говорится, что на мое имя открыт крупный денежный счет в иностранном банке, и что я должен оплатить теперь комиссию за её получение. Что это?**
Банк России по своей инициативе не направляет гражданам письма, не звонит и не рассылает сообщения. При получении электронных писем о поступлении на ваше имя крупной денежной суммы в иностранном банке или организации, происхождение которой вам неизвестно и/или вызывает сомнения, а также с предложением оплатить комиссию/налог/страховку и т.д. для её получения, настоятельно рекомендуем не отвечать на такие сообщения и ни в коем случае не переводить деньги, т.к. это распространенный вид мошенничества.

Также мошенники могут от имени Банка России звонить, рассылать смс/сообщения в мессенджерах с предложением получить компенсацию за купленные ранее лекарственные средства (медицинские приборы, БАДы).

Чтобы не стать жертвами злоумышленников, будьте бдительны, всегда проверяйте информацию на достоверность и не поддавайтесь на провокации.

Во всех случаях, вызывающих подозрение, немедленно обращайтесь в правоохранительные органы!

**На чем играют мошенники, чтобы выманить у вас нужную им информацию?**
Есть основные признаки того, что с вами разговаривает мошенник: собеседник активно использует ваше чувство страха (ваша карта заблокирована, вы можете потерять деньги, данные украдены и т.д.), собеседник давит на жажду наживы (пройдите опрос и получите вознаграждение, получите компенсацию, выплату, очень выгодные условия по кредиту или вкладу и т.д.). При этом от вас требуют срочно принять решение и совершить некоторые действия: сообщить персональные данные, проделать какие-то манипуляции с банковской картой. В противном случае вам угрожают потерей денег или возможности получить их.

Имейте в виду: даже если банк действительно зафиксировал попытку несанкционированной операции с вашего счета, он имеет право приостановить эту операцию на срок до двух суток, поэтому настоящий представитель кредитной организации не будет торопить вас принимать решение. Также вас всегда должны настораживать предложения получить легкие деньги, очень выгодные условия по кредитам или депозитам.

**Как узнать фишинговый сайт и как не стать жертвой фишинга?**
В Интернете множество фишинговых сайтов — это подделки под сайты настоящих финансовых (банков, страховых компаний и др.) или любых других организаций, которые сильно похожи на официальный сайт компании. Цель фишинговых сайтов — выманить личные и финансовые данные, которые нужны мошенникам для кражи денег.

Как правило, жертвы попадают на фишинговые сайты через ссылки, которые приходят им в письмах или СМС. Чтобы не стать жертвой фишинга, не переходите по ссылкам из подозрительных сообщений. Пользуйтесь только проверенными ресурсами. Обращайте внимание, чтобы в строке браузера рядом с названием сайта был значок замочка. Настоящие сайты финансовых организаций в некоторых поисковых системах (Яндекс и Mail.ru) помечены цветным кружком с галочкой, при наведении курсора появляется надпись о внесении в реестр ЦБ РФ.

**Что делать, если банк заблокировал карту?**
Во-первых, не волнуйтесь, деньги, размещенные на счете, при блокировке остаются в полной сохранности, после решения проблемы вы получите к ним доступ.

Если вы получили смс-сообщение или телефонный звонок о блокировке карты, и вас просят сообщить свои личные или финансовые данные для разблокировки, проигнорируйте эту просьбу и позвоните в банк сами по номеру телефона, который указан на оборотной стороне карты.

Для безопасности карта блокируется, если трижды за сутки неправильно введен пин-код. Как правило, в таком случае для разблокировки нужно обратиться в свой банк, либо карта будет разблокирована автоматически на следующий день или через 24 часа после блокировки. Пин-код, при необходимости, можно сменить в интернет-банке, мобильном приложении или в контакт-центре банка. Если такой возможности нет, а пин-код вспомнить вы не можете, карту придется перевыпустить.

Банки обязаны отслеживать подозрительные операции по картам своих клиентов. Поэтому карта может быть заблокирована в случае, если банк заподозрит проведение мошеннических или подозрительных операций по вашему счету, либо операций, имеющих признаки отмывания доходов. По каким бы причинам банк не приостановил работу вашей карты, в день блокировки он обязан уведомить вас о причине такого решения.

Если конкретная операция (перевод) по карте выглядят подозрительно, банк может заблокировать только ее. После этого сотрудник банка должен связаться с вами и уточнить, действительно ли вы совершали такую операцию. В случае подтверждения с вашей стороны, она будет разблокирована. Если представитель банка не сможет дозвониться до вас в течение двух рабочих дней, операция будет автоматически разблокирована.

**Должен ли банк вернуть украденные со счета деньги?**
По закону (ст. 9 «О Национальной платежной системе») банк обязан вернуть (в течение 30 дней по переводам внутри России, в течение 60 дней — по трансграничным переводам) украденные деньги, если хищение произошло не по вашей вине. Но если вы сообщили мошеннику личные и финансовые сведения (данные карты и владельца, трехзначный код с оборотной стороны карты или СМС-код) то банк не обязан возвращать украденные деньги.

**Что делать, если с вашей банковской карты незаконно списали деньги?**

1. Как можно скорее позвоните в банк по номеру на обороте карты, сообщите о мошеннической операции и заблокируйте карту. Карту также можно заблокировать через приложение.
2. Обратитесь в отделение банка и попросите выписку по счету. Напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приеме. (Банк рассмотрит заявление в течение 30 дней. Если операция была международной — в течение 60 дней.)
3. Обратитесь в правоохранительные органы с заявлением о хищении.

Также читайте рекомендации для владельцев пластиковых карт от «Финансовой культуры».

**Какую именно информацию о своей банковской карте ни в коем случае нельзя сообщать посторонним людям?**

Если кто-либо запрашивает у вас номер карты, срок действия, код проверки подлинности карты (три цифры на обратной стороне — CVV или CVC), ПИН-код, а также код из СМС для подтверждения платежей и переводов — это мошенник. Ни в коем случае не сообщайте эти данные в разговоре с незнакомым человеком.

Вы можете указывать номер карты, срок действия, код проверки подлинности карты (CVV или CVC), а также код подтверждения транзакции из СМС только при совершении покупок на проверенных и надежных сайтах — в строке браузера должен быть указан значок замочка

Никогда и никому не сообщайте информацию о ПИН-коде: ее не знает и не должен знать даже банк, в котором вы обслуживаетесь.

**Что делать, если вам звонит человек, представляется сотрудником банка, в котором вы обслуживаетесь, и под тем или иным предлогом просит сообщить ему данные вашей карты, код из СМС или другие персональные данные?**
Настоящий сотрудник банка никогда и ни под каким предлогом не будет запрашивать у вас никакую информацию о вашей карте или персональные данные. Только в том случае, если вы сами позвонили в банк, у вас могут спросить кодовое слово, чтобы идентифицировать вас. Если вам поступил такой звонок, просто положите трубку. Если у вас есть сомнения относительно сохранности денег на вашем счете — перезвоните в свой банк по номеру телефона, указанному на вашей банковской карте или на сайте кредитной организации. Также сообщите в Интернет-приемную Банка России о номере телефона, с которого вам звонили, — он будет заблокирован.