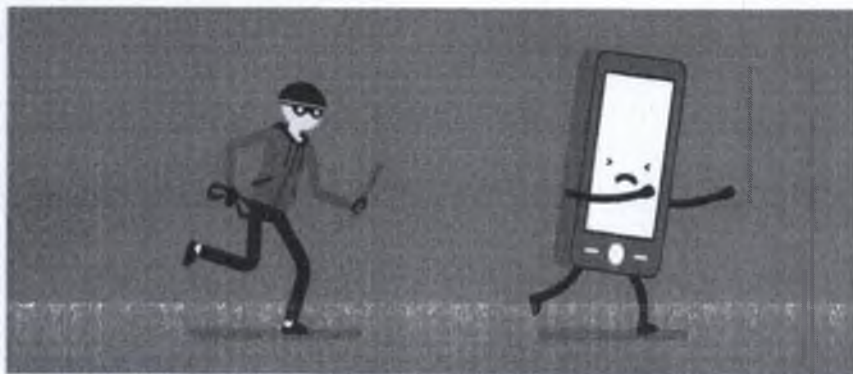


Звонят с номера банка и просят предоставить конфиденциальные данные. Что делать?

Киберпреступники все чаще маскируют свой номер под официальные номера банков. Разбираемся, как не попасться на уловки мошенников.



Для начала проверьте, точно ли это сотрудник банка. Положите трубку, позвоните по официальному номеру банка и уточните, все ли в порядке с вашими счетом и картой.

Почему стоит положить трубку и набрать официальный номер банка самому?

Даже если у вас на телефоне высветился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. Наберите номер горячей линии банка вручную. Телефон горячей линии можно найти на обратной стороне банковской карты или на официальном сайте банка.

Такая бдительность может показаться параноидальной. Но в последнее время киберпреступники все чаще подделывают официальные телефонные номера банков, чтобы обмануть их клиентов.

Мошенники используют специальное программное обеспечение, которое помогает скрыть настоящий номер звонящего, при этом на телефоне человека отражается официальный номер банка. Обычно преступник обращается к собеседнику по имени и отчеству, может назвать фамилию и даже номер и срок действия карты. Эти сведения мошенники, как правило, получают заранее из открытых источников, например из социальных сетей, и с помощью Фишинга.

Даже если информация звучит очень правдоподобно, лучше перестраховаться и позвонить в банк самому, чтобы общаться точно с его сотрудником, а не с преступником.

Чаще всего обманщики звонят поздно вечером, ночью или ранним утром в выходные дни, когда человек спит и не может быстро сориентироваться. Преступник представляется сотрудником банка и сообщает о подозрительной операции, которая требует немедленных действий со стороны клиента. Мошенники хорошо знакомы с психологией: говорят быстро и уверенно,

используют профессиональные термины, нередко фоном включают звуки, имитирующие работу оживленного колл-центра. Все это помогает им втереться в доверие к клиенту банка и сделать так, что он потеряет бдительность.

При этом они торопят и запугивают клиента, дают на его эмоции и уверяют, что случится что-то непоправимое.

Например, обманщики говорят, что по карте проводится подозрительный платеж на крупную сумму и чтобы его остановить, нужно срочно сообщить данные карты, ПИН-код или одноразовый пароль из СМС-сообщения. Если человек колеблется или отказывается их назвать, ему угрожают, что деньги с его карты прямо сейчас уйдут к мошенникам.

Если преступникам удастся узнать нужную им информацию, они получают доступ к счету и снимают с него все деньги.

Как защитить свои деньги от мошенников?

Если клиент сам сообщит преступникам секретную информацию, которую нельзя разглашать, вернуть деньги через банк не получится. Поэтому стоит придерживаться основных правил безопасности, чтобы не поддаваться на уловки мошенников и не потерять деньги:

1. Всегда набирайте только официальный номер банка. Он указан на обратной стороне карты и на официальном сайте банка.
2. Не перезванивайте и не отправляйте СМС на незнакомые номера, не спешите переходить по ссылкам из сообщений «от банка». В любой непонятной ситуации звоните в банк по официальному номеру и уточняйте информацию у оператора.
3. Если вам звонят из банка, финансовой организации или госоргана, уточните ФИО и должность звонящего и скажите, что перезвоните ему сами. Положите трубку и перезвоните по официальному телефону организации или на горячую линию банка. Номер нужно набрать вручную.
4. Не стоит паниковать и спешить. Если банк выявит подозрительную транзакцию, он сразу приостановит ее на срок до двух суток. За это время вы можете либо подтвердить эту операцию банку, либо отменить ее. Это решение надо принять в течение 48 часов - этого времени достаточно, чтобы хорошо все обдумать и без спешки самостоятельно позвонить в банк. Если же вы ничего не сделаете, то через двое суток банк автоматически снимет блокировку и операция пройдет.
5. Ни под каким предлогом никому не сообщайте личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-коды. Называть кодовое слово можно, только если вы сами звоните на горячую линию банка.

Подробнее о том, как защититься от киберкраж, читайте в статье «Мошенничество с банковскими картами онлайн».

Что делать, если с банковской карты украли деньги

Пришло СМС, что с карты списали деньги, но вы ничего не покупали, переводы не делали и наличные не снимали. Вероятно, ваша карта или ее данные попали к мошенникам. Что делать и можно ли вернуть похищенное?



Если коротко, то нужно: немедленно заблокировать карту, сообщить в банк по горячей линии о краже денег и написать в отделении банка заявление о несогласии с операцией. Сделать все это необходимо не позднее следующего дня после того, как банк уведомил вас об операции, которую вы не совершали.

Если вы соблюдали правила использования карты, в частности не хранили ПИН-код вместе с картой и никому не сообщали ее данные, то велик шанс вернуть украденные деньги.

А теперь разберем по шагам, что нужно будет сделать.

1. Заблокировать карту

Чтобы отрезать мошенникам доступ к оставшимся деньгам на карте, ее нужно немедленно заблокировать. Сделать это можно разными способами:

- **Через мобильное приложение банка.** Если оно у вас установлено и там есть опция блокировки карты, найдите в приложении нужную карту и выберите команду «Заблокировать».
- **По телефону горячей линии.** Номер для экстренной связи указан на обратной стороне карты и на официальном сайте банка. Лучше заранее сохранить этот номер в телефоне, чтобы не тратить время на поиски. Оператор службы техподдержки попросит назвать паспортные данные, кодовое слово или код из СМС-сообщения, которое он вам вышлет. После этого сотрудник банка заблокирует карту.
- **В онлайн-банке.** Зайдите в личный кабинет на сайте банка, найдите опцию «Заблокировать карту» и подтвердите свое действие кодом из

СМС.

- **По СМС.** Некоторые банки позволяют блокировать карты по СМС. Обычно для этого надо отправить на короткий номер банка кодовое слово (например, «блокировка») и через пробел последние четыре цифры номера карты. Если у вас только одна карта, то цифры можно не вводить — банк и так поймет, о какой карте речь. Вы получите код, который надо снова отправить на номер банка для подтверждения блокировки.

- **В отделении банка.** Если сообщение о незаконной операции по вашей карте застало вас рядом с офисом банка и у вас есть с собой паспорт, то вы сможете не только заблокировать карту, но и сразу написать заявление на возврат денег.

2. Сообщить о краже и оформить возврат денег



По закону банк обязан вернуть деньги, если вы выполнили два условия:

- Сообщили банку о краже денег с карты не позднее следующего дня после того, как банк уведомил вас о подозрительной операции. Не успеете — банк имеет право вам отказать.
- Не нарушали правила безопасности при использовании карты. В частности, не сообщали мошенникам данные карты, не хранили ПИН-код вместе с картой, не писали код на самой карте, не позволяли никому делать ксерокопии или фотографировать вашу карту. Если банк докажет обратное, то не вернет вам украденные деньги.

Как именно вы должны сообщить о краже — по телефону или лично в отделении — прописано в вашем договоре. Чтобы не терять времени, лучше сразу позвонить в банк и уточнить порядок действий у оператора.

Но в любом случае вам придется сходить в отделение банка, чтобы написать заявление о несогласии с операцией с требованием вернуть деньги. Сохраните у себя копию заявления с отметкой о том, что банк его принял.

Поскольку кража денег — это уголовное преступление, напишите заявление в полицию. Возможно, ваша информация поможет быстрее вычислить и поймать преступников.

Банк проведет служебное расследование. В нем примет участие и платежная система. Если мошенники действовали на территории России, то по закону служебное расследование может длиться максимум 30 дней, если операция была международной — 60 дней.

По итогам расследования с вами свяжется сотрудник банка и сообщит о решении. Если банк убедится, что вы не нарушали правила использования карты и при этом опротестовали операцию вовремя, вам вернут деньги.

Но возможны и другие варианты развития событий:

Банк согласился вернуть деньги, но затягивает перечисление средств



Часто банки указывают срок возврата денег в договоре. Например, это может быть 30 или 60 дней. Если за это время банк не пополнил ваш счет, можно обращаться в суд.

Если же в договоре с банком сроки не установлены, то банк должен выполнять требования Гражданского кодекса. Статья 314 предписывает всем (в том числе банкам) выполнять свои обязательства «в разумный срок». Этот «разумный срок» вы и банк можете понимать по-разному. Но в кодексе есть уточнение: обязательства должны быть выполнены в течение семи дней с момента, когда вы предъявите свои требования.

Другими словами, вы можете подождать пару недель, если за это время деньги не вернут, то идите в банк писать заявление. В нем со ссылкой на Гражданский кодекс нужно потребовать перечислить украденную сумму в срок до семи дней.

Банк отказался возвращать деньги

В этом случае первым делом нужно потребовать от банка письменный отказ с обоснованием, почему он не соглашается вернуть деньги. Если банк такой отказ не выдаст или выдаст, но обоснование вам покажется неубедительным, стоит обратиться в суд. Если вы не нарушали договор с банком и вовремя сообщили о незаконной операции, скорее всего, суд примет решение в вашу пользу и деньги вам все-таки вернут.

Что делать, если банк не уведомил меня о незаконной операции? Можно ли в таком случае вернуть деньги?

По закону банк обязан уведомлять вас обо всех операциях по карте. Каким именно способом он это делает, прописано в вашем договоре. Это могут быть СМС-оповещения, письма по электронной почте или другие способы.

Если мошенники украли деньги с карты, а ваш банк не сообщил вам об операции, то по закону он обязан возместить потери. Даже если вы обнаружили кражу денег со счета не сразу, а через месяц или год после того, как она произошла.

В этом случае сначала нужно написать заявление в банк с требованием вернуть незаконно списанные деньги. Если же банк откажется их перечислить, то можно идти в суд.

Как защитить деньги на карте от мошенников?



Всегда следуйте нескольким главным правилам владельца карты:

1. Контролируйте операции по счету. Например, подключите услугу СМС-информирования по всем своим активным картам. Тогда вы будете сразу получать уведомления о каждой операции

по карте. Вместо СМС-сообщений можно выбрать push-уведомления в мобильном приложении банка. Они всегда бесплатны и не засоряют память телефона. Но в этом случае важно следить, чтобы у вас всегда был подключен

мобильный интернет. Иначе push-уведомление можно получить с серьезным опозданием и не успеть вовремя сообщить банку о краже денег.

2. Никому не сообщайте ПИН-код, CVC-/CVV-КОА (секретный код на обратной стороне карты), срок действия карты и другую информацию. Например, если вам звонят «из службы техподдержки банка» или «менеджер банка» говорит о том, что ваша карта якобы заблокирована, не стоит сообщать им данные своей карты. Настоящий сотрудник банка никогда не спросит у вас секретную информацию, такую как ПИН- код или CVC-/CVV-/код.

«Однажды мне пришло сообщение от банка, в котором я получаю зарплату. Текст типа такого: «Карта заблокирована из-за сомнительных операций». Там были почти все мои деньги на тот момент, я сразу перезвонил по номеру, который был в конце сообщения...»

3. Не позволяйте продавцам и официантам уносить карту из поля вашего зрения. Всегда прикрывайте рукой клавиатуру терминала оплаты или банкомата, когда вводите пароль. Стоит также следить за тем, чтобы с камер наблюдения не было видно, как вы набираете ПИН- код.

4. Заходите только на проверенные сайты и никогда не кликайте по ссылкам из писем неизвестных «доброжелателей».

5. Перепроверяйте любую информацию о блокировке карты, отказе в проведении операции или других проблемах с картой. Для этого звоните на горячую линию банка — и только на нее. Телефон для экстренной связи всегда указан на обратной стороне карты и на официальном сайте банка.

С сентября 2018 года банки могут приостанавливать денежные переводы и платежи с карт, если они выглядят подозрительными. Такие правила безопасности прописаны в новом законе.

Сомнения у банка может вызвать платеж в другой стране, особенно если раньше клиент за границу не ездил. Или если вдруг с карты пытаются списать необычно большую сумму. А если с одной и той же карты вдруг одновременно идет «веерный» перевод сразу на несколько других карт, это точно повод для банка остановить транзакции и временно заблокировать карту.

Основные признаки подозрительных операций определил Банк России, а банки имеют право дополнить их собственными критериями — по итогам мониторинга поведения своих клиентов.

Если операция попала в число подозрительных, банк обязан немедленно связаться с клиентом, чтобы выяснить, действительно ли он давал согласие на этот платеж или перевод.

Если банк не получит ответ в течение двух дней, то разблокирует карту и проведет транзакцию. Если же клиент подтвердит операцию, то и платеж, и

карту разблокируют немедленно. Ну, а если владелец карты сообщит, что не делал этот платеж, банк отменит операцию и предложит перевыпустить карту.

Как защититься от кражи денег с карты

Мошенники умеют не только незаметно воровать телефоны и кошельки, но и уводить деньги с банковских карт. Они придумали для этого множество хитрых способов. Чтобы не попасть в ловушку мошенника, нужно всегда соблюдать семь важных правил.



Правило № 1. Никому не сообщайте свои пароли и коды

ПИН-код от карты — это секрет, который никому нельзя раскрывать. Лучше не сохранять его в телефоне и тем более не записывать на карте. А при вводе ПИН-кода в банкомате или в магазине надо всегда прикрывать клавиатуру рукой.

На обратной стороне карточки есть CVC/CVV-код — три секретные цифры. Они нужны для оплаты покупок в интернете. Чтобы мошенники не смогли потратить деньги с вашей карты, ни в коем случае не диктуйте и не показывайте никому CVC/CVV-код.

Сотрудники банка никогда не спрашивают код с карты, ПИН-код, а также коды из СМС, которые присылает банк. Секретными кодами интересуются только мошенники. Обманщик готов прикинуться кем угодно, лишь бы их выведать: не только работником банка, но и родственником, другом или даже незнакомцем, попавшим в беду.

Звонит незнакомец, извиняется и говорит, что случайно указал ваш номер телефона в какой-то анкете. Он просит продиктовать ему код, который по ошибке пришел вам в СМС. Это точно мошенник. Немедленно бросайте трубку.

Мошенники могут притворяться, что они ваши знакомые, которые якобы хотят скинуть деньги вам на карту. Но для перевода им нужны номер карты, срок ее действия и CVC/CW-код. Это тоже обман. Для того, чтобы перечислить деньги, достаточно номера карты. Никакие другие данные — срок действия, имя владельца или код — не требуются.

Правило № 2. Подключите СМС- оповещения по карте

Это нужно, чтобы сразу же получать от банка СМС обо всех действиях по карте. Например, обо всех покупках, которые оплачены картой. Эти сообщения нужно читать очень внимательно. Если пришло сообщение о покупке, КОТОРУЮ вы не совершали, скорее всего, картой воспользовался мошенник.

Стоит сразу позвонить в банк, сообщить о подозрительном СМС и попросить заблокировать карту. Номер горячей линии банка есть на обратной стороне карты. Лучше всего сохранить этот номер в контактах на своем телефоне и в случае проблем с картой звонить только по нему.

Пришло сообщение, что с вашей карты списали 1000 рублей за неизвестную покупку. И тут же приходит СМС «из службы безопасности», что «по карте проходит подозрительная операция». Чтобы «ее отменить», просят перезвонить по незнакомому номеру телефона или перейти по ссылке. Упс, это снова обман. Не стоит этого делать: по ссылке, скорее всего, вирус, а номер телефона принадлежит мошенникам.

Правило № 3. Пользуйтесь антивирусами

Очень важно установить антивирусные программы на всех устройствах, которыми вы пользуетесь, — на компьютере, планшете и мобильном телефоне. Антивирус защитит от вредоносных программ и сайтов, с помощью которых мошенники крадут деньги.

В интернете можно найти бесплатные версии антивирусных программ с ограниченным функционалом. Главное — скачивать их из официальных магазинов приложений или на сайтах известных разработчиков антивирусов.

Правило № 4. Выбирайте безопасные сайты

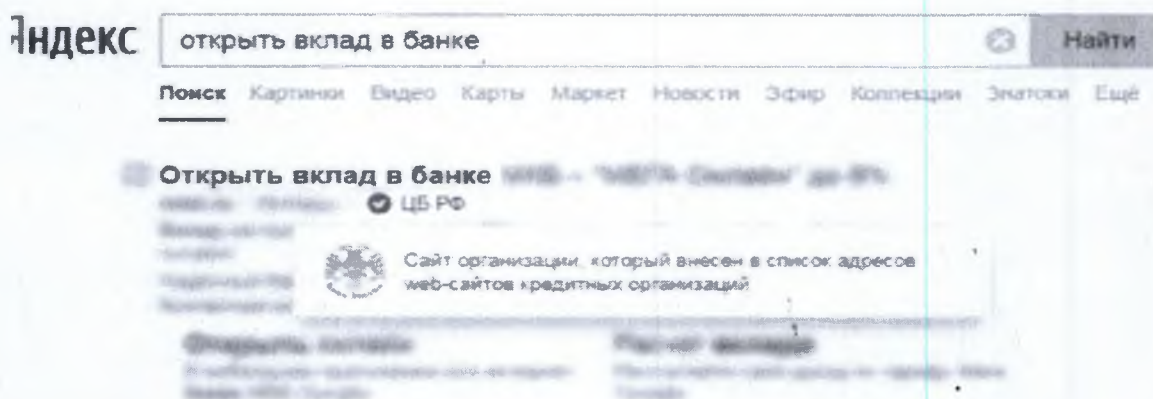


Мошенники создают сайты-двойники популярных онлайн-ресурсов. Например, они могут сделать копию сайта банка или вашего любимого онлайн-

магазина. Если вы введете там свои пароли, коды, данные карты, то они попадут к мошенникам.

Как проверить сайт?

- Сайты банков можно легко проверить с помощью поисковых систем «Яндекс» и Mail.ru. Настоящие сайты реальных банков имеют специальную отметку — галочку в синем кружке. Если такого значка нет — это сайт мошенников.



- Обычно название сайта-двойника почти полностью совпадает с названием какого-нибудь известного сайта, не считая пары букв. Поэтому нужно всегда тщательно проверять адресную строку своего браузера. Набирайте адрес сайта вручную, а лучше сразу сохраняйте официальные и проверенные сайты в закладках.
- Обратите внимание на адрес ресурса. У безопасного сайта он начинается с <https://>. В конце адресной строки защищенного сайта есть значок в виде закрытого замка. Если сайт не имеет защиты, на нем нельзя вводить личную информацию и данные карты.

Прежде чем вводить данные карты или паспорта на каком-либо сайте, важно внимательно изучить его, почитать отзывы в интернете.

Правило № 5. Не оплачивайте покупки с чужих гаджетов

Делать покупки, заходить на сайт банка или в банковское приложение надо только с личного компьютера, планшета и телефона. Установите пароли на все свои гаджеты.

Если потеряете телефон или планшет, на которых было банковское мобильное приложение и куда приходили уведомления и пароли, срочно звоните в банк. Попросите отключить от этого номера телефона все услуги

и заблокировать доступ к счету с потерянного гаджета. Поменяйте логин и пароль отличного кабинета в интернет-банке.

Когда вы восстановите свой номер у мобильного оператора, можно будет снова подключить к нему СМС-уведомления.

Правило № 6. Не переходите по сомнительным ссылкам из сообщений

Никогда не переходите по ссылкам из писем и СМС от незнакомцев. Это может быть вредоносная программа, которая крадет персональные данные.

Но даже если ссылку прислал кто-то из друзей, не спешите ее открывать. Мошенники могли зайти в чужой аккаунт и разослать сообщения от имени знакомого.

Например, в соцсети приходит сообщение от друга: «Смотри, фотки с моего ДР! Они просто огонь!». К сообщению прикреплена ссылка или файловый архив. Не стоит сразу по ним кликать. Лучше позвонить другу или написать в другой социальной сети и уточнить, не спам ли это.

Обычно за подобными ссылками и архивами скрываются троянские программы. Они сами устанавливаются на гаджет, воруют и подделывают ваши данные, в том числе могут переводить мошенникам деньги с ваших счетов.

Правило № 7. Перепроверяйте информацию



Мошенники очень надеются, что вы им сразу поверите. Они специально торопят вас, чтобы не дать времени перепроверить информацию. Но в денежных вопросах нельзя спешить.

Чаще всего мошенники используют такие схемы:

- Звонит незнакомец и сообщает, что ваши родственники или друзья попали в беду. Мошенник попросит срочно перечислить деньги, чтобы

их выручить. Он надеется, что вы испугаетесь и поведетесь на обман. Не спешите переводить деньги: сначала позвоните родным или друзьям и проверьте, все ли у них в порядке.

- Приходит СМС о том, что вам зачислены деньги. Сообщение похоже на уведомление от банка. Тут же звонит какой-то растяпа, говорит, что по ошибке перевел деньги, и просит их вернуть. Просто бросайте трубку. Скорее всего, это мошенник, деньги вам не приходили, а СМС «от банка» — липовое. Позвоните в банк и спросите, приходили ли деньги на счет. А лучше сообщите родителям и попросите помочь вам разобраться.
- Знакомая, с которой вы давно не общались, внезапно пишет в соцсети и спрашивает, как дела. Завязывается переписка, во время которой она неожиданно просит одолжить ей денег. Это сразу должно насторожить. Скорее всего, аккаунт вашей знакомой взломали. И мошенника вовсе не интересует, как у вас дела, — ему нужны ваши деньги. Ни в коем случае ничего не переводите. Напишите знакомой в другой мессенджер или позвоните и уточните, действительно ли ей нужна помощь. Если это обман — пометьте сообщение как спам и напишите жалобу администрации соцсети.

Не забывайте, что мошенники постоянно изобретают новые схемы обмана.

«Участвовала в конкурсе в соцсети Instagram около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала вещь, написала организаторам, после чего мне предложили оплатить доставку в размере 450р. После этого мне предложили перейти по ссылке...»

Ни в коем случае никому не передавайте секретную информацию по карте — даже тому, кто представился сотрудником банка. Никогда не переводите деньги, пока не разберетесь в ситуации. Расскажите о случившемся родителям. Перезвоните в банк самостоятельно по официальному номеру горячей линии и уточните интересующую вас информацию. Главное — не спешите.