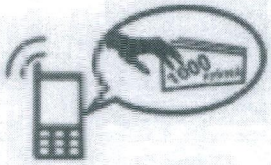
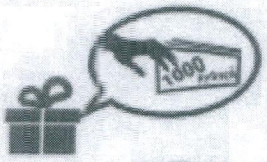
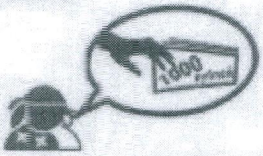
ОСТОРОЖНО – МОШЕННИКИ!



НЕ ДОВЕРЯЙТЕ информации, если вам сообщают, что ваш родственник или знакомый попал в беду и нужна крупная сумма денег, чтобы «вытащить» его.

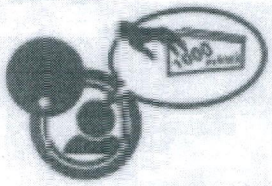


НЕ СОГЛАШАЙТЕСЬ на приглашения принять участие в розыгрыше призов, купить чудодейственные лекарства, приборы или дешевые вещи и продукты.

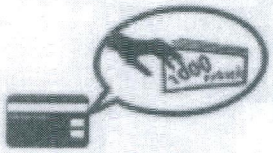


НЕ СОГЛАШАЙТЕСЬ на предложения снять порчу или сглаз, погадать, предсказать будущее, – это хороший повод завладеть вашими деньгами.

ВНИМАТЕЛЬНО ПРОВЕРЯЙТЕ квитанции на оплату штрафов и коммунальных платежей.



НЕ ОТКРЫВАЙТЕ дверь незнакомым людям, даже если они представляются работниками специальных служб, полиции, поликлиники, ЖКХ и т.п. Обязательно перезвоните и уточните, присылали ли к вам этого специалиста.



ПРОВЕРЯЙТЕ любые сообщения о блокировке банковской карты, позвонив по телефону горячей линии вашего банка (указан на оборотной стороне банковской карточки).

ПРОЯВЛЯЙТЕ осторожность, если с вами пытаются заговорить на улице незнакомые люди.

НЕ СТЕСНЯЙТЕСЬ звонить в полицию, если вы подозреваете, что вас хотят обмануть, – ВАМ обязательно помогут.

ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

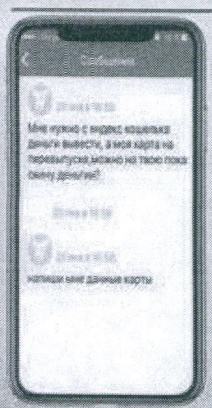
ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

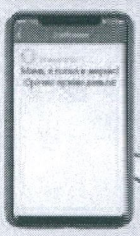


СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

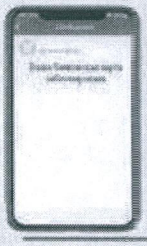
ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!

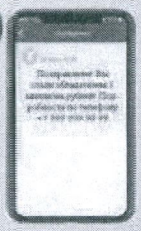


БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

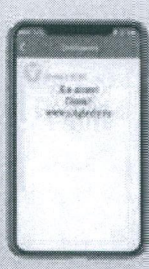
Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

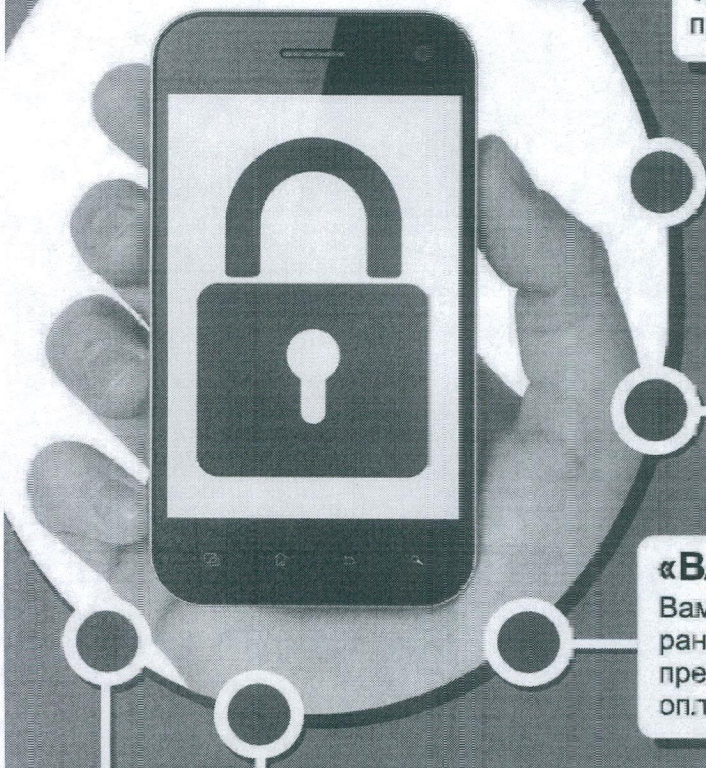


ВИРУС В ТЕЛЕФОНЕ



Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА



«ВАША КАРТА ЗАБЛОКИРОВАНА»
SMS-сообщение о якобы заблокированной банковской карты, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата

«РОДСТВЕННИК В БЕДЕ»
Требование крупной суммы денег для решения проблемы с якобы попавшему в беду родственником

«ВЫ ВЫИГРАЛИ»
SMS-сообщение о том, что вы стали победителем и вам положен приз

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ»
Вам якобы положена компенсация за приобретаемые ранее некачественные БАДы либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ»
просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства со счета по чеку

УСЛУГА, ЯКОБЫ, ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУП К SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ


ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!
ПО ТЕЛЕФОНУ НЕЛЬЗЯ:
Выиграть миллион рублей!
Разблокировать банковскую карту!
Получить компенсацию от банка!
Приобрести редкие товары и уникальные таблетки!
Спасти близкого человека, попавшего в беду!
ДЛЯ ПЕРЕВОДА ДЕНЕГ ДОСТАТОЧНО ЗНАТЬ ТОЛЬКО НОМЕР КАРТЫ ИЛИ МОБ.ТЕЛЕФОН ЕЕ ВЛАДЕЛЬЦА. ИНЫЕ СВЕДЕНИЯ ДАДУТ ПРЕСТУПНИКУ ВОЗМОЖНОСТЬ РАСПОРЯДИТЬСЯ ВАШИМИ СБЕРЕЖЕНИЯМИ ДИСТАНЦИОННО.
ПО ТЕЛЕФОНУ МОЖНО:
СТАТЬ ЖЕРТВОЙ МОШЕННИКА!
ПРИ НАЛИЧИИ СОМНИТЕЛЬНЫХ ПРЕДЛОЖЕНИЙ ОБРАЩАЙТЕСЬ В ПОЛИЦИЮ ПО ТЕЛЕФОНУ - 02 ИЛИ 102 (С МОБИЛЬНОГО)

«Продиктуйте код, чтобы вернуть деньги»

«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.

На звонок ответил как бы сотрудник службы безопасности банка, представился, назвал какую- то распространенную фамилию: Сергеев, Антонов, что-то вроде того. Я рассказал ему, что мне пришло сообщение о блокировке карты, и попросил разобраться.

Сергеев или как его там, не потрудился даже узнать мои паспортные данные или кодовое слово. Зато спросил, часто ли у меня происходят списания и пополнения, на какие суммы, пользовался ли я картой
в незнакомых банкоматах или магазинах в последние дни. Я вспомнил новое кафе, где недавно обедал.

Тогда он сделал вывод: вашу карту считали «цифровым скиммером». Подробно рассказал об этой технологии, звучало все очень правдоподобно.
В конце безопасник объяснил, что активировать карту можно, исключив ее из базы заблокированных. Он попросил назвать номер карты, имя-фамилию, срок действия и три цифры с обратной стороны. Я все продиктовал.

Затем случился апогей моей глупости. Безопасник сказал, что сейчас на телефон придет сообщение с цифровым кодом. Я продиктовал и его. А через минуты две-три пришло сообщение от банка, что с моей карты списаны 30 000 рублей. Тут я, конечно, был шокирован, посмотрел ещё раз на сообщения и понял: они были с разных номеров.

Я позвонил в банк. Там мне сказали, что могут только заблокировать карту, чтобы не было других списаний. Вернуть потерянную сумму теперь если и получится, то нескоро: банк рассматривает заявление до 30 дней».

Мошенники подделывают СМС от банков, надеясь войти в доверие и выманить у жертвы информацию, которая поможет им украсть деньги с ее счета. Они могут использовать шокирующие аргументы - например, написать, что карта заблокирована. Мошенникам выгодно, чтобы человек занервничал, так проще его обмануть. Если вы окажетесь в подобной ситуации, сохраняйте холодную голову, дайте себе время на то, чтобы обдумать информацию.

Если сообщение от банка выглядит подозрительно:

- Внимательно перечитайте текст СМС: оно должно быть понятным, грамотным, без опечаток и «уловок» вроде замены нуля на букву «о», буквы «б» на цифру «шесть» и т.п. Но если сообщение пришло с корректного номера, то не бойтесь того, что оно написано на латинице - банки зачастую пользуются автоматическими сообщениями именно в таком формате.

- Посмотрите на номер для связи с банком: если это настоящее сообщение, то он начинается с 8-800... или состоит из 3-6 цифр. СМС с частного номера - верный признак того, что вам пишут мошенники.

- Прежде чем совершать какие-либо действия, позвоните в банк по номеру, указанному на обороте карты, и уточните, насколько правдива полученная от «специалиста» информация.

- Не переходите по ссылкам, которые указаны в сообщении, пока не убедитесь в его подлинности.

Если вы все-таки перезвонили по номеру, указанному в СМС, не сообщайте трехзначный код с оборота карты и одноразовые пароли, которые приходят в СМС. Это конфиденциальная информация, и ни один банковский сотрудник у вас ее не запросит. К тому же сотрудник банка не может продолжать разговор, пока вы не скажете кодовое слово, указанное вами при оформлении карты.

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 оборотной 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.

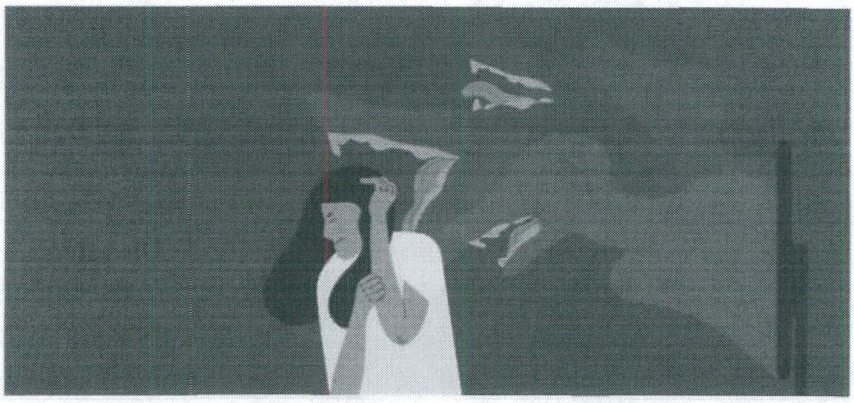
Что делать, если банк не уведомил меня о незаконной операции? Можно ли в таком случае вернуть деньги?

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-код (секретный код на оборотной 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 С\/С-/С\Л/-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 оборотной 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.