Что делать, если вы потеряли карту.

Ищете по всем карманам банковскую карту, а она куда-то исчезла? Разбираемся, как действовать, чтобы пропажа карты не обернулась финансовыми потерями.

Прежде всего удостоверьтесь, что карта действительно потерялась. Возможно, вы забыли ее в другой куртке или оставили на кассе магазина, из которого только что вышли.

Ситуация 1: нет сомнений — карта потерялась или ее кто-то украл.

В таком случае нужно срочно заблокировать карту. Ведь велика вероятность, что мошенники в любую минуту могут расплатиться ею или снять наличные. Заблокировать банковскую карту можно разными способами:

- **По телефону горячей линии.** Универсальный способ. Номер для экстренной связи всегда указан на официальном сайте банка.

Лучше заранее сохранить номер горячей линии банка в мобильном телефоне, чтобы не разыскивать его в экстренном случае.

Оператор службы поддержки попросит назвать паспортные данные, кодовое слово или СМС-код, который пришлет вам на телефон. После этого он заблокирует карту.

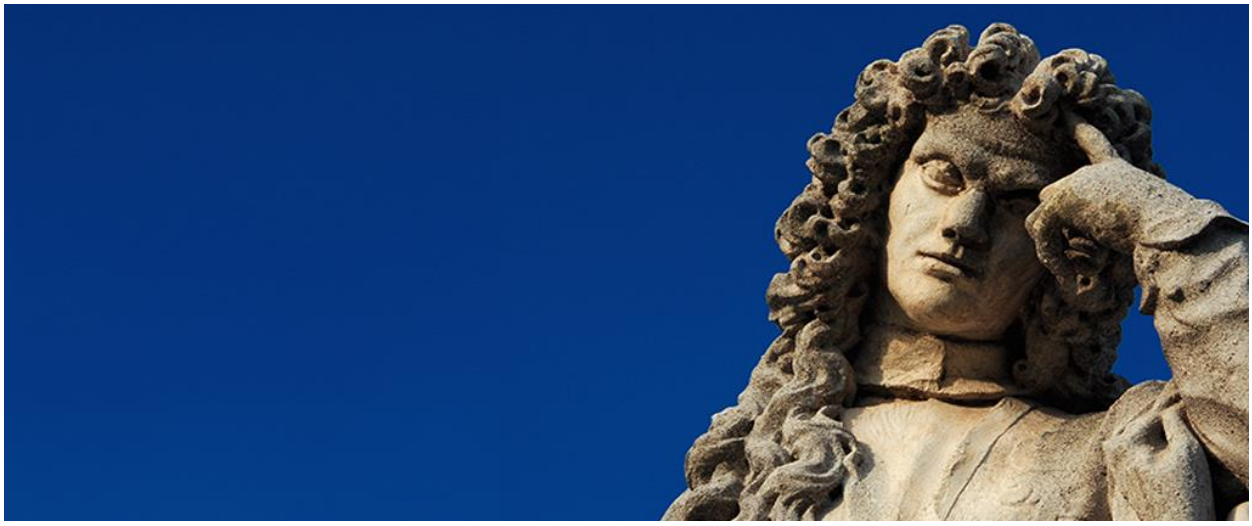
- **Через мобильное приложение.** Самый быстрый способ, если у вас есть доступ к интернету, приложение уже установлено на вашем телефоне и в нем есть опция по блокировке карты.
- **В интернет-банке.** Удобно, если у вас подключен интернет-банкинг и рядом есть компьютер, планшет или смартфон с доступом в интернет. В личном кабинет на сайте банка обычно есть опция «Заблокировать карту». Свое решение надо будет подтвердить кодом из СМС, которое банк вышлет на ваш номер.
- **По СМС.** Некоторые банки используют систему СМС-команд. На короткий номер банка надо отправить кодовое слово (например, «блокировка»). В ответ вы получите код, который надо снова отправить на номер банка, чтобы подтвердить действие. Но лучше

заранее уточнить, предлагает ли ваш банк такую услугу и какие кодовые слова нужно использовать.

- **В отделении банка.** Если вы находитесь рядом с офисом банка или потеряли телефон вместе с картой, пишите заявление о блокировке карты в отделении. Но для этого понадобится паспорт.

Даже после блокировки карты вы по-прежнему можете пользоваться деньгами на счете, к которому она была прикреплена. Снять наличные можно в отделении банка, предъявив паспорт.

Сразу после блокировки карты вы можете оставить заявку на выпуск новой.



Ситуация 2: кажется, карта осталась дома.

Если вы все же надеетесь найти карту и почти уверены, что она лежит где-то дома или на работе, то вам могут подойти другие варианты действий:

- Временная блокировка карты. Некоторые банки предлагают услугу временной блокировки: если карта найдется, вы сможете ее разблокировать и вам не придется тратить время на перевыпуск новой карты. Если же карта действительно утеряна, то ее можно будет закрыть. Услуга временной блокировки может быть доступна через мобильное приложение, онлайн-банк или через оператора горячей линии.
- Нулевой лимит по любым операциям. Это альтернативный вариант: карта вроде бы и активна, но ей нельзя ничего оплатить или перевести деньги на другой счет. Обычно установить нулевой лимит по операциям можно через мобильное приложение, онлайн-банк или через оператора горячей линии. И после этого продолжить спокойно искать карту.

Стоит заранее выяснить в своем банке, можно ли временно блокировать карту и менять на ней лимит. Если окажется, что ваш банк таких опций не предлагает, придется каждый раз взвешивать риски и решать, стоит ли немедленно блокировать карту насовсем или все же подождать и поискать ее.

Карта так и не нашлась. Можно ли ее восстановить?

Если вы так и не нашли карту, но намерены и дальше пользоваться счетом, к которому она привязана, карту нужно перевыпустить. Это занимает в разных банках от 1 до 10 дней.

Подать заявку на перевыпуск можно в отделении банка или через онлайн-банк.

Некоторые банки взимают плату за досрочный перевыпуск — от 100 рублей и выше, в зависимости от типа карты.

Новая карта будет привязана к прежнему счету, но номер и ПИН-код у нее будут новыми.

Если вы не хотите пользоваться прежним счетом, то просто снимите с него деньги в отделении и закройте его.

Сегодня необязательно носить с собой карту, чтобы ею расплачиваться. Сервисы вроде Apple Pay и Android Pay позволяют платить с помощью смартфона. В них применяется биометрическая идентификация, которая считается более надежной, чем ПИН-код или код из СМС.

Если вы потеряли кредитную карту, по которой у вас есть задолженность, то лучше ее перевыпустить. Ведь вносить платежи по кредиту все равно нужно, даже если карта исчезла. Пока ждете новую карту, гасить задолженность придется в отделении банка через кассу или другим способом, который указан в вашем кредитном договоре.

Что делать, если мошенники уже успели украсть деньги с карты, пока я ее не заблокировал?

Если будете действовать быстро, у вас есть большой шанс вернуть похищенное. Вы можете опротестовать операцию по карте, которую совершили мошенники. Но сделать это нужно не позднее следующего дня после того, как получите от банка уведомление об операции.

Если вы уложитесь в этот срок, банк вернет деньги. Правда, перед этим он должен будет убедиться, что вы не нарушили правила безопасности при использовании карты. Например, что вы сами не сообщили преступникам данные своей карты или не написали ПИН-код прямо на карте.

Как контролировать все операции по карте?

Чтобы не дать шанса мошенникам украсть ваши деньги, внимательно отслеживайте все операции по картам. Банк обязан уведомлять вас обо всех платежах — в вашем договоре прописано, каким способом он должен это делать.

Лучше всего подключить СМС-оповещения. Тогда вы сразу заметите списания, которые вместо вас сделал кто-то другой, и сможете оперативно позвонить в банк. Многие банки

берут плату за СМС-информирование, но стоит оценить все риски и принять решение, что важнее.

Стандартный и обычно бесплатный вариант — письма об операциях по электронной почте. Но он требует от вас дисциплины — придется не реже раза в день внимательно проверять письма от банка.

Некоторые банки также предлагают новую услугу — push-уведомления через мобильное приложение. Это тоже бесплатно и удобно — такие уведомления не засоряют память телефона и почту. Но для их получения на телефоне постоянно должен быть подключен интернет.

Отследить операции по карте вы также можете через мобильное приложение или онлайн-банк. Всегда можно получить выписку по счету в отделении банка и иногда через банкомат. Если у вас украли карту, имеет смысл перепроверить все последние платежи.

Какие банковские реквизиты можно и нельзя сообщать другим.

Продавая старую технику на сайте объявлений, Екатерина чуть не лишилась денег на счете. Мошенник под видом покупателя пытался выведать у девушки не только номер банковской карты, но и срок ее действия — якобы для перевода оплаты за товар.

В отличие от большинства аферистов хитреца не интересовали три секретные цифры с обратной стороны карты. И поэтому Екатерина едва не поверила ему, но настояла на том, что номера карты достаточно для перевода. И это спасло ее сбережения.

Разбираемся, какие реквизиты можно сообщать другим, а какие нельзя, и почему.

Какие банковские данные безопасно называть посторонним?

Все зависит от того, зачем у вас их спрашивают:

Чтобы перевести вам деньги

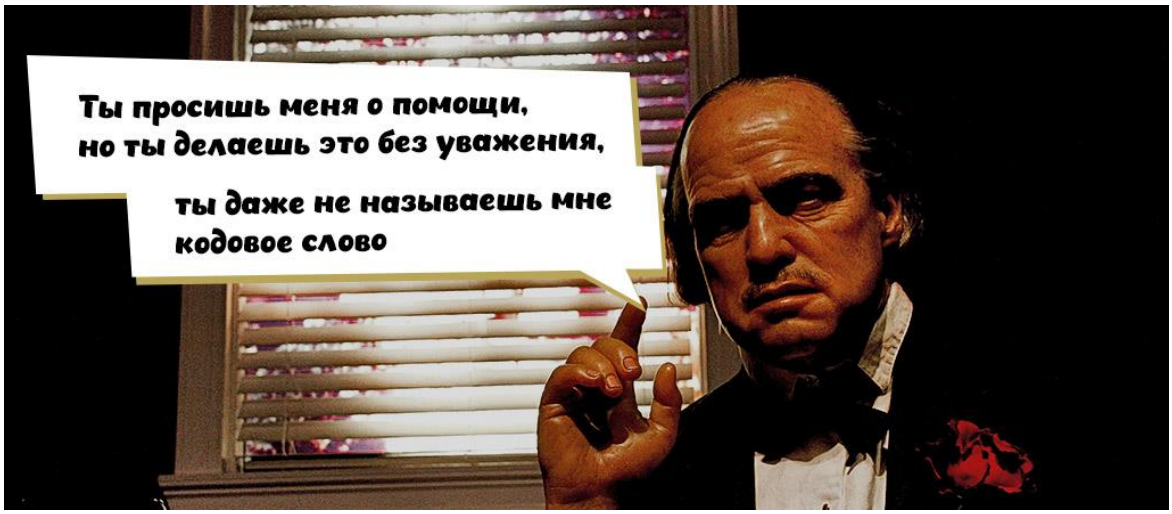
В этом случае вы можете без опаски сообщить отправителю:

- **Название банка и номер телефона, к которому привязан счет**. В большинстве случаев этих данных достаточно для перевода. Они позволят другому человеку мгновенно перекинуть вам деньги, например через Систему быстрых платежей.
- **Номер банковской карты**. Он расположен на ее лицевой стороне и обычно состоит из 16 цифр. Зная этот номер, человек сможет отправить вам деньги через приложение другого банка, терминал или банкомат. Называть номер карты безопасно, если вы не сообщите вдобавок другие реквизиты.
- **Номер расчетного счета**. Он состоит из 20 цифр. Его можно найти в своем онлайн-банке или запросить в отделении банка по паспорту. Переводы по номеру счета предпочитают организации — например, когда оплачивают работу фрилансеров. Дополнительно они запрашивают реквизиты банка получателя — БИК, корреспондентский счет — их тоже можно называть без риска для себя, ведь эти данные общедоступны и не открывают доступ к вашим накоплениям.

Мошенник не сможет вывести деньги с ваших счетов, зная лишь название банка, ваш телефон, номер карты или счета. Но будьте осторожны: аферисты часто используют эти данные в многоступенчатых схемах обмана.

Например, преступники звонят от имени «службы безопасности банка» или даже «отдела расследования полиции», обращаются по имени-отчеству и называют номер карты. Так они стараются внушить доверие, а затем убеждают перевести деньги на «безопасный» — на самом деле мошеннический — счет.

Поэтому никакую информацию о своих счетах и картах не стоит передавать другим без надобности. И ни в коем случае не публикуйте свои персональные данные и банковские реквизиты в открытом доступе, например в соцсетях. Ведь мошенники внимательно их изучают.



Чтобы прояснить ситуацию с банком.

Предположим, вам на карту неожиданно пришли деньги, и вы не знаете, кто и зачем вам их отправил. Пытаясь разобраться в ситуации, вы звоните в банк.

Вначале сотрудник должен убедиться, что это действительно вы, а не мошенник. Для этого он спросит ваше ФИО, номер паспорта, а также может уточнить:

- **Последние четыре цифры номера карты**. По ним он быстро найдет ее в системе, чтобы разобраться в ситуации. Будьте внимательны: диктовать нужно именно последние цифры длинного номера с лицевой стороны карты.
- **Кодовое слово.** Вы указываете его, когда подписываете договор с банком.

Если вы сами обращаетесь в банк, то лучше звонить по официальному номеру, указанному на его сайте или на обороте карты. В таком случае можно без риска сообщать оператору информацию, которую он запрашивает.

Но будьте осторожны, если вам внезапно звонят из банка и просят уточнить конфиденциальные данные. Не теряйте бдительность: даже когда у вас на телефоне высвечивается знакомый короткий номер банка — он может оказаться подменным. Всегда лучше положить трубку, самостоятельно набрать номер горячей линии и прояснить ситуацию.

Какие банковские данные нельзя никому сообщать и почему?

Есть данные, которые сотрудники банков никогда не спрашивают, — если кто-то пытается их у вас выведать, вы точно столкнулись с мошенниками. Важно всегда держать в секрете:

- **Три цифры с оборота карты**. CVV (Card Verification Value) или CVC (Card Validation Code) код. Эти три цифры должны быть известны только вам. Обычно их надо вводить при оплате покупок в интернете. Назовете эти цифры кому-либо вместе с реквизитами карты — по сути, дадите зеленый свет мошенникам, которые с радостью пошопятся за ваш счет.
- **Пароли и коды из банковских уведомлений**. Банк рассылает секретные одноразовые коды и пароли для подтверждения ваших операций или входа в личный кабинет. Это дополнительная защита ваших счетов от мошенников. Сообщить постороннему эти цифры — все равно что отдать вору ключи от квартиры, где деньги лежат.

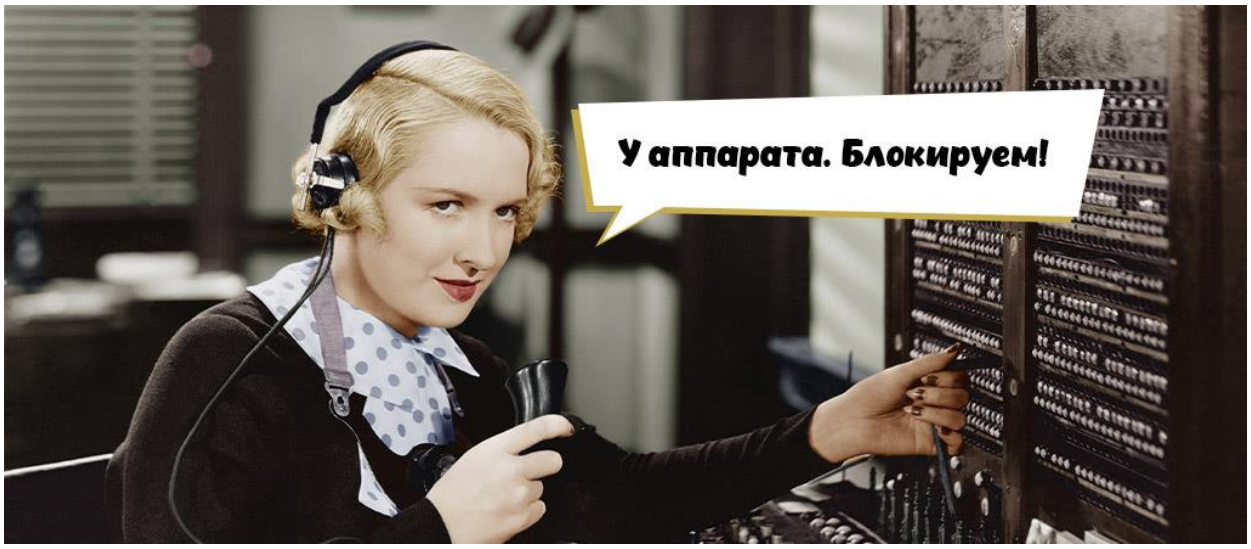
«Мне во ВКонтакте написала давняя знакомая. Сказала, что потеряла мой номер и попросила его напомнить. Я напомнила. И тут она попросила выручить ее: она что-то покупала, и продавец должен был скинуть ей код подтверждения...»

Будьте бдительны, не наступайте на чужие грабли!

- **Срок действия карты.** Иногда для онлайн-покупок по карте не нужен ни CVV/CVC код, ни пароли и коды из СМС и push-уведомлений от банка — достаточно номера карты и срока ее действия. Поэтому его тоже нельзя никому называть. Настоящие сотрудники банка и сами могут его проверить.
- **ПИН-код карты.** Держите его в секрете, не пишите на карте и не храните рядом. Если мошенник ее украдет, то снять все деньги со счета для него не составит труда.

Чтобы выманить у вас конфиденциальные данные, аферисты используют уловки социальной инженериии фишинг. Никогда не вводите данные карты на незнакомом сайте — вначале убедитесь, что он безопасный.

Если вы сообщили преступникам конфиденциальную информацию и лишились денег, банк вам ничего не компенсирует. Даже неосознанная «помощь» мошенникам считается нарушением правил безопасного использования карты.



Что делать, если уже сообщил мошенникам конфиденциальную информацию?

Срочно блокируйте карту: это можно быстро сделать в мобильном приложении банка или по номеру горячей линии. Так вы отрежете мошенникам доступ к деньгам на счете, и, возможно, они не успеют украсть все ваши накопления.

Если злоумышленники заполучили логин и пароль от вашего личного кабинета на сайте банка, попросите оператора горячей линии немедленно отключить дистанционный доступ к счету. Иначе мошенники смогут не только присвоить все ваши сбережения, но и оформить кредит на ваше имя.

«Нужен был кредит, на крупную сумму. Я подала заявление в несколько банков. В одном отказали почти сразу, я ждала что решат ещё два. Через три дня позвонил мужчина, представился сотрудником одного из вот этих банков. Я подтвердила, что обращалась в его банк, за кредитом. Сотрудник спросил, есть ли у меня их карта. Вроде как — для одобрения кредита нужно внести ее данные в мою заявку...»

Будьте бдительны, не наступайте на чужие грабли!

Затем карту надо будет перевыпустить — тогда ее реквизиты изменятся, а прежние, известные преступникам, станут недействительными. Для онлайн-банка создайте новые логин и пароль.

На всякий случай запросите свою кредитную историю — убедитесь, что мошенники не оформили займы на ваше имя.