

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 инженерии](#) и [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](#). По каким признакам можно сразу разоблачить афериста, вы узнаете из текста [«Как быстро распознать мошенника»](#).

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](#).

Подробнее о том, как действовать, если злоумышленникам все же удалось вывести сбережения с ваших счетов, читайте в статье «[Что делать, если с банковской карты украли деньги](#)».

Разобраться, с помощью каких схем обманщики выманивают чужие данные и сбережения, поможет статья «[Социальная инженерия: почему люди сами отдают мошенникам деньги](#)». Еще больше историй можно найти в разделе «[Грабли](#)».