

## «Получили ваше заявление о закрытии счета. Где хотите забрать деньги?»

Валентина, Череповец

Мне позвонили с какого-то городского номера и сказали, что это из банка. Они получили мое заявление на закрытие счета и хотят узнать, когда и в каком отделении я хочу забрать деньги с этого счета. Я удивилась, потому что такое заявление не писала. И сказала им об этом. Мне по телефону ответили, мол, это кто-то за меня написал и хочет получить мои деньги. Я испугалась: что же делать? Нужно, говорят, поскорее перевести деньги на какой-то безопасный банковский счет. Дальше сотрудник попросил меня сказать ему полный номер карты, к которой привязан мой счет, чтобы перевести деньги. Стала искать карту, но от волнения не смогла быстро ее найти. И говорю: я вам перезвоню, как только ее найду. Сотрудник стал меня запугивать, что надо торопиться или у меня украдут деньги. И спросил, есть ли у меня любая другая карта. Мне стало как-то не по себе, что меня так торопят, я занервничала и положила трубку. Решила, что лучше схожу в отделение банка в соседнем доме и там все спокойно разужнаю. Пришла в отделение, а мне говорят, что это были мошенники.

### Совет эксперта по противодействию мошенничеству:

Мошенники используют самые разные предлоги, чтобы получить доступ к банковскому счету человека и украсть его деньги. Часто обманщики сообщают, что «по карте проводится подозрительный платеж» на крупную сумму. Валентину напугали сообщением «о закрытии счета». Могут появиться и другие легенды о том, как «злоумышленники покушаются на ваши деньги».

Цель мошенников неизменна — выманить конфиденциальные данные: полные реквизиты карты, включая секретный CVC/CVV-код на обратной стороне, а также пароли и коды из СМС. Якобы с помощью этой информации можно будет «обезопасить счет клиента».

Если поверить мошенникам и сообщить секретные данные, которые они просят, то можно лишиться всех денег на счете.

С какими бы тревожными известиями вам ни звонили из банка, не стоит терять бдительности. Имя, отчество и другие персональные данные мошенникам легко раздобыть из открытых источников — например, из соцсетей. Номер, который отображается на телефоне при звонке, может оказаться поддельным.

В любых ситуациях стоит придерживаться основных правил безопасности, чтобы защититься от мошенников:

- Ни под каким предлогом никому нельзя сообщать личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-коды. Банк не вернет деньги, если выяснится, что клиент сам раскрыл конфиденциальные данные.
- Когда звонит сотрудник банка и сообщает об угрозе мошенничества, проблемах с картой или других форс-мажорах, нужно вежливо прервать разговор, положить трубку и позвонить в банк по его официальному номеру. Телефон «горячей линии» банка указан на его официальном сайте и на обратной стороне карты. Номер лучше набирать вручную: если звонили мошенники, то обратный вызов может соединить с ними же.
- Нельзя выполнять никакие инструкции незнакомцев: перезванивать, отправлять СМС на неизвестные номера, переходить по ссылкам из сообщений «от банка», скачивать мобильные приложения по первому требованию. Прежде чем что-то предпринять, стоит взять паузу, позвонить по номеру «горячей линии» и проконсультироваться у оператора. Настоящие сотрудники банка никогда не запугивают и не торопят клиентов.