

«Я звоню из банка, вам придет СМС с официального номера»

Антон, Новосибирск

Звонок с городского номера. Солидный мужской голос басит: я сотрудник службы безопасности банка, мы зафиксировали несанкционированную операцию по вашему счету и несколько неудачных попыток входа в ваш интернет-банк. Я, понятно, напрягся: что делать? Он: я сейчас открою вам резервный счет, чтобы перевести туда ваши деньги, и тогда они будут в безопасности. Только, говорит, перед этим надо провести верификацию, чтобы удостовериться, что это действительно вы. Нужно сообщить номер, срок действия карты и три цифры с обратной стороны. Я не понял: а зачем три цифры? Ведь их нельзя никому выдавать. Он отвечает: сотруднику банка можно. А вдруг вы не из банка, спрашиваю. А он: чтобы вы не сомневались, сейчас вам придет СМС-сообщение с официального номера банка об открытии резервного счета.

И точно — приходит СМС с номера банка, с которого получаю отчеты о платежах и зачислении зарплаты. В нем действительно про резервирование счета, как и говорил безопасник. И еще написан код, который нужно отправить в обратном сообщении. Вот этот код, который указан в СМС, мне не говорите, предупреждает мужик. Он секретный и вы не должны его никому сообщать. Это меня и подкупило: я ему поверил. Ну и продиктовал все реквизиты карты. Он сказал, что сейчас переведет мои деньги на безопасный счет и перезвонит.

Когда положил трубку, на телефон стали приходить уведомления, что с моей карты снимаются деньги. Я сначала подумал, что все в порядке, — это их переводят на тот резервный счет. Но потом вдруг засомневался и решил уточнить, когда и как смогу вернуть их обратно на счет карты? Звоню по тому номеру, с которого мне безопасник звонил, а он недоступен. Тогда набрал номер банка, который написан на карте. А сотрудница сказала, что меня обманули мошенники. Карту заблокируют и перевыпустят, но деньги не вернут, потому что я сам назвал преступнику секретные данные.

Только я не понял, почему тогда мне банк прислал СМС? Оно же на самом деле пришло с настоящего номера.

Совет эксперта по противодействию мошенничеству:

Антон столкнулся с мошенником, который выдал себя за сотрудника банка и рассказал легенду о «резервном счете», чтобы выведать данные карты и украсть с нее деньги.

Чтобы история показалась правдоподобной, аферист оставил на сайте банка заявку на «дистанционное резервирование счета» для бизнеса, указав номер телефона своей жертвы. И на самом деле Антон получил СМС-уведомление от банка для подтверждения этой заявки. В стрессовой ситуации он воспринял сообщение как доказательство слов обманщиков об открытии мифического «резервного счета».

На самом деле не существует никаких специальных счетов, на которых прячут деньги от мошенников.

Для резервирования бизнес-счета через сайт банка предпринимателю обычно достаточно заполнить анкету — указать ФИО, номер телефона и ИНН. Злоумышленник мог раздобыть данные Антона в результате утечки персональной информации или просто вбить ИНН наугад — и подать заявку от его имени. Получив онлайн-запрос, банк сразу же присылает СМС с кодом — его нужно отправить в ответном сообщении, чтобы подтвердить свое намерение завести расчетный счет.

Но банки никогда не присылают СМС для подтверждения подлинности звонков.

Настоящий сотрудник банка может уточнить только полный номер карты и имя владельца, но никогда не потребует срок действия карты, ПИН-код, CVC/CVV-код (три цифры с обратной стороны карты) или коды из PUSH- и СМС-сообщений. Только мошенники просят такие данные — ведь с их помощью можно вывести деньги с карты.

Поскольку Антон нарушил правила безопасности и сам выдал конфиденциальную информацию мошенникам, банк не возместит ему потери. Остается только обращаться в полицию.

Иногда аферисты используют и другую схему — предлагают человеку самостоятельно перевести сбережения на «резервный счет» через онлайн- или мобильный банк и даже через банкомат. Но затем оказывается, что этот «безопасный счет» принадлежит преступникам.

И если клиент банка сам отправит на него деньги, вернуть их тоже будет невозможно.

Если вам сообщают какую-то тревожную информацию о ваших счетах и просят срочно назвать конфиденциальные данные или перевести деньги, не паникуйте и не выполняйте эти инструкции. Лучше всего сразу положить трубку и перезвонить на горячую линию, номер которой указан на обратной стороне вашей карты и на официальном сайте банка. Настоящие сотрудники банка расскажут вам, что делать.