«Назовите код из СМС — иначе отключим ваш номер»

Ольга Алексеевна, Ангарск

На днях мне позвонили с незнакомого номера. Мужчина представился сотрудником моей сотовой компании. Он сообщил, что мой договор на телефонное обслуживание заканчивается и нужно как можно скорее его продлить, иначе я потеряю свой номер. Чтобы не тратить время на поездки в офис, собеседник предложил продлить договор по телефону.

От меня требовалось только продиктовать код из сообщения, которое поступит на мой номер. Якобы этот код заменяет мою подпись в договоре на оказание услуг сотовой связи. У меня на миг возникли сомнения, но «сотрудник» сказал, что времени на раздумья нет – нужно либо сейчас все оформить по его инструкции, либо я должна срочно ехать в головной офис, который находится в областном центре.

И это было даже не давление, а скорее, проявление заботы: собеседник извинялся, что сложилась такая ситуация, и всячески старался помочь. Якобы они должны были предупредить об окончании срока договора заранее, но, видимо, произошел технический сбой, из-за которого теперь приходится все делать в последний момент. Просил прощения за доставленные неудобства.

В итоге я поддалась на уговоры и согласилась продлить договор дистанционно. Дальше мужчина начал называть разные платные услуги, которые якобы были у меня подключены и входили в ежемесячную плату. Пообещал, что отключит их и что теперь, по новым условиям, абонентское обслуживание будет обходиться мне дешевле. Тут как раз мне пришло СМС с кодом, который я назвала своему собеседнику.

Масштаб трагедии я оценила только на следующий день. Хотела перевести деньги своей сестре, но не смогла зайти в банковское приложение. Позвонила на горячую линию банка и узнала, что мой мобильный банк переведен на другой номер телефона, а главное – с моего счета сняли все сбережения и оформили на мое имя кредит.

Совет эксперта по противодействию мошенничеству:

Ольга Алексеевна оказалась жертвой довольно распространенной схемы. Сначала с помощью кода из СМС мошенники получили доступ к ее личному кабинету на сайте оператора связи. Там они настроили переадресацию всех входящих сообщений на свой номер. Затем поменяли пароль от мобильного банка – Ольга Алексеевна уже не могла видеть эти уведомления от банка. А потом злоумышленники сняли все деньги с банковских счетов и набрали кредитов на ее имя.

Мошенники довольно часто действуют от имени различных организаций – банков, государственных учреждений или известных компаний. Меняются лишь легенды, которые помогают аферистам выдать обман за действительность и втереться в доверие жертвы.

Например, в одной из схожих схем звонящие представляются не сотрудниками сотового оператора, а службой безопасности банка. Говорят, что обзванивают клиентов для верификации контактов «на фоне участившихся случаев подмены номеров». Человек должен назвать код из банковского уведомления якобы для подтверждения своего номера телефона. На самом деле этот код подтверждает перевод денег на счет мошенников.

Банки не компенсируют потери клиентам, которые сами сообщили преступникам конфиденциальные данные для доступа к своим счетам или коды для подтверждения операций. Людям остается только обращаться в полицию, а кредит пытаться оспорить через суд.

Многие аферисты – тонкие психологи. Они умеют играть на эмоциях, отвлекать внимание и усыплять бдительность. Подробнее о том, какие методы они используют и как не стать их жертвами, можно узнать из статьи «Социальная инженерия: почему люди сами отдают мошенникам деньги».

Когда незнакомец выходит с вами на связь и пытается выманить какие-то данные, просит назвать секретные коды из сообщений, сразу же прервите такое общение. Самостоятельно свяжитесь с той организацией, от имени которой вам звонили, и перепроверьте информацию. Номера горячих линий обычно указаны на официальных сайтах компаний, а контакты для связи с банками также можно найти на их платежных картах.