«Скажите код — или ваш телефон перестанет работать»

Полина, Архангельск

Я собиралась с дочкой в поликлинику, когда очень некстати зазвонил телефон. Приятная девушка представилась менеджером моего мобильного оператора и сообщила, что у меня истекает срок действия сим-карты. Чтобы не потерять номер, мне нужно перезаключить договор на обслуживание.

Я пообещала заглянуть в офис в ближайшие дни и нажала отбой. Но девушка позвонила снова. Сказала, что я неправильно ее поняла. Продлить срок действия симки необходимо прямо сейчас, иначе номер заблокируют и я больше не смогу им пользоваться. Это можно сделать прямо по телефону. Нужно только назвать код из СМС, который сейчас придет.

Не было времени разбираться, не хотелось опаздывать к врачу. Решила, что не случится ничего страшного, если назову эти цифры. И продиктовала код.

Этого оказалось недостаточно. Собеседнице вдруг потребовались мои паспортные данные. Тут я уже возмутилась — эта информация точно есть у оператора. Я сказала, что мои данные не менялись и их можно найти в старом договоре. Положила трубку и больше не отвечала на ее звонки. Но вопрос, с кем же я все-таки говорила, тревожил меня.

Я внимательно перечитала СМС с кодом, который просила девушка. Там были некий «одноразовый пароль» и «логин» – мой номер телефона. Решила не терять время на догадки и позвонила в техподдержку мобильного оператора.

Сотрудник колл-центра объяснил, что у сим-карт нет срока действия и с подобными просьбами их сотрудники не обзванивают абонентов. А код, который я назвала девушке, был нужен для входа в мой личный кабинет на сайте оператора. Поэтому надо срочно проверить, что изменилось в кабинете после того, как мошенники получили к нему доступ.

Оказалось, что мне установили переадресацию, которую я сразу отменила. Никакие другие услуги обманщики не подключали и никакие мои настройки не меняли. Теперь вот думаю, что еще могли успеть сделать мошенники и стоит ли ждать каких-то последствий?

Совет эксперта по противодействию мошенничеству:

Преступники используют легенду с просроченными сим-картами, для того чтобы настроить переадресацию всех звонков и сообщений человека на свой номер. Так они будут узнавать все секретные коды, которые ему приходят, в том числе от банков. В результате мошенники смогут получить доступ к банковским кабинетам, обчистить счета и даже попытаться оформить кредиты или займы.

Чтобы настроить переадресацию, аферисты стараются получить доступ к личному кабинету человека на сайте мобильного оператора. Для этого им нужны телефон жертвы и код, который ей придет в СМС. Номер Полины мошенники уже знали, а код она сообщила им сама. Дальше преступникам оставалось только подключить нужную им услугу.

Перехватывая сообщения и звонки Полины, преступники могли бы, к примеру, попытаться взломать ее интернет-банк или оформить онлайн-заем на ее имя.

Что делать, если вы оказались в подобной ситуации?

Как можно скорее заблокируйте карты и онлайн-доступ к счетам, которые привязаны к вашему телефонному номеру. Сообщите о мошенниках в свой банк.

Проверьте, какие новые услуги появились на вашем телефонном номере. Отмените все лишнее, в первую очередь переадресацию. Ведь пока взломщикам приходят ваши коды, есть риск, что они доберутся до вашего онлайн-банка, электронной почты, социальных сетей, кабинета «Госуслуг».

Через пять рабочих дней после случившегося запросите свою кредитную историю и посмотрите, нет ли у вас новых кредитов и займов. Как оспорить мошеннические ссуды, если они появились, читайте в статье «На мой паспорт взяли кредит. Что делать?».

Как обезопасить себя на будущее

Никогда не называйте секретные коды посторонним людям. Особенно если вас торопят и запугивают. Лучше положить трубку, самостоятельно позвонить в ту организацию, сотрудником которой представился собеседник, и уточнить информацию. Контакты надежнее взять с официального сайта компании.