«Продиктуйте код и получите выгодный тариф. И долги по кредиту»

Сергей, Барнаул

Сегодня позвонили из моей сотовой компании и сказали, что от меня поступила заявка на перевод номера к другому оператору. Даже не успел ничего ответить, как менеджер предложил выгодный тариф, чтобы я остался.

Новый тариф и правда был очень выгодный, так что я сразу согласился. Но вообще-то я не собирался никуда переходить и никакие заявки не отправлял. Решил уточнить, не могли ли мошенники пытаться забрать мой номер себе.

Собеседник подтвердил, что такое бывает. Сказал, что сейчас придет код — нужно его назвать, тогда подключится новый тариф, а переход в другую компанию аннулируется.

С официального номера оператора пришел код, который я передал собеседнику. Он сказал, что новый тариф подключится в течение получаса. Поблагодарил за то, что пользуюсь их услугами, и попрощался.

Тут же на телефон пришло сообщение, что мой аккаунт на Госуслугах заблокирован из-за подозрительной активности. Чтобы восстановить доступ, нужно перезвонить в службу поддержки по такому-то номеру.

Звонить никуда не стал, решил сначала проверить свои Госуслуги. Ввел пароль, но код на телефон не получил. Посмотрел на сайте телефон их службы поддержки — он не совпадал с тем, что был в сообщении. Да и сообщение само пришло с какого-то непонятного номера.

Похоже, мошенники все-таки угнали мой номер и пытались взломать кабинет на Госуслугах. Благо я вовремя спохватился. Со своим мобильным оператором я уже связался. Но нужно ли еще что-то проверить, могли ли мошенники еще что-то сделать?

Совет эксперта по противодействию мошенничеству:

У преступников была задача — настроить переадресацию звонков и сообщений с телефона Сергея на свой номер. Так они смогли перехватывать все уведомления — не только от Госуслуг, но и от банковских приложений и финансовых сервисов. Чтобы добраться до личного кабинета Сергея на сайте оператора и изменить там настройки, им требовался код. Им удалось его выудить под предлогом смены тарифного плана.

Иногда схема обмана немного трансформируется — абоненту рассказывают, что у него истек срок действия сим-карты и если человек не хочет потерять свой номер, ему нужно срочно назвать код.

Проблему с мобильным оператором Сергей уже решил — отменил переадресацию. Но в первую очередь стоило заблокировать все карты, которые привязаны к телефонному номеру, и сообщить о происшествии в свой банк.

Теперь Сергею как можно скорее нужно связаться со своим банком, объяснить ситуацию и узнать, что происходило со счетами в последнее время. Если мошенники уже вывели деньги, вернуть их будет сложно — банки не обязаны компенсировать ущерб, когда клиенты сами помогают преступникам получить доступ к счетам.

Но не исключено, что сам банк признал операции подозрительными и приостановил их. Например, из-за того, что вход в личный кабинет был из другого города и с нового телефона. Такая блокировка перевода и карты действует максимум два дня. За это время нужно успеть связаться с банком и подать заявление, что операции шли без согласия клиента.

Даже когда никакого ущерба не обнаружилось, но у преступников был доступ к вашему банковскому кабинету, не лишним будет сообщить об этом в банк и перевыпустить карты. Ведь аферисты наверняка узнали их реквизиты.

После этого стоит проверить все другие важные сервисы — в частности, Госуслуги, электронную почту, соцсети. Возможно, преступники успели до них добраться и поменяли пароли, тогда придется восстанавливать к ним доступ.

Но может быть, мошенники еще не взломали аккаунты, ведь одних только кодов из СМС для этого недостаточно. Нужно знать логины и пароли, а нередко еще и контрольный вопрос. Поэтому обманщики используют многоступенчатые схемы, чтобы выведать секретные данные.

Сообщение от «поддержки Госуслуг», которое получил Сергей, тоже было обманом. Госпортал действительно может временно заблокировать аккаунт, например если несколько раз ввести неправильный пароль. Но при этом сотрудники сервиса не обзванивают пользователей и не присылают сообщений с просьбой срочно связаться.

Если бы Сергей набрал номер из сообщения, то попал бы на фальшивую техподдержку. Мошенники начали бы убеждать его, что учетная запись в опасности, и попытались выманить данные для входа в аккаунт.

Добравшись до личного кабинета Сергея на Госуслугах, преступники узнали бы номер его паспорта, СНИЛС, ИНН, адрес регистрации. С помощью этих данных аферисты могли попытаться набрать онлайн-займов.