«Продиктуйте код, чтобы вернуть деньги»

Артем, Казань

Однажды мне пришло сообщение от банка, в котором я получаю зарплату. Текст типа такого: «Карта заблокирована из-за сомнительных операций». Там были почти все мои деньги на тот момент, я сразу перезвонил по номеру, который был в конце сообщения.

На звонок ответил как бы сотрудник службы безопасности банка, представился, назвал какую-то распространенную фамилию: Сергеев, Антонов, что-то вроде того. Я рассказал ему, что мне пришло сообщение о блокировке карты, и попросил разобраться.

Сергеев или как его там, не потрудился даже узнать мои паспортные данные или кодовое слово. Зато спросил, часто ли у меня происходят списания и пополнения, на какие суммы, пользовался ли я картой в незнакомых банкоматах или магазинах в последние дни. Я вспомнил новое кафе, где недавно обедал.

Тогда он сделал вывод: вашу карту считали «цифровым скиммером». Подробно рассказал об этой технологии, звучало все очень правдоподобно. В конце безопасник объяснил, что активировать карту можно, исключив ее из базы заблокированных. Он попросил назвать номер карты, имя-фамилию, срок действия и три цифры с обратной стороны. Я все продиктовал.

Затем случился апогей моей глупости. Безопасник сказал, что сейчас на телефон придет сообщение с цифровым кодом. Я продиктовал и его. А через минуты две-три пришло сообщение от банка, что с моей карты списаны 30 000 рублей. Тут я, конечно, был шокирован, посмотрел ещё раз на сообщения и понял: они были с разных номеров.

Я позвонил в банк. Там мне сказали, что могут только заблокировать карту, чтобы не было других списаний. Вернуть потерянную сумму теперь если и получится, то нескоро: банк рассматривает заявление до 30 дней.

Совет эксперта по противодействию мошенничеству:

Мошенники подделывают СМС от банков, надеясь войти в доверие и выманить у жертвы информацию, которая поможет им украсть деньги с ее счета. Они могут использовать шокирующие аргументы — например, написать, что карта заблокирована. Мошенникам выгодно, чтобы человек занервничал, так проще его обмануть. Если вы окажетесь в подобной ситуации, сохраняйте холодную голову, дайте себе время на то, чтобы обдумать информацию.

Если сообщение от банка выглядит подозрительно

- Внимательно перечитайте текст СМС: оно должно быть понятным, грамотным, без опечаток и «уловок» вроде замены нуля на букву «о», буквы «б» на цифру «шесть» и т.п. Но если сообщение пришло с корректного номера, то не бойтесь того, что оно написано на латинице — банки зачастую пользуются автоматическими сообщениями именно в таком формате.

- Посмотрите на номер для связи с банком: если это настоящее сообщение, то он начинается с 8-800... или состоит из 3–6 цифр. СМС с частного номера — верный признак того, что вам пишут мошенники.

- Прежде чем совершать какие-либо действия, позвоните в банк по номеру, указанному на обороте карты, и уточните, насколько правдива полученная от «специалиста» информация.

- Не переходите по ссылкам, которые указаны в сообщении, пока не убедитесь в его подлинности.

Если вы все-таки перезвонили по номеру, указанному в СМС, не сообщайте трехзначный код с оборота карты и одноразовые пароли, которые приходят в СМС. Это конфиденциальная информация, и ни один банковский сотрудник у вас ее не запросит. К тому же сотрудник банка не может продолжать разговор, пока вы не скажете кодовое слово, указанное вами при оформлении карты.