Смс от лжебанка с вредоносными ссылками

Марина, Геленджик

Каждый месяц бывший муж переводит мне на карту алименты. Как-то вечером мы созвонились, и он сказал, что перевел четыре тысячи. Мне сразу же пришло смс от банка о том, что деньги поступили

Ночью я получила еще одно уведомление от банка, о том, что моя карта заблокирована. Чтобы отменить блокировку, нужно было пройти по ссылке из сообщения. Я нажала на ссылку, и тут мой телефон завис. Такое случается с телефонами, так что это меня не напугало, гораздо больше я волновалась о заблокированной карточке. Телефон перезагрузился, проблема была вроде бы решена, поэтому поговорить с банком о причинах внезапной блокировки я решила позже.

Утром я отвела дочку в сад и пошла к банкомату, хотела снять присланные деньги. Меня ждал сюрприз — денег на карте не было. Я сразу же обратилась в банк и запросила детализацию счета. Выяснилось, что ночью от меня банку поступали смс-команды на перевод средств на непонятные счета в другие города. При этом никаких уведомлений о списании денег и изменении баланса на карте не приходило!

Сотрудники службы безопасности посоветовали написать заявление о несогласии с транзакцией и обратиться в полицию, так как скорее всего, я стала жертвой мошенничества. Команды вместо меня отправлял вирус, заразивший мой телефон. Оказалось, что полученное мной смс о блокировке карты якобы от банка было ложным, и пройдя по ссылке и перегрузив телефон, я загрузила вирусную программу. Она тут же настроила отправку смс на указанный номер с нужным текстом и стала перехватывать входящие смс-уведомления от банка.

Чтобы вернуть пропавшие деньги, банку нужны были доказательства, что деньги переводила не я. В моей ситуации таким доказательством считается заведённое уголовное дело. Я собрала и принесла в полицию все справки и выписки. После того, как дело было открыто, банк около двух недель рассматривал моё заявление, после чего мне вернули деньги на счёт.

Совет эксперта по противодействию мошенничеству:

Подобные программы-вирусы мошенники «вшивают» не только в сообщения от банка, но и в смс с обещанием выигрыша, интригующего контента или в смс якобы от потенциального покупателя, заинтересованного в обмене вашего товара с сайта объявлений на свой. Короткие смс — например, «Смотри, что нашёл в интернете. Это ты на фото?» или «Я по объявлению. Обмен интересен?» — оканчиваются вредоносной ссылкой. Из любопытства пользователь переходит по ней и загружает вирусную программу.

Соблюдайте эти простые правила, чтобы избежать подобных ситуаций

- Настороженно относитесь к любому смс, содержащему ссылку — даже если вы уверены, что оно от банка. Внимательно изучите правила безопасной работы при дистанционном банковском обслуживании на официальном сайте вашего банка. Как правило, банк размещает их в разделе «Безопасность» / «Информационная безопасность». Прочитайте рекомендации и узнайте, какую информацию у вас могут запросить, какого рода смс ваш обслуживающий банк никогда не рассылает и как проверить подлинность тех или иных уведомлений.

- Установите на смартфон и компьютер антивирус.

- «Пробейте» номер, с которого поступило сообщение. Зачастую уже попадавшие в схожую ситуацию пользователи оставляют предостережения о мошенниках на сайтах и форумах.

- Проверьте имя отправителя сообщения, если оно выглядит как уведомление от банка. В названиях лжебанка обычно встречается ошибка.

- Не покупайте телефоны «с рук». На рынке б/у-смартфонов очень высок риск приобрести гаджет с вирусными программами.

- Подключите два канала уведомлений о транзакциях — получайте их не только по телефону, но и по электронной почте.

- Если вы все же перешли по зловредной ссылке и после этого смартфон «завис», из-за чего его пришлось перезагружать, обратитесь в службу помощи банка, переведите средства с карты на безопасный счет и на всякий случай заблокируйте её. Обязательно проверьте телефон на наличие вирусов.