«Ничего не покупала, а деньги списали!»

Виктория, Калуга

Отдыхала в Таиланде этой зимой, нужно было снять деньги с карты. Я по натуре человек недоверчивый, а уж в чужой стране пытаюсь быть бдительной вдвойне. Нашли банкомат международного банка, пока ездили на экскурсию. Делала все, как по инструкции: прикрывала клавиатуру рукой, когда вводила пин-код, мужа попросила подстраховать — там много людей крутилось вокруг.

Вроде бы все прошло хорошо, отдых закончился, прилетели. Дней через пять приходит сообщение о списании со счета около 10 000 рублей, за ним сразу еще почти 14 000 рублей. Это все за какие-то секунды происходит, прямо у меня на глазах. Само собой, я паникую, ничего сообразить не успеваю!

Звоню в банк, блокирую карту, прихожу в себя. Я не имею привычки оставлять реквизиты на незнакомых сайтах, никаких вирусов в телефоне не замечала. В службе безопасности сказали, что с моего счета сделали перевод на другой счет и покупку в магазине Таиланда.

В итоге деньги я, конечно, не вернула, но могла бы потерять гораздо больше, чем 24 000 рублей. Хорошо, что быстро среагировала и заблокировала карту. Все деньги выкачать не успели, но обидно вот так попадаться".

Совет эксперта по противодействию мошенничеству:

Этот случай — классический пример скимминга. Человек использует банкомат со специально установленной мошенниками почти невидимой накладкой со считывающим устройством и ложной клавиатурой. Данные его карты, записанные на магнитной полосе, попадают в руки злоумышленников. Затем мошенник может изготовить дубликат карты — и использовать полученные сведения для покупок.

Как не стать жертвой скимминга?

- Используйте банкоматы, расположенные в отделениях банка. Если вы за границей, лучше выбрать известный международный банк в центре города, что снижает вероятность обмана, но не исключает ее.

- Прикрывайте рукой клавиатуру. Он фальшивых кнопок это не убережет, но защитит от веб-камеры, которую мошенники иногда устанавливают на банкомате, чтобы считать вводимый ПИН-код.

- Обращайте внимание на внешний вид банкомата, картоприемника, клавиатуры. Проверьте, нет ли у банка подвижных или съемных элементов — они могут быть частью считывающего устройства. Лучше всего, когда на банкомате есть «крылья» для клавиатуры — они не дают установить другие устройства. Если на банкомате находятся визуально отличимые части, лучше воспользоваться другим.

- Не храните на карте крупные суммы. Заведите специальную карту для путешествий или снятия наличных: переводите на нее деньги с основного счета через приложение перед походом к банкомату.

- Установите дневной лимит на снятие. Это можно сделать либо в мобильном приложении вашего банка, либо в офисе банка.

- Подключите СМС-уведомления и СМС-авторизацию на все операции. Так вы сможете контролировать списания и быстро заблокировать карту при необходимости.

Что делать, если вы ничего не покупали, а деньги с карты списались?

Как можно скорее позвоните в банк, сообщите о мошеннической операции и заблокируйте карту. После этого оставьте заявление о несогласии с операцией: получив его, банк проведет служебное расследование и решит, возмещать ли ущерб. Если вы соблюдали меры безопасности и обратились не позже чем через сутки после списания, можете рассчитывать на возмещение. Однако если вы сообщили злоумышленникам ПИН-код или код из СМС, деньги вернуть не получится. Также обратитесь в местную полицию, чтобы остановить мошенников.