«Продлим ваш ОСАГО, введите данные карты»

Сергей, Тверь

Перед Новым годом я был в запаре, потерял бдительность и отдал деньги мошенникам. Целыми днями был в разъездах, голова кругом. Поэтому когда на электронку пришло письмо с предложением продлить ОСАГО, я только обрадовался: надо же, какой сервис, помнят обо мне – сам-то чуть не забыл! Сомнений не возникло, ведь мой полис действительно заканчивался, а в письме был указан номер моего автомобиля.

До этого я оформлял страховку только в офисе, но многие знакомые давно покупают электронные полисы. А тут даже заполнять ничего не нужно – только перейти по ссылке из письма, что я и сделал. Ссылка вела на страницу оплаты с логотипом страховой компании, там же были указаны данные моей машины – марка, модель, год выпуска, номер. Сумма была рассчитана вполне правдоподобная. Я ввел реквизиты карты. Когда подтвердил операцию, деньги списались и на почту пришло письмо, а в нем – файл с полисом. Он выглядел, как и прежний на бланке, с номером, датами и всеми данными.

Но через несколько дней я случайно услышал от знакомых о новой схеме развода с ОСАГО и на всякий случай решил проверить свой полис. В базе РСА полис с таким номером нашелся, но только зарегистрирован был на другого человека и в другой страховой. Я внимательно перечитал письмо с предложением продлить страховку и понял, что в спешке не заметил: электронная почта не совпадает с той, что указана на сайте страховщика.

Так что я не только потерял деньги, но еще и спалил данные карты. Даже удивительно, что ее полностью не обчистили. В срочном порядке закрыл ее и заказал новую.

Кроме того, я ездил без страховки, пока не обнаружил подставу. Хорошо, что не попал в аварию, а то не знаю даже, как расплатился бы.

Совет эксперта по противодействию мошенничеству:

В декабре 2021 года был шквал афер с ОСАГО. Отчасти это объясняется тем, что нередко люди откладывают покупку машины на зимние месяцы, когда автодилеры предлагают скидки. И в результате полисы, оформленные при покупке, заканчиваются и продляются тоже примерно в это же время года. На руку преступникам играет и предпраздничная суета, когда люди в спешке могут не заметить признаков мошенничества.

Обычно преступники просто запускают рекламу в интернете с предложением продлить ОСАГО на выгодных условиях или спамят электронную почту и мессенджеры. Но иногда им удается взломать базы страховых компаний или воспользоваться утечкой персональных данных, и тогда они делают автовладельцам персональные предложения. В таком случае в их письмах сразу есть данные и автомобиля, и его владельца.

У получателя складывается впечатление, что это рассылка от настоящих страховых компаний. Если он поверит и перейдет по ссылке из письма или сообщения, то попадет на фишинговую страницу. Если там ввести данные своей карты, мошенники смогут списать не только сумму страховки, но и все деньги с карточного счета.

В подобных ситуациях банк не обязан ничего компенсировать, ведь клиент сам перевел деньги мошенникам и выдал им реквизиты своей карты.

Финансовые решения нельзя принимать в спешке. Всегда внимательно проверяйте адрес электронной почты, с которого вы получили письмо, и ссылку, по которой нужно провести оплату.

Лучше вообще не переходить по ссылкам из рекламы, электронных писем, СМС и сообщений в мессенджерах. Безопаснее зайти на официальный сайт компании, услугами которой вы хотите воспользоваться. В поисковых системах «Яндекс» и Mail.ru настоящие сайты финансовых организаций, многих сервисов и онлайн-магазинов маркируются специальными галочками. Координаты финансовых компаний также можно найти в реестрах Банка России.