

«Внесите предоплату за поездку — вот ссылка»

Анита, Волгодонск

Давно хотели с мамой съездить в Тамань. Наконец-то решились, но из-за пандемии брать билеты на поезд или автобус не рискнули — все-таки слишком много народу, а мама уже в возрасте. Возникла идея забронировать поездку на популярном сервисе по поиску попутчиков.

Я нашла отличное предложение — водитель был готов взять нас с собой за 2000 рублей за двоих и не возражал, если мы будем с собакой. Он сразу одобрил наш запрос на бронирование. Стали обсуждать детали по оплате, переписка по его инициативе быстро перешла в один из мессенджеров — якобы он все время за рулем и удобнее общаться голосовыми сообщениями, а не переписываться через сервис.

Попросил заранее внести предоплату 50%. Говорит, что обычно это через сайт делается, но сейчас там ведутся технические работы. Дескать, можно без проблем перевести деньги по ссылке — и скинул ее. Я перешла, оказалась на платежной странице сервиса (как мне тогда показалось) и ввела данные карты.

Сначала у меня снялась сумма предоплаты, а следом еще две тысячи. Я не поняла, в чем дело, стала звонить водителю, но он не отвечал. Обратилась в техподдержку сервиса — они развели руками, мол, это был мошенник, и они его, конечно, заблокируют. Но компенсировать ничего не смогут. В правилах сервиса указано, что нельзя вносить предоплату, и если кто-то ее просит, то это обман.

Успокаивает лишь то, что на счету было всего три тысячи, и то, что платила специальной картой — я ее использую только для покупок в интернете. Зарплатную хватило ума не светить.

Маме я ничего не сказала, чтобы она не расстраивалась. В результате удалось найти нормального водителя, который не просил предоплату. Правда, чуть дороже вышло, но хоть путешествие не сорвалось.

Совет эксперта по противодействию мошенничеству:

Это отработанная схема социальных инженеров. Мошенник, притворившийся продавцом товара или услуги, скидывает покупателю ссылку на фишинговый сайт.

Эти страницы создают специально, чтобы выманить данные карт пользователей. Они практически полностью копируют дизайн и веб-адрес известных магазинов, сервисов или финансовых организаций. В случае с Анитой сайт был замаскирован под платежную страницу популярного сервиса, где люди ищут попутчиков.

Аферист умышленно перевел общение с официальной площадки в сторонний мессенджер. Это позволило ему обойти защитные механизмы сервиса, которые блокируют отправку подозрительных ссылок пользователям.

После того как Анита ввела на фейковой странице данные карты, включая срок действия и три цифры с оборота, преступник получил доступ к ее счету и смог все с него украсть.

Банк ничего не компенсирует клиенту, который сам сообщил злоумышленникам конфиденциальную платежную информацию или перевел им деньги. Остается только заблокировать и перевыпустить скомпрометированную карту.

Столкнуться с подобной схемой можно на любой крупной площадке, где люди продают друг другу вещи или предлагают платные услуги. Причем мошенник может прикинуться как продавцом, так и покупателем.

Чтобы защититься от обмана, важно всегда следовать правилам кибергигиены:

- Не выводите общение за рамки маркетплейса – например, в мессенджеры или соцсети. Сторонние чаты чаще всего не распознают подозрительные ссылки, в отличие от самих сервисов.
- Всегда проверяйте, настоящий ли перед вами сайт, прежде чем вводить платежные данные. Научиться отличать безопасные страницы от мошеннических поможет статья «Фишинг: что это такое и как от него защититься».

- Не переходите по ссылкам от незнакомцев – они могут оказаться не только фишинговыми, но и вредоносными. Тогда на ваше устройство попадет опасный вирус, крадущий личные данные. Как обезопасить компьютер и смартфон от хакеров, читайте в статье «Как защитить свои гаджеты от мошенников».

- Обязательно читайте правила безопасности сервиса, прежде чем им пользоваться. Если бы Анита это сделала, то знала бы, что на площадке запрещена предоплата, а любые намеки на нее – признак мошенничества.

- Если сайт позволяет проводить оплату, используйте его внутренние механизмы, например сервис «безопасная сделка». В этом случае ваша оплата резервируется на счете площадки и будет перечислена продавцу или исполнителю только после того, как вы получите товар или услугу. Если сделка сорвется, вам вернут деньги.