«Вернем деньги за задержку заказа в «черную пятницу». Назовите остаток на счете»

Динара, Казань

Обожаю скидки и всегда жду «черную пятницу». В этот раз, как только начались распродажи, зашла на свой любимый маркетплейс и назаказывала всякой всячины – косметику, подарки родным на Новый год. Решила и себя порадовать – купила классный фен со скидкой. Заказ должен был прийти через три дня.

Потом получаю уведомление: из-за большого количество заказов доставка задерживается – аж на две недели. Но если новогодние подарки мне не к спеху, то фен был нужен срочно. Мой старый сломался. Зачем указывать нереальные сроки, если понятно, что во время распродажи покупателей будет много?

В обычных магазинах сейчас тоже скидки, так что решила не ждать и отменить заказ через приложение. Бот написал, что передал вопрос сотруднику службы поддержки. Но у них много обращений, поэтому быстро ответить они не смогут. Я честно ждала три часа, а потом не выдержала.

Нашла канал маркетплейса в популярном мессенджере, написала им в комментах все, что про них думаю. И через пару минут мне в личку приходит сообщение от службы поддержки: они предлагают отменить заказ, обещают быстро вернуть деньги и еще начислить 10% бонусами в качестве извинения.

Я обрадовалась – ну хоть какая-то выгода. Мне скинули ссылку на форму возврата. Там нужно было ввести номер карты, имя владельца, срок действия, три цифры с оборота и остаток денег на карте. Якобы все это нужно для идентификации клиента.

Я вбила все данные, которые были на карте. А чтобы проверить баланс, зашла в свой мобильный банк. И вдруг задумалась: зачем маркетплейсу знать, сколько у меня денег на счете? Поскорее стерла из

формы все данные и закрыла сайт от греха подальше. Нет уж, решила, дождусь, пока мне в приложении маркетплейса ответят, как обычно.

Скоро в чате приложения мне действительно написали, что заказ отменили, деньги вернут на карту. Никаких дополнительных данных не спросили.

Но что это было вообще? Кто со мной связался в мессенджере? И могут ли у меня теперь украсть деньги с карты, если я что-то вводила на непонятном сайте, но потом стерла?

Совет эксперта по противодействию мошенничеству:

Преступники всегда активизируются во время «черных пятниц» и других распродаж, потому что люди в спешке и азарте часто теряют бдительность и порой попадаются даже в примитивные ловушки.

Чаще всего мошенники просто создают поддельные сайты магазинов и маркетплейсов. Покупатели вводят там данные своих карт, и преступники их обчищают.

В случае с Динарой обманщики решили действовать хитрее – сыграть на том, что во время ажиотажа продавцы часто не справляются с валом заказов. Недовольные покупатели заходят в соцсети, мессенджеры магазинов и маркетплейсов и жалуются на задержки заказов в комментариях к постам. Там их и находят аферисты.

Клиентам кажется естественной ситуация, когда техподдержка продавца спешит на помощь. Но в мессенджере крайне сложно проверить, кто именно обращается к вам от имени техподдержки. Мошенники просто ставят логотип магазина себе на аватар, чтобы вызвать доверие у покупателя.

Дальше они действуют по классической схеме – присылают ссылку на фишинговую страницу и просят ввести полные реквизиты карты, в том числе срок действия и три цифра с ее оборота. Зная эти данные, преступники могут списать деньги со счета.

У Динары аферисты хотели выяснить еще и остаток на карте. Видимо, они хотели обнулить ее счет за одну операцию. И в то же время опасались, что, если попробуют списать слишком большую сумму, платеж не пройдет. А клиент получит уведомление о несанкционированной операции и успеет заблокировать карту.

Хотя девушка не закончила оформление возврата, а данные карты стерла, есть вероятность, что преступники успели их зафиксировать. Поэтому риск, что у нее украдут деньги, исключить нельзя. Динаре лучше срочно заблокировать карту и перевыпустить ее.

Как не потерять деньги во время онлайн-шопинга?

- Оформлять и отменять заказы можно только через официальный сайт либо приложение интернет-магазина или маркетплейса. Если продавец предлагает перейти в сторонний мессенджер, это повод насторожиться.

- Не открывайте ссылки от неизвестных отправителей. Всегда проверяйте адрес сайта, где нужно вводить данные карты. Даже если просто переходите из маркетплейса на страницу банка.

- Делайте заказы только на ресурсах с безопасным соединением. Их адрес начинается с https://, а рядом стоит значок закрытого замка.

- Для онлайн-шопинга лучше завести отдельную карту и переводить на нее деньги непосредственно перед оплатой покупок.

- Если вы все же попались на уловки обманщиков – подайте заявление о мошенничестве в полицию. Также свяжитесь с настоящей техподдержкой маркетплейса по контактам с его официального сайта, расскажите о ситуации. Магазин не отвечает за действия злоумышленников и не вернет вам похищенные деньги, но может предупредить других покупателей об опасности.