«Переведи с карты 1 рубль, чтобы получить приз»

Зинаида, Мурманск

Участвовала в конкурсе в соц.сети Instagram около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала кроссовки, написала организаторам, после чего мне предложили оплатить доставку в размере 450 р.

После этого мне предложили перейти по ссылке, где нужно было оплатить сумму в 1 р. (они это объяснили тем, что такие конкурсы сопровождаются налогами, и чтобы их не платить, участники вносят символическую сумму в размере 1 р.).

В сумме платежа я указала 1 р., после оплаты с карты у меня списалась 21 000 р. С данным инцидентом разбирается прокуратура. Будьте внимательны люди, и не будьте такими доверчивыми, как я!

Совет эксперта по противодействию мошенничеству:

Конкурсы в социальных сетях очень популярны, и мошенники могут использовать их в качестве приманки для доверчивых пользователей.

Сначала киберпреступники прислали участнице конкурса ссылку на фишинговый сайт. А затем попросили перевести через него 1 рубль, чтобы узнать секретную информацию о ее банковской карте: номер, срок действия, код проверки подлинности карты (три цифры на обратной стороне — CVV/CVC), имя и фамилию владельца.

Мошенники рассчитывают на то, что предоплата всего лишь в 1 рубль не испугает человека и он охотно согласится перевести деньги в обмен на желанный приз.

Чтобы не попасться на удочку мошенников, всегда следуйте правилам безопасности:

- Не доверяйте конкурсам, в которых вы должны что-либо оплатить, — это явный признак мошенничества. На то они и конкурсы, чтобы разыгрывать подарки бесплатно.

- Не спешите переводить деньги неизвестным получателям по первому требованию и никогда не переходите по ссылкам от незнакомцев.

- Убедитесь, что аккаунт организатора конкурса не фейковый. Нередко мошенники создают поддельные страницы организаций и медийных лиц, а затем проводят «конкурсы» от их имени. Некоторые известные личности и компании проходят верификацию (у названия страницы появляется синяя галочка), чтобы их читатели точно знали, что перед ними настоящий аккаунт. Но далеко не все блогеры проходят эту процедуру. Ссылки на настоящие аккаунты организаций в соцсетях можно найти на их официальных сайтах.

- Не вводите данные банковской карты на сомнительных сайтах. В адресной строке безопасного сайта есть значок в виде закрытого замка, а ссылка начинается с https://.

- Проверяйте сертификат безопасности сайта. Для этого нажмите на значок замка и в открывшемся окне выберите «Просмотр сертификатов». Нужно убедиться, что сертификат выдан именно этому сайту, и срок его действия не истек.

- Установите антивирусы на все гаджеты, которыми пользуетесь, чтобы защититься от вредоносных сайтов и программ.

- Не храните крупные суммы денег на карте, которую используете для повседневных трат. Лучше завести отдельную карту для покупок в интернете и каждый раз перечислять туда нужную сумму.

- Если вы столкнулись с подозрительным конкурсом в социальной сети, пожалуйтесь ее администрации.