«Отсканируйте QR-код для перевода денег за ваш товар»

Григорий, Саранск

Продавал синтезатор на популярном сайте объявлений. Мне в чат пришло сообщение, что мой товар купили с доставкой. И следом QR-код — типа нужно перейти по ссылке и ввести данные карты, на которую хочу получить оплату.

Я отсканировал код телефоном с экрана компьютера, открылась страница с описанием моего синтезатора, ценой и тут же — форма для заполнения реквизитов карты.

Начал уже вводить, но тут смотрю: нужно написать не только номер, но еще и срок действия, и три цифры с оборота. Внимательнее посмотрел на страницу и тогда только заметил, что это фейк: в адресе сайта ошибки, дизайн тяп-ляп. Хорошо, что вовремя заметил.

Совет эксперта по противодействию мошенничеству:

Мошенники рассчитывали на то, что Григорий введет данные карты на поддельном сайте и тем самым откроет им доступ к счету, с которого можно будет украсть все деньги.

Преступники зашифровали фишинговую ссылку в картинку с QR-кодом, чтобы обойти защитные механизмы сайта объявлений. Обычно служба безопасности онлайн-площадки блокирует сомнительные ссылки, но публикацию картинок не запрещает. Ведь пользователям нужно обмениваться фотографиями товаров.

Нередко мошенники предлагают перенести обсуждение деталей сделки в сторонний мессенджер — и там могут прислать ссылку или QR-код для перехода на фейковую страницу.

На фишинговый сайт могут попытаться увести как покупателя, который должен ввести данные своей карты для оплаты, так и продавца, которому на карту должны поступить деньги.

Чтобы продажа или покупка товара на сайте объявлений не обернулась для вас убытками, следуйте правилам кибербезопасности:

- Общайтесь с покупателями и продавцами только во внутреннем чате сайта объявлений, где блокируются фишинговые ссылки. А оплату лучше проводить через сервис «безопасная сделка», которую предлагают крупные онлайн-площадки.

- Насторожитесь, если вам предлагают перейти в сторонний мессенджер или на какую-либо внешнюю страницу, «чтобы заполнить форму для перевода», в том числе по QR-коду.

- Всегда проверяйте сайт, прежде чем вводить на нем какие-либо данные. Убедитесь, что это не фишинговая страница, замаскированная под портал объявлений, онлайн-магазин или службу доставки.

- По телефону или в личных сообщениях никому не сообщайте полные реквизиты своей банковской карты, включая срок действия и три цифры с обратной стороны, а также пароли и коды из уведомлений от банка. Для перевода от одного человека другому достаточно только номера карты.

- Заведите отдельную карту для покупок в интернете и не храните на ней крупные суммы. Тогда, даже если мошенники получат доступ к счету, им не удастся лишить вас всех сбережений.