«Хочу купить ваш товар! Давайте обсудим детали в мессенджере»

Елена, Москва

Иногда меня спрашивают, безопасно ли проводить сделку через сайт объявлений. Так вот рассказываю, что мошенники делают. Чтобы никто не попался!

Короче, я продавала компьютер через известный портал объявлений. Нашелся покупатель и предложил детали сделки обсудить не в чате самого сайта, а в мессенджере. Типа так удобнее. Обсудили. Он пишет: да, все устраивает, сейчас буду оплачивать, нужно ввести номер вашей карты для перевода. И кидает ссылку, где я должна указать номер.

Открываю ссылку, там страница с описанием товара и обычная форма, куда вводить номер карты, срок действия и секретный код. Я уже начала искать карту, а сама думаю: стоп! Почему я должна все номера с карты там вводить, это же он покупает, а не я?

Посмотрела внимательнее на адрес ссылки, которую мне скинули, а он какой-то странный, вроде название сайта объявлений, но с удвоенной первой буквой. Сама страница очень похожа на настоящую, но все равно как будто что-то не то.

Короче, вовремя дошло, что меня пытаются обмануть. Этот покупатель просто сделал зеркало сайта и хотел, чтобы я ему слила все данные карты. Не на ту напал! Будьте внимательны!

Совет эксперта по противодействию мошенничеству:

Суть этой схемы в том, что мошенник уводит пользователя из чата безопасной онлайн-площадки для сделок — сервиса объявлений, доставки товаров или другого известного сайта. Обманщик предлагает перейти в один из мессенджеров, потому что там якобы «будет удобнее обсудить детали сделки». На самом деле он просто боится, что служба безопасности сервиса отследит его и помешает провернуть аферу.

Использовать такую схему может не только покупатель, но и продавец. Мошенники создают фальшивые объявления, и как-

только появляется потенциальный покупатель, они предлагают продолжить общение за пределами сервиса.

Затем мошенник в мессенджере присылают фишинговую ссылку. Она может быть замаскирована под страницу подтверждения покупки сервиса, на котором было опубликовано объявление, или под сайт для доставки товара. С первого взгляда отличить фейковую страницу от настоящей довольно сложно: дизайн совпадает с оформлением знакомого сервиса, указаны верная информация о товаре, адрес доставки, контактные данные, которые мошенник заранее выяснил у пользователя.

На поддельной странице предлагается ввести полные реквизиты банковской карты, чтобы якобы получить деньги за товар, оплатить покупку или доставку. Если человек введет полные данные карты, включая трехзначный код с обратной стороны, то мошенник сможет украсть деньги с его счета.

Иногда ссылка содержит опасный вирус, который крадет данные с гаджета.

Чтобы не попасться на обман, следуйте правилам финансовой безопасности:

- Не переходите по ссылкам из писем и уведомлений от незнакомцев.

- Насторожитесь, если при оформлении покупки на популярном сайте вам предлагают перейти на стороннюю площадку. Лучше проводить все расчеты внутри сервиса: многие из них предоставляют услугу «безопасная сделка». К тому же система безопасности сайта блокирует вредоносные ссылки.

- Не вводите данные карты на подозрительных страницах. Подробнее о том, как отличить фейковый сайт от безопасного, читайте в тексте «Фишинг: что это такое и как от него защититься».

- Установите антивирусы на все гаджеты, которыми пользуетесь.

- Заведите отдельную карту для шопинга в интернете и не храните на ней много денег. Кладите на эту карту нужную для покупки сумму непосредственно перед оплатой. Тогда в случае мошенничества вы потеряете только ее, а не все свои сбережения.