Псевдопокупатели в интернете и фишинг данных карты для «предоплаты»

Евгений, Ростов-на-Дону

Год назад я разместил в интернете объявление о продаже сельхозоборудования. Через некоторое время нашелся покупатель, расспросил о товарах, мы быстро сошлись в цене. С доставкой тоже уладили — за техникой решено было отправить транспортную компанию. Покупатель был из другого региона, так что мы договорились, что он переведёт деньги мне на карту.

Я сообщил номер карты для перевода, в дополнение к которому покупатель запросил у меня паспортные данные, сказал, что нужно для компании по грузоперевозкам. Я решил, что такое вполне возможно, и отправил ему свои данные.

Через пятнадцать минут последовал звонок, мужчина представился сотрудником банковской службы безопасности. Он сообщил, что на мой счет должна поступить крупная сумма, для которой требуется подтверждение транзакции, и запросил код подтверждения из смс, которое присылает банк при проведении платежа.

Я проверил экран телефона — сообщение действительно поступило, в нём была информация о какой-то регистрации и цифры. Я продиктовал данные из смс «работнику» службы банка, а спустя пару минут на мой телефон «посыпались» сообщения о списании средств— пополнения каких-то телефонных счетов и мобильные переводы на чужие карты.

Совет эксперта по противодействию мошенничеству:

Евгений — один из многих попавших в эту ловушку продавцов. Цель мошенника — получить данные, которые дадут доступ к деньгам на карте продавца. В истории Евгения злоумышленник, уже имея на руках номер карты, заполучил разовый пароль из сообщения от банка, чтобы повторно зарегистрировать карту в системе онлайн-банкинга. Продиктованный пароль служил кодом для восстановления доступа в личный кабинет. Получив такой доступ, мошенник может

управлять не только счётом карты, номер которой он знает, но и всеми остальными счетами клиента.

Иногда человек сам передаёт доступ к интернет-банку, через банкомат, — совершает под диктовку необходимые операции и сообщает пароли из приходящих от банка смс. Аферисты тут же входят в личный кабинет и переводят средства на свои счета.

Главный признак того, что связавшийся с вами покупатель — мошенник, это требование конфиденциальной информации для проведения платежа: пин-кода, пароля из смс, трёхзначного кода (CVV2 или CVC2).

Для перевода денег на карту достаточно указать номер карты и ФИО держателя. Если платёж проводится через другой банк, могут понадобиться и другие реквизиты, однако персональная информация к ним не относится. Кроме того, некоторые банки позволяют переводить деньги по номеру телефона — система сама найдёт данные клиента, к которым привязан номер.

Также следует насторожиться, если потенциальный покупатель категорически отказывается покупать с помощью наложенного платежа и торопится завершить сделку — готов сразу оплатить, не расспросив при этом о товаре и его свойствах, причинах продажи.