«Ваш товар купили, перейдите по ссылке»

Валерий, Нижний Новгород

Продавал свой старый планшет через приложение известного сайта объявлений. Пришло смс, что кто-то купил планшет и уже перевел деньги. Там была написана сумма 10 000 р и ссылка. Я жму по ссылке, открылась страница сайта, на котором я постил информацию о продаже. Там мое объявление с описанием и фото планшета, и пометка, что поступила оплата. Но еще была фраза внизу, что мне надо установить последнюю версию приложения иначе что-то там пойдет не так. Я нажал «Продолжить».

Дальше были какие-то уведомления, телефон стал глючить, потом появилось сообщение, что был сбой в системе и что надо ввести данные карты, тогда смогу использовать приложение. Я ввел и тут же с карты списались все деньги. Хорошо, что на ней было немного — где-то 130 рублей, не больше. Я позвонил на сайт объявлений и мне сказали, что это были мошенники и, скорее всего, я скачал вирус. И что мой планшет на самом деле никто еще не купил. Очень странная ситуация, пришлось повозиться, чтобы очистить телефон. По итогу я установил себе антивирус, перевыпустил карту, а планшет продал знакомым.

Совет эксперта по противодействию мошенничеству:

Валерий скачал на свой телефон опасный троян, который маскируется под известные сайты и приложения — крупные порталы объявлений, онлайн-магазины, агрегаторы отелей и другие онлайн-сервисы. Вирус ориентирован на устройства на базе Android. С помощью этого трояна кибермошенники преодолевают защитные механизмы мобильного устройства пользователя и выманивают данные его банковской карты. Подробнее о работе трояна можно узнать из обзора.

Вирус собрал открытую информацию с сайта объявлений — описание товара, фотографии, номер телефона Валерия — и прислал ему СМС со ссылкой, которая вела на фишинговую страницу. На ней был логотип сайта объявлений и даже фото планшета, поэтому страница не вызвала у Валерия подозрений. Нажав кнопку «Продолжить», вместо обещанной «новой версии приложения» он скачал троян.

После этого вирус стал забрасывать Валерия тревожными уведомлениями о сбоях в системе. На фишинговой странице Валерий ввел данные своей карты, и они попали к мошенникам, которые смогли вывести с нее деньги.

Чтобы предотвратить кражу денег со своих счетов, необходимо следовать правилам кибергигиены:

- Установить антивирусы на все гаджеты, которыми вы пользуетесь.

- Отключить на гаджетах разрешение на установку приложений из непроверенных источников и не скачивать данные, если ваше устройство предупреждает о риске.

- Не переходить по ссылкам из писем и уведомлений от неизвестных отправителей.

- Не вводить данные карты на подозрительных сайтах.

- Всегда внимательно проверять адресную строку браузера. Адрес безопасного ресурса начинается с https://, и в адресной строке есть значок в виде закрытого замка. Важно убедиться, что перед вами не сайт-клон популярного ресурса. Адрес поддельного сайта может отличаться от адреса настоящего ресурса только парой знаков.