**Уловки фишинг-мошенников**

**Что сегодня может быть проще, чем купить в Интернете понравившийся товар? Совершить такую покупку может даже ребенок или пользователь, не вполне уверенно владеющий навыками работы с персональным компьютером. Это удобно, поскольку не надо тратить время на походы по магазинам, особенно в поисках обычных товаров. Есть немало торговых площадок, которые предоставляют возможность оплаты с использованием банковских платежных карт и доставки товара в любой уголок мира. Но развитие электронной торговли и большое число людей, вовлеченных в данный процесс, не остались незамеченными злоумышленниками. Расскажем о наиболее распространенных способах совершения противоправных действий с использованием торговых интернет-площадок.**

****

**«Предоплата» (обман продавца)**

Суть данного способа заключается в том, что зло­умышленник выступает в роли потенциального покупателя товара. На одной из интернет-площадок с объявлениями он находит продавца и копирует его контактные данные. В дальнейшем ищет данного продавца в мессенджерах или пишет в социальных сетях, представляясь якобы покупателем с указанной торговой площадки. В ходе переписки, злоумышленник сообщает, что товар ему понравился и он хочет его приобрести, в связи с чем уже якобы совершил предоплату. Для того, чтобы получить данные средства, злоумышленник высылает продавцу ссылку на поддельную страницу (зачастую она может выглядеть как один из разделов официального сайта интернет-площадки или банковского учреждения), где продавцу нужно ввести номер своей карты, имя держателя, срок действия, CVV-код, указанный на оборотной стороне карты. После получения конфиденциальных сведений злоумышленник совершает хищение средств.

**«Доставка» (обман покупателя)**

Злоумышленник намеренно размещает объявление на интернет-площадке о продаже товара по крайне выгодной цене. После того, как потенциальный покупатель начинает вести переписку во внутреннем чате площадки, злоумышленник под различными предлогами убеждает его продолжить общение в мессенджере или социальной сети. Во время общения мошенник уговаривает покупателя внести предоплату или оформить доставку и, чтобы развеять сомнения покупателя, сообщает о якобы новой услуге удержания (холдирования) средств, которая появилась на торговой площадке (якобы если доставка не произойдет, то торговая площадка автоматически вернет средства на карту). При этом покупателю высылается ссылка на поддельную страницу, которая имитирует официальную страницу торговой площадки или интернет-банкинга, где нужно ввести данные карты, чтобы совершить предоплату. В качестве данных карты покупателя просят заполнить номер карты, имя держателя, срок ее действия, CVV-код (3 цифры на оборотной стороне карты). В некоторых случаях злоумышленник может попросить назвать проверочный код из СМС-уведомления банка. Как только пользователь вводит данные своей карты, с нее списываются деньги, посылка не приходит и средства не возвращаются.

****

**«Возврат средств» (обман покупателя или продавца)**

После того как злоумышленник использовал одну из описанных выше схем для хищения денежных средств, спустя некоторое время он вновь связывается с потерпевшим (в мессенджерах или социальный сетях), но в этот раз представляется сотрудником торговой площадки или транспортной компании и сообщает, что произошла ошибка и деньги списаны случайно. После этого злоумышленник высылает потерпевшему ссылку на поддельную страницу возврата средств, где нужно вновь ввести данные своей карты и сумму, которую ему якобы должны вернуть. После того, как указанная информация вводится потерпевшим, с его счета повторно списываются деньги.

 *Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет, следует вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки. Ведя общение с пользователем, стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность).*

 *Очень внимательно надо относиться к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком. Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты.*

 *Важно уточнить у собеседника номер телефона, если он не указан в объявлении, а потом позвонить на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку.*

 *Используйте отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии.*

 *Избегайте перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если вам прислали такую ссылку, прежде чем по ней перейти, внимательно проверьте доменное имя (адрес ресурса). Сделать это можно, отыскав в интернете официальный сайт и сверив написание доменного имени. Отличие в одну букву или символ свидетельствует о том, что перед вами ссылка на поддельный ресурс.*



***Если вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо в срочном порядке произвести блокировку карты, позвонив в банк, либо самостоятельно в интернет-банкинге.***

*По информации УВД Брестского облисполкома*