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. Этот процесс обусловлен тем, что большинство людей сегодня все чаще испытывает дефицит свободного времени и тратить его на походы по магазинам, особенно в поисках обычных товаров, стало для многих недоступной роскошью. Кроме этого, купить или продать товар в сети Интернет стало очень просто благодаря огромному числу торговых площадок, которые делают этот процесс максимально быстрым и удобным, предоставляя возможность оплаты с использованием банковских платежных карт и доставки товара в любой уголок мира.

Согласно исследованиям, рынок электронной коммерции в Республике Беларусь ежегодно растёт и вовлекает все новых пользователей. По статистике, только РУП «Белпочта» обрабатывает около 30 тысяч почтовых отправлений в день, при этом подавляющее большинство наших граждан совершают онлайн-покупки именно на белорусских интернет-площадках.

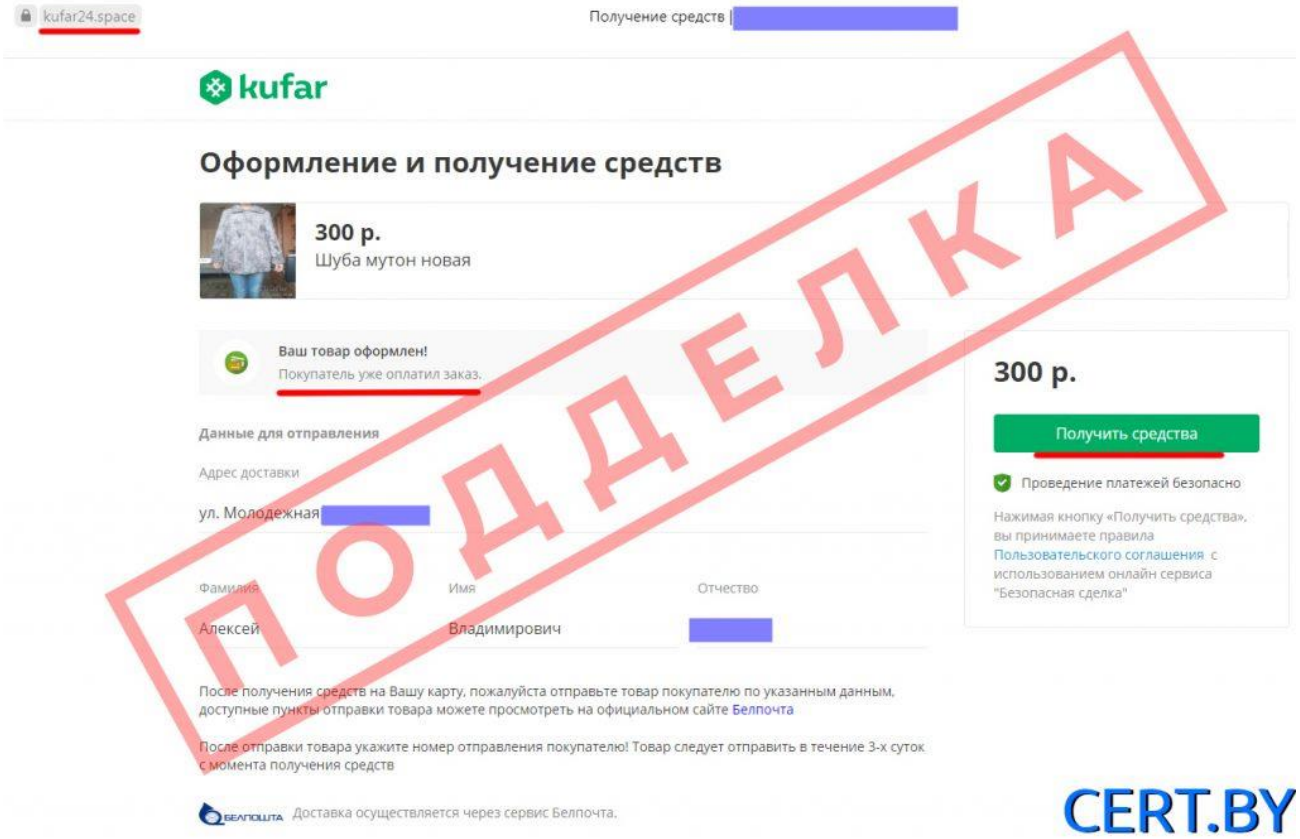
Такое резкое развитие электронной торговли и большое число людей, вовлеченных в данный процесс, не остались незамеченными злоумышленниками.

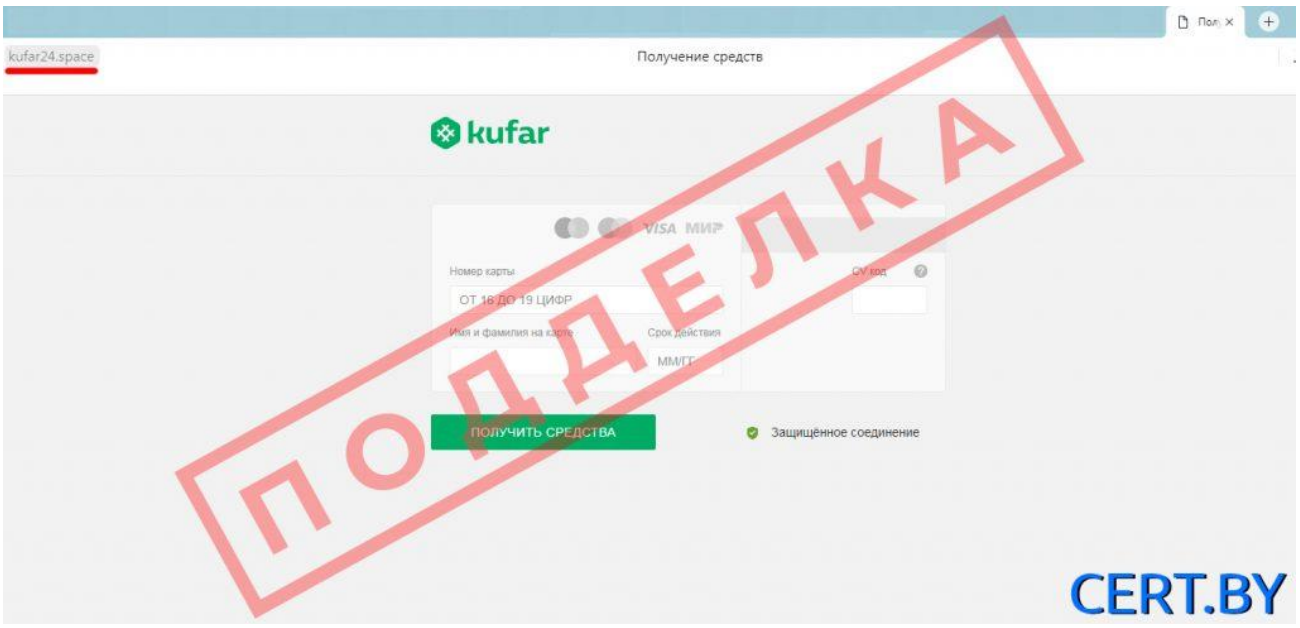
В настоящее время наиболее распространены следующие способы совершения противоправных действий с использованием торговых интернет-площадок:

1. «Предоплата» (обман продавца)

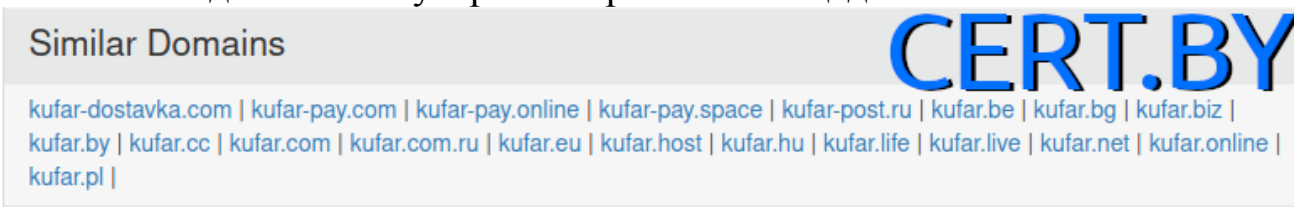
Суть данного способа заключается в том, что злоумышленник выступает в роли потенциального покупателя товара. На одной из интернет-площадок с объявлениями он находит продавца и копирует его контактные данные. В дальнейшем ищет данного продавца в мессенджерах или пишет в социальных сетях, представляясь 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 (зачастую высылается скриншот электронного карт-чека о перечислении средств). Для того, чтобы якобы 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. Кроме этого преступники порой дополнительно просят продавца предоставить информацию, содержащуюся в СМС-сообщении, поступившем из банка, якобы для подтверждения получения предоплаты. После получения конфиденциальных сведений, злоумышленник совершает хищение средств.





Примеры поддельных ресурсов, названия, которых схожи с названием одной из популярных торговых площадок:



2. «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, злоумышленник 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 ссылку 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.

3. «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 (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);
- 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 относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;
- уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);
- использовать 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;
- избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если Вам прислали такую ссылку, то, независимо от того, кто ее прислал, прежде чем по ней перейти, следует внимательно проверить 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.