Профилактика фишинга

С каждым годом мошенники придумывают новые и изощренные методы обмана граждан. Если случаи развода, когда злоумышленники представляются потенциальными покупателями товара, на первый взгляд, кажутся безобидными, то ситуации, когда аферисты выдают себя за партнеров для романтических отношений, наносят настоящий удар под дых по уши влюбленному человеку. Ведь потерпевший лишается в таких ситуациях не только денег, но и надежд построить любовные связи.

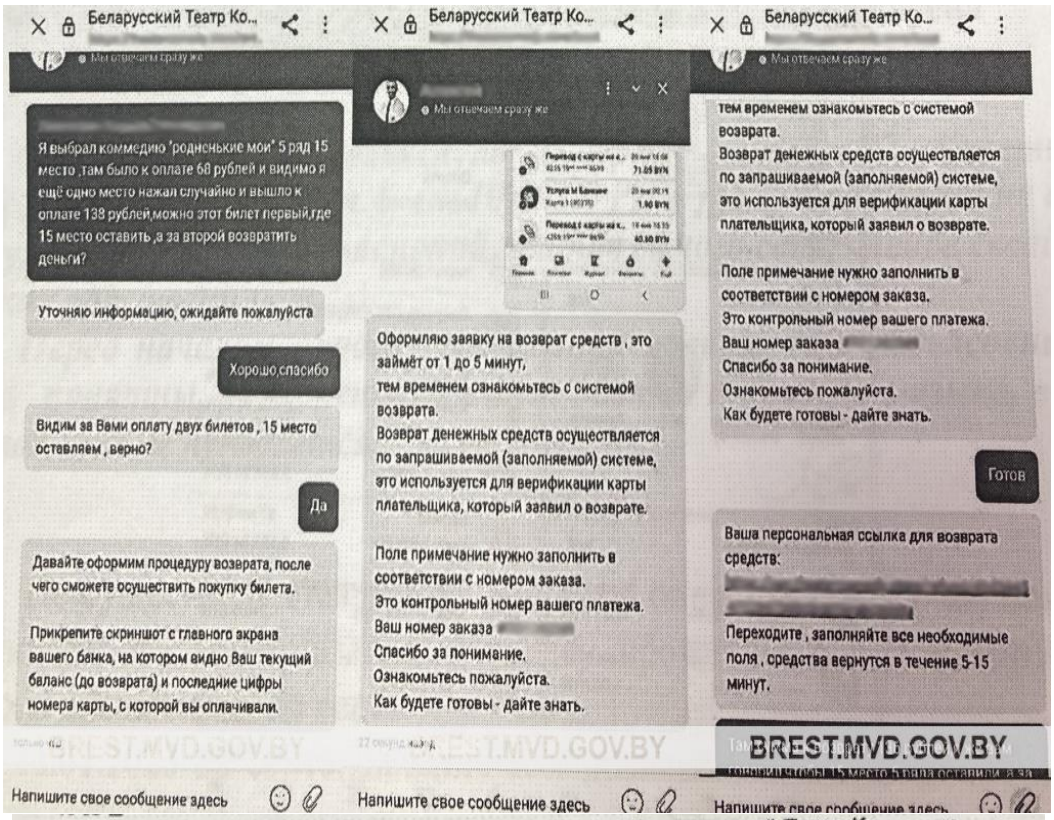
Предугадать, что попадешь в неприятную ситуацию, в начале знакомства довольно сложно. Злоумышленники, как правило, используют фотографии привлекательных девушек и общаются с потенциальной жертвой на непринужденные темы. Диалог строится как при типичных знакомствах: сначала узнают друг друга, а через пару дней все сводится к планированию личной встречи.

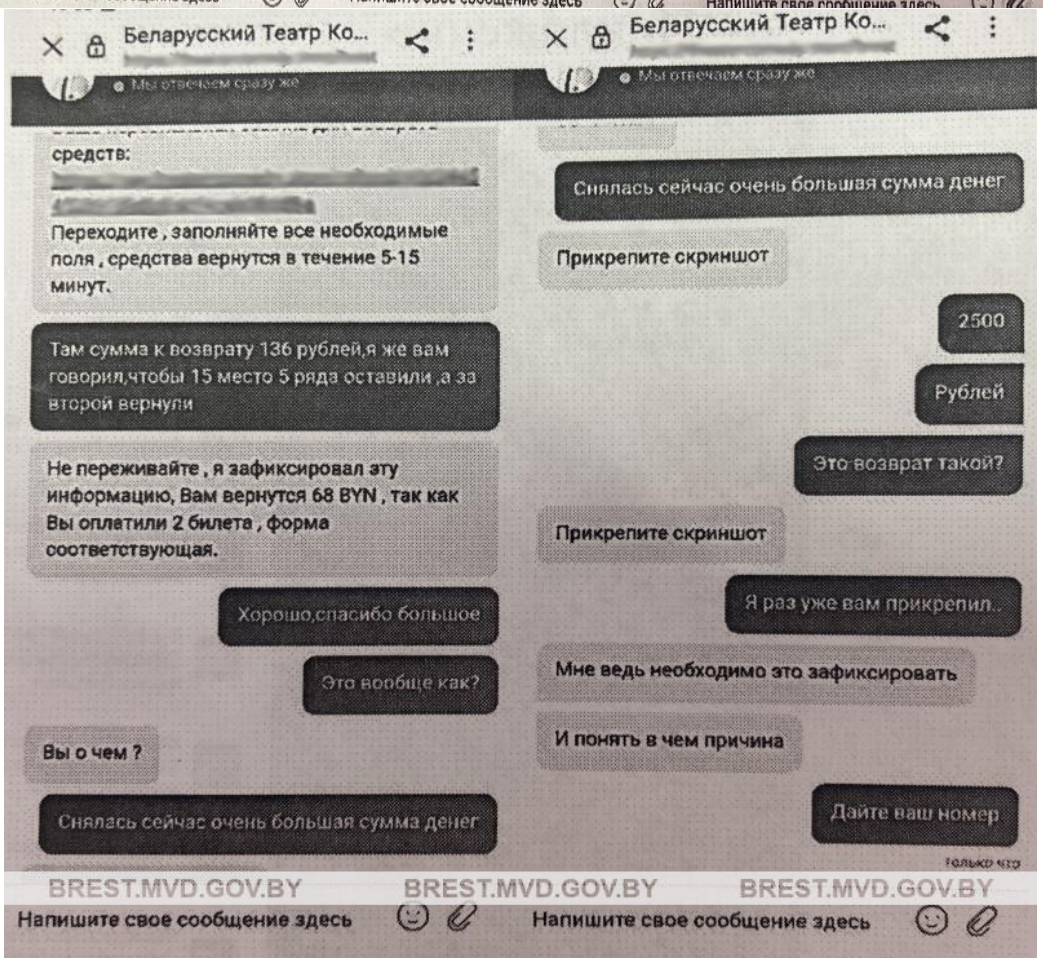
Выбирают для нее кино или театр. При этом начинают подогревать интерес, мол, там можно снять отдельную комнату, в которой два мягких кресла, проектор. Обращают внимание, что туда сложно достать билеты, нужно прямо сейчас забронировать. Затем скидывают ссылку для оплаты. Вот тут-то и стоит насторожиться и внимательно проверить ее подлинность.

Так, в Московский РУВД обратился 21-летний житель Бреста, который сообщил, что неизвестный похитил с его счета 558 рублей.

Мужчина пояснил, что познакомился с девушкой на сайте знакомств, а спустя время продолжил общение в «Телеграме». Через несколько дней общения барышня предложила сходить в театр.

Место, время и спектакль она выбрала сама, оставалось только перейти по ссылке и ввести данные карты. Предприняв несколько попыток провести оплату, каждый раз, совершая ее, ресурс выдавал за ошибку.





Когда заявителю пришло сообщение о списании денег, понял, что сайт для оплаты билетов оказался поддельным, а сам попался на уловку мошенника.

Аналогичным образом лишился денег и 20-летний житель Бреста. Молодого человека злоумышленники «развели» на 628 рублей.

Данный вид мошенничества называется **фишинг**. Перейдя по ссылке, гражданин вводит реквизиты банковской платежной карты. В результате злоумышленник использует эти данные для хищения денежных средств со счета.

Фи́шинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Для этого злоумышленники подменяют страницу используемого жертвой интернет-сервиса на мошенническую, которая внешне является двойником оригинала. Фишинговая страница может иметь сходство с разными сервисами: Kufar, Белпочта, службой доставки, банками, ЕРИП и т.д. В соответствии с этим может использоваться разный предлог для перехода на страницу преступником (забрать зачисленные им деньги, подтвердить получение посылки на почте или в службе доставки, подтвердить прием средств на одном из банковских сервисов и т.д.). Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением оригинальных сайтов. Когда пользователь заходит на такую поддельную страницу и вводит логин и пароль, они становятся доступны мошенникам.

Стоит отметить, что применяемая злоумышленниками схема хищений характерна не только для Беларуси. Столь же системно эти преступления совершаются в отношении пользователей схожих ресурсов, ориентированных на иные государства: России (avito.ru), Украины (olx.ua), Казахстана (olx.kz) и др.

Чтобы не попасться на такую уловку, правоохранители рекомендуют соблюдать ряд правил:

- внимательно относитесь 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.

- 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.

По информации УВД Брестского облисполкома