Мошенничество в сети Интернет. Как не стать жертвой мошенников!

В последнее время на территории г. Горки и Горецкого района значительно возросла активность мошенников, которые посредством телефонных звонков выманивают у белорусских граждан их конфиденциальные данные. Как правило, такие вызовы приходят на территорию Республики Беларусь с изначально подмененным номером. Указанный подвид мошенничества среди специалистов по безопасности имеет название «вишинг».

Вишинг – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой.

В большинстве случаев мошенники:

- представляются сотрудниками банков или иных организаций и предлагают отменить подозрительную операцию, либо заявку на кредит;

-Под видом покупателей товара, реализуемого на Интернет-площадках, выманивают реквизиты карт через мессенджеры либо копии известных сайтов (Куфар, Европочта, Белпочта, СДЭК, Интернет-банк и др.)

Схемы обмана и правила защиты от мошенников, чтобы не попасться на их уловки.

- ПОДОЗРИТЕЛЬНЫЕ ЗВОНКИ

Мошенники обзванивают клиентов, представляясь сотрудниками различных служб банков, Национального банка, Ассоциации банков, правоохранительных органов. Звонок поступает на мобильный телефон или в мессенджер (Viber, WhatsApp). При этом номера телефонов, с которых осуществляется звонок, могут быть похожи на официальные телефоны этих организаций.

Чтобы войти в доверие, злоумышленники могут обращаться по имени, назвать адрес или часть цифр номера карты. В процессе разговора возможны переключения на сотрудников иного (обслуживающего) банка. Цель – убедить клиента предоставить данные, необходимые для входа в Интернет-банк, а также для осуществления платежа. Получив информацию, мошенник списывает деньги со счетов. Кроме того, часто клиент, предоставив все данные, одобряет, тем самым, оформление на свое имя кредита. В этом

случае, он теряет не только средства со своих счетов, но и сумму одобренного кредита.

Самые распространенные уловки мошенников:

Отмена перевода/заявка на кредит

В большинстве случаев, звонящий сообщает о подозрительных операциях по карточке либо об оформлении кредита или овердрафта на ваше имя. Для блокировки подозрительной операции или отмены заявки на кредит злоумышленник при разговоре требует срочно предоставить следующие данные (возможно, не все из перечисленного):

· личный номер паспорта;

· полный номер карточки или последние 4 цифры карточки и CVV-код;

· СМС-коды, которые приходят на ваш телефон от банка (М-код, 3D-secure kod).

Участие в спецоперации

Мошенник, представившись сотрудником службы безопасности банка, сообщает о проведении служебного расследования по факту хищения денежных средств клиентов неустановленным сотрудником банка. Однако, клиента просят не звонить в банк, так как звонок может помешать расследованию, и предупреждают о наличии уголовной ответственности за препятствование расследованию. Далее звонок переключается якобы на сотрудника правоохранительных структур (МВД, прокуратура и т.п.), который продолжает вводить клиента в заблуждение. Во время общения на любой стадии разговора под предлогом страхования вклада, блокировки счета и т.д. предпринимаются попытки получения конфиденциальных данных. Также для проверки «недобросовестных» сотрудников банка, клиента вынуждают оформить кредит, уверяя, что его не надо будет потом погашать, и убеждают установить приложение «AnyDesk – удаленное управление» из Google Play или App Store, позволяющее получить доступ к счету клиента для осуществления несанкционированного перевода денежных средств.

<u>Памятка, как не стать жертвой мошенников в сети Интернет.</u>

1) Если вам нужно перечислить деньги на карточку, вам нужно предоставить отправителю только **полный номер карты**;
2) Вы **никак не должны «подтверждать», либо «получать» перевод**, независимо от того, откуда и как он отправлен (в том числе, при переводе из-за границы). Банк не требует подтверждать получение перевода СМС-кодом;
3) Никогда **не пополняйте карту «для получения перевода»**;

4) В случае совершения сделок на Куфаре, общайтесь с покупателями и продавцами **только на официальном сайте Куфара** – там вредоносные ссылки автоматически блокируются. Не переходите в другие мессенджеры и соц. сети для общения с покупателем.
5) Предоставьте покупателю данные виртуальной карты с нулевым или незначительным остатком. Открыть виртуальную карту можно мгновенно и бесплатно в Интернет-банке.
6) Если вы хотите посетить какой-то сайт, сами введите его адрес в поисковую строку.

Будьте бдительны и аккуратны, соблюдайте вышеуказанные требования для того, чтобы оставаться в безопасности.

Начальник Горецкого РОВД Максим Павлович Дёменский