Рекомендации
«Схемы обмана и правила защиты от мошенников, чтобы не попасться на их уловки»

1) 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 при звонках на мобильные телефоны, а также в мессенджерах Viber и WhatsApp: отмена перевода/заявки на кредит/поступление запроса на вывод средств с вашего счета.

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 (идентификационный) номер паспорта;

• полный номер карточки или последние 4 цифры карточки и CVC-код с обратной стороны карты;

• СМС-коды, которые приходят на ваш телефон от банка (М-код, 3D-Secure);

логины (имя пользователя) и пароли от ДБО;

ПИН-код от карточки, используемый для совершения операций с использованием карточки;

сеансовые пароли доступа в Интернет-банк.

А также не забывайте, если есть подозрение, что ваши конфиденциальные данные доступа в ДБО стали известны мошенникам, оперативно заблокируйте доступ к вашем личному кабинету в мобильном приложении и Интернет-банке через функцию: «Блокировка учетной записи».

Помните!

Сотрудники банка никогда не запрашивают такую информацию: чтобы удостоверить личность, они уточняют дату рождения и кодовое слово,

которое вы указали при регистрации. Этой информации оператору достаточно, чтобы идентифицировать вас и отменить подозрительную транзакцию, если на неё действительно поступил запрос.

Звонящий мошенник торопит, не позволяет подумать – тараторит и пугает безвозвратным списанием денег. Спешка, резкие формулировки и психологическое давление должно насторожить – операторы банка так не общаются. Типичные фразы: «была подозрительная операция / активность», «нужно срочно заблокировать списание, сообщите данные», «потом будете разбираться с банком сами» и тому подобное.

2) 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, прокуратуры 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.

Помните!

Не видитесь на запугивания и уговоры! Часто мошенники уже что-то знают о вас. Пусть то, что они обращаются по имени, не отключает вашу бдительность. И помните: в зоне риска - все клиенты всех банков.

3) Отмена заказа на покупку/доставку товара.

В данном случае под видом работников интернет-магазина 21vek или иной торговой площадки злоумышленники звонят клиентам белорусских банков и сообщают, что на их имя оформлен заказ на покупку/доставку товара. Клиент сообщает, что покупку не совершал.

Далее мошенники уточняют, в каком банке обслуживается клиент, и предлагают сделать отмену. Получив конфиденциальную информацию, пытаются осуществить процедуру смены логина/пароля в интернет-банке. Клиенту направляется от банка СМС-сообщение с кодом, которое злоумышленники просят сообщить для отмены заказа.

Помните!

СМС-код от банка ни в коем случае нельзя передавать никому, даже сотруднику банка. Это «ключ», необходимый для одобрения платежа по вашей карточке, а также для смены секретных параметров доступа в ваш личный кабинет интернет-банка.

4) Продажа товаров в интернете.

Мошенники создают копии известных сайтов (Куфар, ay.by, сайты интернет-банков, Белпочты, Европочты, СДЭК и др.), чтобы списывать деньги с карточек.

Если вы разместили объявление о продаже вещи в интернете, к вам может обратиться (часто через мессенджер) мошенник под видом покупателя. Он сообщает, что хочет приобрести ваш товар, и предлагает оформить доставку с оплатой на вашу карточку. Мошенник присылает ссылку, по которой нужно пройти якобы для оформления доставки или получения перевода.

По ссылке размещается мошеннический сайт, внешне очень схожий с сайтом, на котором вы разместили объявление (например, Куфар, ay.by и др.), либо сайтом почтовой службы (например, Белпочты, Европочты, СДЭК и др.). На странице также может быть размещена копия информации о продаваемом вами товаре, чтобы вызвать доверие.

Для «получения перевода» у вас потребуют ввести все реквизиты карты и СМС-код от банка. Если вы введете эти данные, то подтвердите перевод в адрес мошенника.

В переписке мошенник может сообщить, что для получения перевода остаток на вашей карте должен быть не ниже определенной суммы (как минимум, суммы перевода). Таким образом он гарантирует себе возможность списания средств с вашей карты.

На большинстве мошеннических сайтов есть даже «служба поддержки», которая может убеждать вас ввести нужные данные и даже пополнить карту, чтобы увеличить сумму списания.

Наибольшую угрозу представляют копии сайтов интернет-банков. Внешне они очень схожи с настоящими сайтами и предназначены для сбора секретных параметров – логина, пароля и авторизационного кода. Получив их, мошенник инициирует списание с вашей карты и вынудит вас ввести СМС-код от банка на том же мошенническом сайте, имитируя это как зачисление перевода.

Помните!

Если вам должны перечислить деньги на карточку, вам нужно предоставить отправителю только полный номер карты.

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.

• Никогда не переходите по ссылкам, полученным от отправителя якобы для получения перевода/ оформления доставки.

• Никогда не пополняйте карту «для получения перевода».

• 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 социальные сети для общения с покупателем.

• Предоставьте покупателю данные виртуальной карты с нулевым или незначительным остатком. Открыть виртуальную карту можно мгновенно и бесплатно в интернет-банке.

• Если вы хотите посетить какой-то сайт, сами введите его адрес в поисковую строку.

5) Помощь родственнику или знакомому.

Мошенник может обратиться к вам в социальных сетях со взломанного аккаунта вашего родственника или знакомого. Он может попросить зачислить на вашу карту денежный перевод (например, из-за того, что его карта пока не получена в банке или истек срок ее действия). Для осуществления перевода мошенник попросит вас назвать полный номер карты, срок действия, CVC/CVV-код (3 цифры на обороте карты) и СМС-коды от банка. Если вы предоставите эти данные, то одобрите списание со своей карты в адрес мошенника.

Мошенник также может под видом родственника или знакомого попросить одолжить ему денег. В таком случае, он предложит вам самостоятельно сделать перевод по указанным им реквизитам.

Кроме этого, злоумышленники звонят гражданам и говорят, что их близкие попали в серьезное ДТП. Мошенники запугивают своих абонентов словами, что за подобное предусмотрена серьезная ответственность, и в скором времени их близкие отправятся в места не столь отдаленные. В итоге граждане передают злоумышленникам крупные суммы денег, а позже узнают об обмане. Данная схема преступников получила апгрейд: если раньше деньги были нужны для решения вопросов с правоохранительными органами с целью избежать ответственности за совершенное ДТП, то сейчас средства просят передать на проведение срочной операции родственнику, попавшему в дорожно-транспортное происшествие.

Помните!

Прежде чем выполнить такую просьбу, необходимо связаться с родственником или знакомым по телефону и уточнить, действительно ли он просит сделать перевод либо предоставить реквизиты карты. Потратив всего одну минуту, вы сохраните свои средства. Для зачисления перевода на вашу карту требуется только полный номер карты. Никакие другие реквизиты банку не нужны. Вам также не нужно никак подтверждать получение перевода.

6) Получение посылки в отделении РУП «Белпочта»

Мошенники звонят гражданам и говорят, что на его имя поступила посылка с наложенным платежом, которую он должен немедленно забрать в почтовом отделении. Чаще всего в качестве лже-отправителя выступает какой-нибудь интернет-магазин.

Помните!

РУП «Белпочта» никогда не звонит клиентам. О новых посылках адресатам сообщают с помощью SMS-сообщений, сообщением в

мессенджере «Viber» или уведомлением в почтовом ящике. Отправителем электронных сообщений всегда должен значиться «belpost.by».

Кроме этого, сотрудники РУП «Белпочта никогда не требуют от человека немедленно и обязательно забрать посылку. Адресат имеет полное право вообще от нее отказаться. Тем более, если не помнит, чтобы что-то где-то заказывал.

Что можно спросить у подозрительного звонящего, чтобы изобличить мошенника.

Мошенники выдают себя, когда им задают конкретные вопросы о месте их работы или ваших банковских продуктах. При подозрении можно уточнить:

• официальное название подразделения;

• ФИО руководителя;

• тип и условия обслуживания вашей карты.

• общие вопросы вроде «где находится главный офис банка?» задавать не стоит – эта информация общедоступна.

Копайте вглубь и обращайте внимание на то, как собеседник реагирует на ваши вопросы. Если он теряется, злится, хамит, ошибается, прекращайте разговор и звоните в банк по номерам, указанным на обратной стороне карты, расскажите о ситуации.