**КАК НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ**

«Вишинг»-один из методов мошенничества, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудники банка, покупателя и т.д.), под разными предлогами выманивают у граждан конфиденциальную информацию или побуждают к совершению определенных действий со своим банковским счетом/платежной картой.

Схема большинства преступлений проста: преступники звонят жертве в любом из мессенджеров, как правило это «Viber», либо с абонентских номеров иностранных государств, маскируются под сотрудников банков, сотрудников правоохранительных органов и сообщают о проблемах с банковским счетом. Вас не должно сбивать с толку если номер абонент подписан как «BELARUSBANK», «МВД» и т.д. Для решения проблем предлагают сообщить личные данные (номер карты, идентификационный номер паспорта и прочее), после чего с помощью этих данных и выводят средства со счета жертвы. Как правило, человека торопят, призывают принять решение здесь и сейчас, просят никому об этом не сообщать из-за чего он теряется и предоставляет информацию. Но стоит помнить, что сотрудники банков никогда не звонят клиентам в мессенджерах. Также как правило, мошенники обращаются с конкретной целью и знают необходимую им информацию о пользователе.Нередки случаи, когда злоумышленники о проведении служебного расследования по факту хищения денежных средств клиентов неустановленным сотрудником банка, в связи, с чем просят не звонить в банк, мотивируя это тем, что звонок может помешать расследованию и предупреждают о наличии уголовной ответственности за препятствование расследованию (при этом могут ссылаться на произвольный номер статьи Уголовного кодекса Республики Беларусь).

***Аналогичным способом были похищены денежные средства жительницы д. Лесная Славгородского района:***

*Так, гражданке И, жительнице Славгородского района позвонил неизвестный номер, пользователь которого представился сотрудником финансового отдела ОАО «Белагропромбанк» и пояснил, что к её банковскому счёту пытаются получить несанкционированный доступ злоумышленники, в связи с чем ей необходимо получить в местном отделении банка максимально возможный кредит для последующего выявления мошенника среди работников местного отделения банка. В дальнейшем, со слов злоумышленника, когда мошенники будут выявлены, весь оформленный кредит будет автоматически списан. Гражданка И, находясь под действием обмана злоумышленников, в местном отделении ОАО «Белагропромбанк» г. Славгорода оформила на свое имя кредит в сумме 5000 белорусских рублей и перевела их на расчетный счет, который указал злоумышленник, якобы с целью выявления мошенников, которые попытаются их в дальнейшем похитить. После перевода денежных средств с ней перестали выходить на связь, весь диалог в мессенджере был удален.*

***Еще один из ярких примеров произошел с еще одним жителем Славгородского района****.*

*В феврале 2022 года возбуждено уголовное дело по ч.3 ст. 212 УК Республики Беларусь (хищение имущества путем модификации компьютерной информации совершенное в крупном размере) неизвестный, представившись работником банка, обманом убедил жителя Славгородского района обратиться в местное отделение банка и получить на свое имя кредит в сумме 8000 рублей, а именно неизвестный пояснил, что на имя гражданина кто-то пытается оформить кредит и для того чтобы мошенники не сделали этого ему необходимо самому обратиться в банк для оформления указанного кредита. При этом неизвестный уговаривал гражданина не рассказывать ничего работникам банка и иным лицам в том числе и родственникам, так как с его слов в этом могут быть замешаны работники банка. После оформления кредитного договора мошенник уговорил гражданина предоставить личные коды доступа к расчетному счету (номер банковской карты и срок ее действия, трехзначный код с обратной стороны карты и коды предоставленные банком в СМС-сообщениях). Получив указанные коды, неизвестный провел денежные операции по нему, тем самым похитив их, а также попытался оформить кредитный договор еще на 4000 рублей, однако вовремя заметившие это сотрудники банка связались с потерпевшим. На их вопрос о попытке оформления кредита, он пояснил, что кредит на 4000 рублей он не оформлял, после этого работники банка посоветовали проверить свой счет и обратиться в милицию, а указанная заявка была отменена работниками банка.*

*За указанное преступление предусмотрено наказание от штрафа до лишения свободы сроком от трех до пятнадцати лет.*

В связи с этим прошу соблюдать следующие меры предосторожности, чтобы не попасть на уловки кибермошенников:

1. Не рекомендуем отвечать на звонки, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе, код которого начинается с префикса схожего с префиксом Республики Беларусь (+372, +373 и т.д.) либо префикса иностранного государства (+135, +485 и т.д.).

2. ПОМНИТЕ: Код вашей карты и пароли подтверждения операций НЕ ИМЕЕТ ПРАВА спрашивать даже сотрудник банка.

3. Не верьте любой информации от незнакомца, даже если звонок поступил с официального телефона горячей линии банка.

4. Возьмите за правило: если Вам поступил неизвестный звонок и под каким-либо предлогом звонящие пытаются выяснить у Вас номер банковской карты, личные данные, говорят о том, что с Вашей карты пытаются похитить денежные средства, помните – это 100 % звонят мошенники.

5. Прервите разговор и самостоятельно позвоните на телефон горячей линии банка, набрав номер вручную, указанный на обратной стороне Вашей банковской карты.

6. В случае, если мошенникам все же удалось получить сведения о реквизитах вашей карточки, Вам необходимо как можно скорее её заблокировать.

7**.** Ни под каким предлогом не соглашайтесь на просьбы «якобы» работника банка на оформление кредитов на ваше имя, так как работники банка об этом просить не будут.

8. По просьбе неизвестных не устанавливайте никаких незнакомых приложений на свое мобильное устройство.

Также убедительно просим довести указанную информацию до своих родных, близких, друзей и знакомых, в особенности пожилых граждан, чтобы они могли избежать аналогичных случаев хищения денежных средств с их банковских карт и не стали жертвами мошенников.

**ХИЩЕНИЕ ДЕНЕГ ЧЕРЕЗ KUFAR !!!**

Как мошенники обманывают тех, кто публикует объявления о продаже на сайте Kufar.by. Здесь есть две основные схемы.

***В первой схеме*** мошенник по номеру телефона из объявления находит продавца в мессенджерах и предлагает купить у него товар по предоплате, в том числе якобы через «Куфар Доставку». После этого мошенник присылает жертве ссылку на поддельный сайт, где нужно ввести данные своей карты якобы для того, чтобы получить денежный перевод. Адрес сайта может незначительно отличаться от настоящего (например, kufar.cc или kufar.store), а дизайн будет очень похожим на настоящий. После того как жертва введет на нем данные своей карты, мошенники получат доступ к деньгам на счету.

***Вторую схему*** в «Куфаре» называют «продвинутой». Она возможна в том случае, если сработала первая. Тогда мошенник еще раз выходит на связь с жертвой или же притворяется сотрудником службы поддержки и говорит, что произошел ошибочный перевод. Чтобы вернуть деньги, жертве нужно пройти по ссылке и ввести данные своей карты. Разумеется, сайт будет фишинговым (поддельным), и деньги спишут еще раз.

**ЗАПОМНИТЕ!**

• при использовании торговой площадки Kufar совершайте все действия исключительно на самой платформе объявлений и не заводите диалог о продаже или покупке товара в мессенджерах (Viber, WatsApp, Telegram).

• не переходите по ссылкам, которые высылают неизвестные собеседники.

**За хищение имущества путем использования компьютерной техники по ст. 212 УК Республики Беларусь предусмотрено наказание от штрафа до лишения свободы сроком от трех до пятнадцати лет/**

Старший оперуполномоченный

отделения уголовного розыска

Славгородского РОВД

Филипп Владимирович Николаев