**ВНИМАНИЮ ПОТРЕБИТЕЛЕЙ: О БЕЗОПАСНОСТИ ИНТЕРНЕТ-ПОКУПОК И ИНТЕРНЕТ-ПРОДАЖИ СВОИХ ВЕЩЕЙ**

**Как действуют мошенники?**

Мошенники создают копии сайтов белорусских интернет-ресурсов, как правило, банковских, торговых, почтовых или сайтов, на которых размещают объявления физические лица о продаже своих вещей. Внешне (по дизайну и цветовому оформлению, логотипам) они практически ничем не отличаются от настоящих сайтов. Лишь при внимательном изучении доменного имени мошеннического сайта можно обнаружить отличие от оригинала: при правильном указании названия самого сайта значится иностранная доменная зона (например, вместо «.by» указано «.сс» или «.su»), лишние символы (точка или тире) и (или) замена одной буквы или дублирование одной и той же буквы и т.д. Зачастую, интернет-пользователь не обращает на это внимания, видя визуально знакомое оформление ресурса и для совершения платежа вводит реквизиты своей банковской карты. На это и рассчитывают мошенники – создание копий широко известных интернет-ресурсов направлено на хищение денежных средств со счетов банковских карт граждан.

К физическим лицам, которые размещают объявления о продаже своих вещей, мошенники, как правило, выдают себя за «покупателей», предлагая осуществить расчет в безналичной форме – якобы хотят перечислить деньги за товар на банковскую карту. При этом якобы для удобства и быстроты присылают в мессенджере ссылку (являющуюся переходом не на настоящий, а на мошеннический (фишинговый) сайт), которую нужно открыть и ввести сведения о реквизитах банковской карты.

Таким путем мошенники получают конфиденциальную информацию и похищают денежные средства со счетов граждан (потребителей товаров или услуг, продавцов личных вещей).

**Что такое фишинговые сайты?**

Фишинг (англ. fishing рыбная ловля, выуживание) – вид интернет-мошенничества, цель которого – получить идентификационные данные пользователей, такие как пароли, номера кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинговые сайты обладают доменными именами, схожими до степени смешения с официальным торговым интернет-ресурсом (название может отличаться буквально одним символом либо национальной доменной зоной), и содержат изображение товарного знака, дублируют веб-дизайн и контент страниц официального интернет-ресурса.

Новые появляются практически сразу после блокировки старых, а схожесть с реальными сайтами порой достигает очень высокого уровня.

Копируют (подделывают) различные ресурсы: торговые площадки, платформы и сервисы, на которых доступна оплата онлайн каких-либо товаров или оказания услуг, интернет-банкинги банков и др.

Таким образом, в настоящее время наблюдается две основные схемы мошенничества, когда мошенник выступает в роли:

продавца (исполнителя услуги);

покупателя (заказчика услуги).

**На 1-м этапе (подготовка):**

мошенник создает одну страницу, внешне похожую на страницу авторизации официального сервиса, накладную, бланк отправки курьерской службы (платежное обязательство) или же полностью копирует весь сайт интернет-ресурса;

производит регистрацию домена, визуально схожего с оригинальным;

начинает поиск жертвы.

**На 2-м этапе (реализация):**

действуя под предлогом приобретения (либо продажи) товара на официальном интернет-ресурсе, мошенники обращаются к автору соответствующего объявления (продавцу) и осуществляют с ним переписку посредством популярных интернет-мессенджеров;

в ходе переписки вводят потенциальную жертву в заблуждение и под предлогом получения денежных средств за продаваемый товар, отправляют продавцу (жертве) активную ссылку, переходя по которой гражданин (жертва) оказывается на фишинговом интернет-сайте, на котором предлагается ввести данные банковской карты для «получения» денежных средств;

на самом же деле жертва, указывая конфиденциальные данные банковской карты, «предоставляет» мошеннику доступ к списанию с указанного им банковского счета денежных средств.

**Схема обмана продавца товара №** **1 (предоплата):**

**1.** Мошенник находит продавца на настоящем интернет-ресурсе (площадке объявлений), копирует его контактные данные, но на настоящем интернет-ресурсе продавцу не пишет, поскольку пересылка фишинговых ссылок там блокируется владельцем интернет-ресурса. Ищет номер продавца в мессенджерах (Viber, Telegram, WhatsApp) и представляясь «покупателем» с настоящего интернет-ресурса говорит, что уже совершил предоплату

**2.** Высылает продавцу ссылку на поддельную (фишинговую) страницу либо сайт, где продавцу нужно ввести номер своей карты для того, якобы, чтобы получить деньги. Среди данных, которые просит злоумышленник, номер банковской карты, имя держателя, срок действия, CVV-код (3 цифры на оборотной стороне карты)

**3.** Иногда мошенник также просит продавца предоставить проверочный код из СМС-уведомления банка, ссылаясь на то, что перевел предоплату и хочет убедиться, что она поступила на счет продавца

**4.** С помощью собранных данных мошенник переводит с банковской карты жертвы часть либо все денежные средства

**5**. Если схема успешно сработала, мошенник может повторно связаться с продавцом товара, только уже представившись службой поддержки интернет-ресурса, и сказать, что произошла ошибка. Под предлогом возврата ошибочно переведенных средств, мошенник предлагает снова перейти на поддельную (фишинговую) страницу или сайт и снова ввести данные банковской карты продавца (жертвы)

**6.** Мошенник повторно списывает денежные средства, имеющиеся на банковской карте

**Схема обмана покупателя товара №** **2 (доставка):**

**1.** Мошенник выставляет товар на настоящем интернет-ресурсе (площадке объявлений) по крайне выгодной цене (преднамеренно занижает его стоимость, делая товар очень привлекательным по цене)

**2**. Когда находится потенциальный покупатель, мошенник убеждает перейти в мессенджер (Viber, Telegram, WhatsApp) под предлогом того, что там удобнее общаться

**3**. Во время общения мошенник уговаривает покупателя на предоплату и доставку товара под предлогом того, что уехал из города, нет времени и т.д. Чтобы развеять сомнения покупателя, мошенник говорит о новой услуге, которая якобы появилась на настоящем интернет-ресурсе: если доставки не будет, торговая площадка автоматически вернет денежные средства на банковскую карту

**4**. Высылает покупателю в мессенджере ссылку на поддельную (фишинговую) страницу, которая имитирует страницу настоящего интернет-ресурса (например, страницу «Доставка»), где нужно ввести данные банковской карты, чтобы совершить предоплату

**5**. Как только покупатель вводит данные своей банковской карты, с нее списываются денежные средства; товар, естественно, не присылается и деньги не возвращаются

**6.** Если эта схема успешно сработала, мошенник может повторно связаться с покупателем и сказать, что якобы произошла ошибка и товар «уже забрали» (или передумал продавать) и предложить вернуть деньги, либо представиться службой поддержки настоящего интернет-ресурса и рассказать о возможности возврата денежных средств за недоставленную посылку.

Мошенник высылает ссылку на поддельную (фишинговую) страницу для возврата денежных средств, где покупателю предлагают ввести данные банковской карты покупателя и сумму, которую ему должны вернут

**7.** Мошенник повторно списывает денежные средства с банковской кары покупателя

**Схема обмана покупателя № 3 (отправка товара по почте)**

**1.** Мошенник выставляет товар по очень выгодной цене (преднамеренно занижая его стоимость, делая товар очень привлекательным по цене) на официальном сайте торговой площадки. Когда потенциальный покупатель пишет ему на торговой площадке (площадке объявлений), под любым предлогом предлагает перейти в мессенджер (Viber, Telegram, WhatsApp)

**2**. Уговаривает отправить товар по почте. При этом мошенник специально создает ажиотаж вокруг объявления, говорит о том, что на днях уезжает из города, а товар готовы купить другие покупатели

**3.** Предлагает оплатить товар уже после его отправки. В качестве «доказательства» отправки посылки мошенник высылает ссылку на поддельную (фишинговую) страницу трекинга посылки или скан поддельного документа об оплате (квиток любой службы доставки: Белпочта, Европочта, СДЭК )

**4**. После того как покупатель поверил, что посылка отправлена, мошенник присылает ссылку на поддельную (фишинговую) страницу, где нужно оформить перевод стоимости за товар, введя реквизиты банковской карты

**5**. Как только пользователь вводит данные своей банковской карты, с его счета списываются деньги, а посылка, естественно, не приходит

**Интернет-пользователям следует помнить, что самая надежная защита – это осведомленность, бдительность и осторожность.**

**На что следует обратить внимание**:

коммуникация с мошенниками осуществляется через социальные сети, с номера телефона, как правило, зарегистрированного за пределами Республики Беларусь либо на подставное лицо;

помните, что наиболее безопасный способ общаться с продавцом или покупателем – через личные сообщения **на настоящем интернет-ресурсе**, если ваше общение переходит в мессенджер (Viber, Telegram, WhatsApp и т.д.), официальный интернет-ресурс не сможет вас защитить;

мошенники используют особенности человеческого восприятия и поведения (предлагают легкое решение насущной проблемы; создают чувство нехватки времени; торопят, не дают подумать или посоветоваться с близкими и др.);

до оплаты покупки убедитесь, что вы находитесь на настоящем интернет-ресурсе (сайте интернет-магазина, почтового оператора, площадке объявлений); вас должно насторожить отсутствие контактной информации о владельце сайта; много мелких грамматических ошибок, опечаток, несоответствий; слишком низкие цены на товары; призывы к срочным действиям, много восклицательных знаков; предложение быстро и легко заработать; большое количество негативных отзывов;

до ввода данных своей банковской карты, позвоните продавцу (покупателю) и убедитесь, что у вас есть его реальный белорусский номер. Вас должно насторожить, когда продавец (покупатель) под любым предлогом пытается избежать личного общения по телефону; факт переписки в мессенджере не подтверждает того, что этот номер действительно принадлежит тому, кто вам пишет;

если вы хотите воспользоваться услугами по отправке (доставке) почтовых отправлений (посылок), обратите внимание, что такие услуги оказываются непосредственно отправителю. Для этого отправитель должен самостоятельно зарегистрироваться на сайте почтового оператора и сделать заявку на отправку почтового отправления. **Почтовый оператор никогда не запрашивает данные о банковской карте отправителя**. Отправка посылки происходит непосредственно в отделении почтовой связи почтового оператора. Для получения наложенного платежа (денежных средств) необходимо лично обратиться в отделение почтовой связи; выдача наложенного платежа производится только наличными денежными средствами после предъявления документа, удостоверяющего личность.

**Как не стать жертвой мошенников? Советы для интернет-пользователей:**

**убедитесь, что вы на настоящем интернет-ресурсе** (интернет-магазина, почтового оператора, площадки объявлений): безопасней всего заходить напрямую, вводя адрес самостоятельно [https://www.ххх.by/](https://www.xn--u1aaa.by/) или через приложение для [Android](https://play.google.com/store/apps/details?id=se.scmv.belarus) и [iOS](https://apps.apple.com/by/app/kufar-besplatnye-ob-avlenia/id1149312972);

**добавьте настоящие сайты** интернет-магазина, почтового оператора, площадки объявлений, на которых вы регулярно вводите данные, в закладки браузера;

**совершайте все действия на настоящем интернет-ресурсе** (общение в чате, перевод денег на карту, использование доставки), не переходя на общение в мессенджеры;

**не переходите по ссылкам**, которые вам высылают **в мессенджерах**: чтобы попасть на настоящий сайт, сами вписывайте адрес сайта в поисковую строку;

**не совершайте никаких операций** с банковской картой или счетом, **если вам диктуют действия**в мессенджере или по телефону;

**не сообщайте никому свои паспортные данные, данные банковских карт** (даже под предлогом перевести вам платеж), **коды из СМС-сообщений** от вашего банка;

**не сообщайте** и не вписывайте **трёхзначный код** (CVC2/CVV2) с обратной стороны банковской карты;

**не сканируйте QR-коды**, которые вам присылают **в мессенджерах**;

**не переводите предоплату** за товар **с подозрительно низкой стоимостью**;

**не оплачивайте товары** и услуги переводом на банковскую карту или по номеру телефона, если вы не знакомы с получателем;

оформите отдельную банковскую карту для онлайн-платежей и храните на ней небольшую сумму;

подключите СМС-уведомление от банка: вам будет приходить информация обо всех операциях по банковской карте;

скачивайте мобильные приложения только из каталога официальных магазинов для электронных устройств.

**Что делать, если вы стали жертвой мошенников:**

если все-таки мошенники нашли способ похитить ваши деньги с банковской карты, и вы успели это оперативно обнаружить, сразу обращайтесь в банк (контакт-центр банка либо по номеру телефона, указанному на банковской карте) – возможно, сотрудники банка успеют отменить операцию и вернуть деньги;

если вы ввели данные банковской карты, то необходимо в срочном порядке произвести ее блокировку, позвонив в банк;

сообщите о мошенничестве владельцу настоящего интернет-ресурса (интернет-магазина, почтового оператора, площадки объявлений), направив в службу поддержки скриншот поддельной (фишинговой) страницы с точным адресом, указанным в адресной строке, с описанием произошедшей ситуации;

обратитесь с заявление о действиях мошенников в правоохранительные органы.