Внимание! Фишинговые сайты!

В национальном сегменте сети Интернет Республики Беларусь наблюдается значительное повышение мошеннической активности, связанной с использованием фишинговых страниц и даже целых сайтов.

Целью данной разновидности фишинга является получение не только учетных данных от каких-либо сервисов (логин и пароль), но и данных платежной карты (номер, срок действия, имя и фамилия держателя и CVC2/CVV2 код).

Также стоит отметить, что продуманный целевой фишинг не обходится без использования социальной инженерии. Причем если раньше в основном происходила рассылка фишинговых писем на электронную почту, где была возможность блокировать массовые рассылки, то теперь злоумышленники используют еще мессенджеры и социальные сети, что значительно расширяет целевую аудиторию.

В случае успеха злоумышленник может перечислить с карты жертвы некую сумму денег, если на счете будет достаточно средств. А если получит данные для входа в личный кабинет интернет-банкинга, перечислит все деньги со счета, либо, с использованием межбанковской системы идентификации (МСИ), может открыть счета в других банках (о которых жертва длительное время может не знать), для проведения транзитных операций. В худшем случае, оформит онлайн-кредиты, в которых можно снять наличные, перевести или потратить средства

онлайн. А через некоторое время жертве придет извещение о задолженности или повестка в суд за неуплату.

Данная мошенническая активность направлена на государственные органы и организации, юридических и физических лиц.

Подделываются различные ресурсы:

- интернет-банкинги банков;
- торговые площадки;
- различные платформы и сервисы, на которых доступна оплата онлайн каких-либо товаров или оказания услуг.

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

В настоящее время наблюдается две **основные схемы мошенничества:**

- Злоумышленник выступает в роли продавца (исполнителя услуги).
- Мошенник притворяется покупателем (заказчиком услуги).

У каждой схемы существуют свои модификации, которые позволяют мошенникам, в том числе повторно, обманывать пользователей.

Пример маскировки под площадку Kufar.by

Совместно с площадкой объявлений Куфар мы составили детальное описание того, как злоумышленники сегодня пытаются обманывать белорусов.

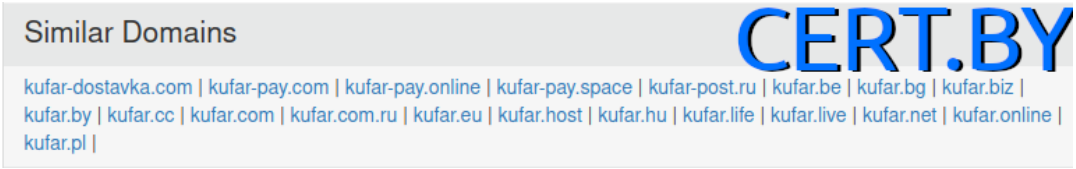
Каждая из схем обмана подразумевает 2 этапа: подготовку и реализацию. Подготовка практически не меняется, в то время как реализация может быть разыграна по-разному.

«Все зависит от обстоятельств и того, кто в данный момент выступает в роли жертвы, — рассказывает Анастасия Наумова, начальник службы поддержки пользователей Куфара. — Мошенники хорошо чувствуют эмоции собеседников, играют на доверчивости

и открытости белорусов. Могут рассказывать, что попали в сложную жизненную ситуацию и продают вещь за бесценок потому, что нужно оплатить лечение родственнику, учебу ребенку или спасти бизнес, пострадавший от кризиса.»

Подготовка:

1. Злоумышленник создает одну страницу, внешне похожую на страницу авторизации официального сервиса, накладную, бланк отправки курьерской службы (платежное обязательство) или же полностью копирует весь сайт.
2. Производит регистрацию домена, визуально схожего с оригинальным. Название может отличаться буквально одним символом либо национальной доменной зоной. Например, пытаясь замаскировать фишинговую страницу под сервис площадки объявлений Kufar.by, злоумышленник может выбрать следующие домены (в списке для сравнения указан и оригинальный домен):



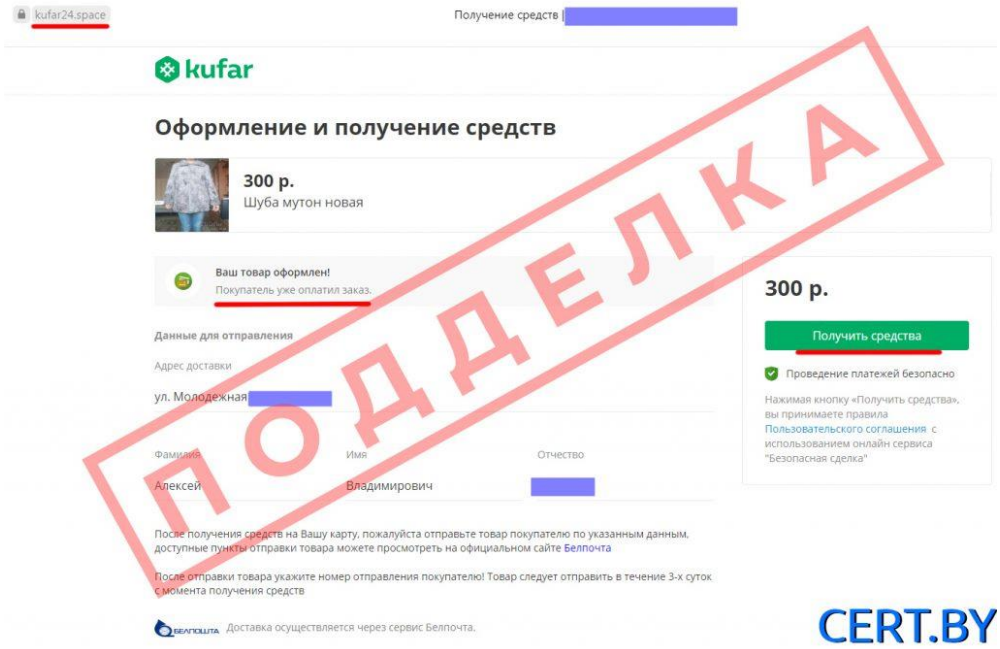
После того, как поддельный сайт создан и размещен на похожем на официальный сайт домене, преступник начинает поиск жертвы.

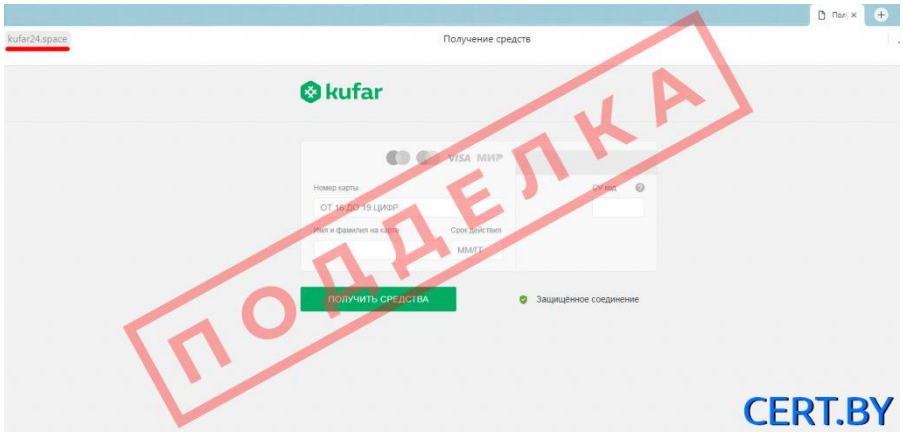
«На данный момент известно о 6 типичных схемах мошенничества, — рассказывает Анастасия Наумова, начальник службы поддержки пользователей Куфара. — Они направлены как на продавцов, так и на покупателей товаров.»

Схема обмана продавцов № 1 (Предоплата)

1. Преступник находит продавца на официальной площадке объявлений, копирует его контактные данные, но на площадке не пишет, поскольку пересылка фишинговых ссылок там невозможна. Ищет номер продавца в мессенджерах или пишет в соцсетях, представляясь якобы покупателем с Куфара.
2. Говорит, что уже совершил предоплату. Высылает продавцу ссылку на поддельную страницу, где продавцу нужно ввести номер своей карты для того, чтобы получить деньги. Среди данных, которые

просит злоумышленник: номер карты, имя держателя, срок действия, CVV-код на оборотной стороне карты.





3. Иногда мошенник также просит продавца предоставить СМС-код подтверждения платежа, ссылаясь на то, что перевел предоплату и хочет убедиться, что она поступила на счет продавца.

4. С помощью собранных данных мошенник может попытаться перевести с карты жертвы некую сумму денег, и, если на счете будет достаточно средств, ему это удастся.

Схема обмана продавцов № 2 (Предоплата)

1. Если предыдущая схема успешно сработала, мошенник может повторно сам связаться с покупателем или представиться службой поддержки и сказать, что произошла ошибка.

2. Чтобы вернуть ошибочно переведенные средства, он предложит перейти на фишинговый сайт и снова ввести данные своей карты.

3. Если продавец это сделает, мошенник может повторно списать деньги.

Схема обмана покупателей № 1 (Доставка базовая)

1. Преступник выставляет товар на официальной площадке объявлений по крайне выгодной цене.

2. Когда потенциальный покупатель пишет ему, преступник убеждает перейти в мессенджер или социальную сеть под предлогом того, что там удобнее общаться.

3. Во время общения мошенник уговаривает покупателя на предоплату или доставку под любым предлогом: уехал из города, нет времени.

4. Чтобы развеять сомнения покупателя, говорит о новой услуге холдирования средств, которая появилась на Куфаре: если доставки не будет, Куфар автоматически вернет средства на карту.

5. Высылает покупателю ссылку на поддельную страницу, которая имитирует страницу сервиса «Куфар Доставка» или интернет-банкинга, где нужно ввести данные карты, чтобы совершить предоплату. В качестве данных карты покупателя просят заполнить номер карты, имя держателя, срок ее действия, CVV-код (3 цифры на оборотной стороне карты). В некоторых случаях злоумышленник может попросить назвать проверочный код из СМС-уведомления банка.

6. Как только пользователь вводит данные своей карты, с нее списываются деньги, посылка, естественно, не приходит и средства не возвращаются.

Схема обмана покупателей №2 (Доставка повторная)

1. После того, как предыдущая схема полностью реализована, и покупатель начинает подозревать, что его обманули, мошенник повторно связывается с покупателем.

2. Говорит, что произошла ошибка, товар уже забрали (или передумал подавать), готов вернуть деньги.

3. Высылает ссылку на поддельную страницу возврата средств, где покупателю нужно ввести все те же данные своей карты и точную сумму, которую ему должны вернуть.

4. После того, как покупатель повторно вводит данные своей карты, с его счета повторно списываются деньги.

Схема обмана покупателей №3 (Возврат средств)

1. После того, как мошенник реализовал схему «Доставка», он пишет пострадавшему покупателю, представляется службой поддержки Куфара.
2. Говорит, что посылка была не доставлена, извиняется и рассказывает про возможность возврата средств за посылку.
3. Присылает ссылку на фишинговую страницу, где покупателю снова нужно ввести данные своей карты и сумму, которая соответствовала сумме предыдущего списания.
4. После того, как покупатель повторно вводит данные, мошенник снова крадет деньги с банковского счета.

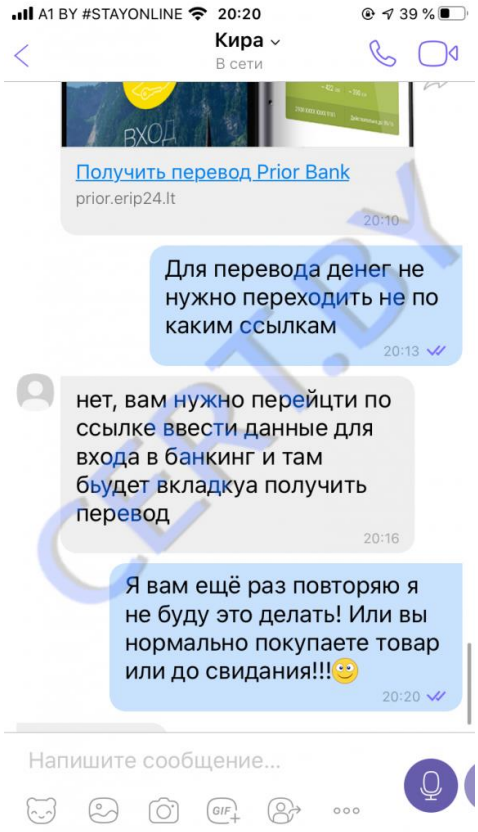
Схема обмана покупателей №4 (Мошенничество с накладными)

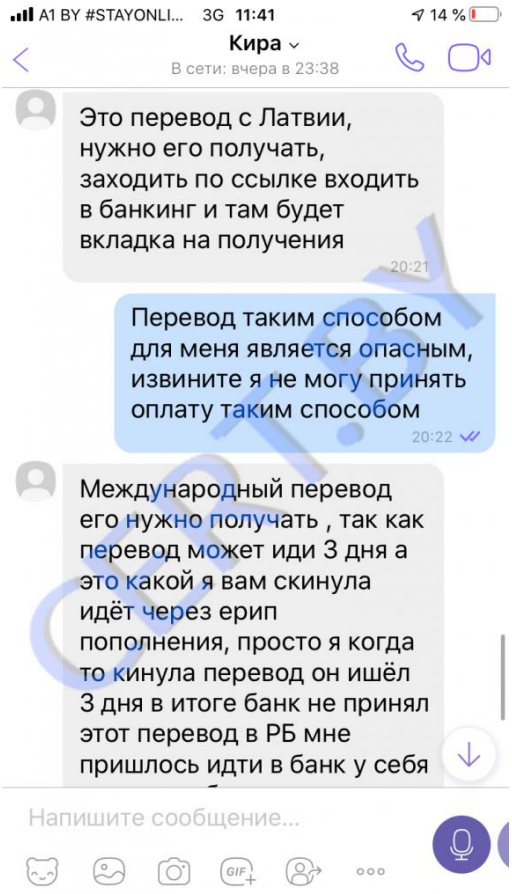
1. Преступник выставляет товар по очень выгодной цене на официальном сайте.
2. Когда потенциальный покупатель пишет ему на Куфаре, под любым предлогом предлагает перейти в мессенджер.
3. Уговаривает отправить товар по почте. При этом мошенник специально создает ажиотаж вокруг объявления. Он может говорить, что буквально на днях уезжает из города, или что товар готовы купить другие покупатели.
4. Продавец говорит, что можно оплатить товар уже после того, как он его отправит, при этом готов предоставить доказательства.
5. Если покупатель соглашается, в качестве доказательства отправки мошенник высылает ссылку на поддельную страницу трекинга посылки или скан поддельного документа об оплате. Минимальное знание фотошопа позволяет преступнику сымитировать квиток любой службы доставки, будь то СДЭК, Белпочта или любая другая компания.
6. После того, как покупатель поверил, что посылка отправлена, мошенник присылает ссылку на фишинговую страницу, где нужно оформить перевод суммы за товар.
7. Как только пользователь вводит данные своей карты, с его счета списываются деньги, а посылка, естественно, не приходит.

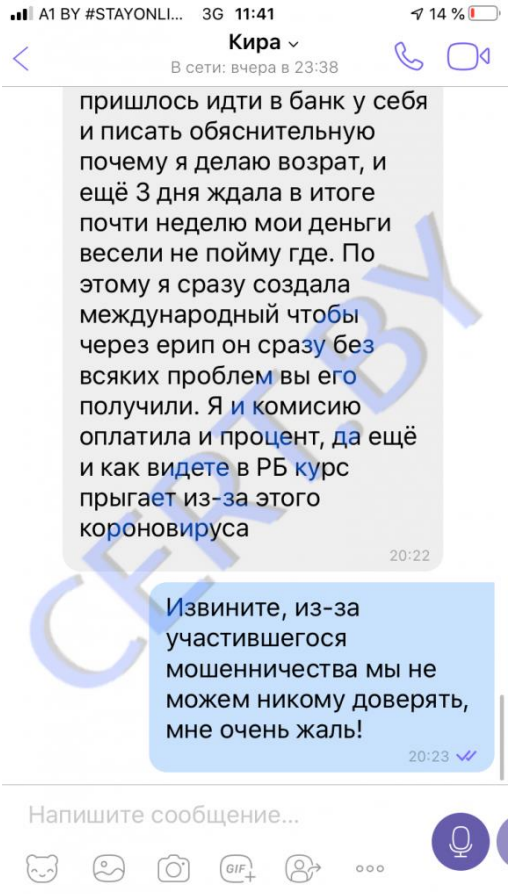
Пример правильного поведения для каждого

Мошенник работал по схеме обмана продавцов №1. Но благодаря очень внимательной и бдительной девушке, в этот раз ничего не вышло. Ей написал «покупатель» в Вайбер по вопросу покупки товара, который она продавала на ресурсе Куфар. Писал мошенник с литовского номера, торопился и очень хотел скорее «оплатить». Но, заподозрив неладное, девушка решила продолжить беседу просто ради интереса.

Что из этого вышло и как может пытаться вводить в заблуждение мошенник можно увидеть на скриншотах, предоставленных нам героиней истории.




A1 BY #STAYONLI... 3G 11:41 14 %
Кира
В сети: вчера в 23:38
Это перевод с Латвии, нужно его получать, заходить по ссылке входить в банкинг и там будет вкладка на получения
20:21
Перевод таким способом для меня является опасным, извините я не могу принять оплату таким способом
20:22
Международный перевод его нужно получать , так как перевод может иди 3 дня а это какой я вам скинула идёт через ерип пополнения, просто я когда то кинула перевод он ишёл 3 дня в итоге банк не принял этот перевод в РБ мне пришлось идти в банк у себя
Напишите сообщение...


A1 BY #STAYONLI... 3G 11:41 14 %
Кира
В сети: вчера в 23:38
пришлось идти в банк у себя и писать обяснительную почему я делаю возрат, и ещё 3 дня ждала в итоге почти неделю мои деньги весели не пойму где. По этому я сразу создала международный чтобы через ерип он сразу без всяких проблем вы его получили. Я и комисию оплатила и процент, да ещё и как видете в РБ курс прыгает из-за этого короновируса
20:22
Извините, из-за участившегося мошенничества мы не можем никому доверять, мне очень жаль!
20:23
Напишите сообщение...

Рекомендации:

1. К любым операциям, производимым с использованием Вашей банковской карты, относится максимально внимательно и осторожно. Терять бдительность никогда нельзя.

2. Для оплаты покупок в Интернете **завести отдельную карту** и не хранить на ней много денег.

3. **Если Вам прислали ссылку** на почтовый ящик, в мессенджер или SMS-сообщением, то, независимо от того кто прислал, даже если это Ваш друг, знакомый, государственный орган или организация, с которой Вы постоянно ведете переписку, или абсолютно незнакомый человек, прежде чем ее открывать, следует особенно внимательно проверить доменное имя. При возникновении малейшего сомнения, что ссылка ведет не на официальный ресурс, ее необходимо проверить. Сделать это можно отыскав в интернете официальный сайт и сверив домен, либо проверив информацию о дате регистрации домена (у фишинговых обычно от нескольких дней до нескольких месяцев) на интернет-ресурсе https://hb.by/whois.aspx или подобные ему (например: https://whois.net, https://whois.domaintools.com) в поле «Creation Date».

Пример информации о дате регистрации официального домена:

Domain Name: **kufar.by**
Updated Date: 2019-07-30
Creation Date: **2010-09-23**
Expiration Date: 2021-10-04

Пример информации о дате регистрации выявленного фишингового домена:

Domain Name: **KUFAR24.SPACE**
Updated Date: 2020-06-21T08:16:28.0Z
Creation Date: 2020-06-21T08:14:10.0Z
Registry Expiry Date: 2021-06-21T23:59:59.0Z

4. **Если ресурс оказался поддельным** либо самому не удается определить, то необходимо сделать скриншот фишинговой страницы (чтобы в адресной строке был виден адрес), и отправить в службу поддержки оригинального ресурса, а также на почту support@cert.by, с описанием подробностей ситуации (например, каким путем получена

ссылка на фишинговый ресурс, вводили ли какие-либо данные и т.д.), после чего отказаться от проведения каких либо операций.

5. **Если стали жертвой мошенников:**

- Если ввели данные банковской карты, то необходимо в срочном порядке произвести ее блокировку, позвонив в банк либо, в интернет-банкинге либо три раза введя неверный пароль, с последующей ее заменой.
- Если ввели авторизационные данные от интернет-банкинга, то необходимо немедленно звонить в банк и сообщить о компрометации учетных данных от интернет-банкинга.
- В случае необходимости обратиться в правоохранительные органы с заявлением о мошенничестве.