⚠️ Скам-кошельки с «щедрыми» seed-фразами

Так называемые «щедрые» кошельки — набирающая обороты схема криптовалютного мошенничества. На разных ресурсах — в тематических чатах, мессенджерах, социальных сетях — может появиться сообщение с просьбой помочь с выводом средств.

🔍 В чем заключается схема обмана

Все сводится к тому, что мошенники на просторах интернета, например, в группах в мессенджерах, в социальных сетях, на тематических форумах и других каналах, публикуют seed-фразу (уникальный набор слов для доступа к криптокошельку) с какой-то просьбой. Чаще всего это призыв о помощи с выводом средств. Все выглядит так, что человек случайно поделился личной информацией о кошельке — по неопытности.

На первый взгляд все выглядит правдоподобно — человек недавно установил криптокошелек, получил на него зарплату или крупный перевод от друга, но еще не разобрался, как эти деньги вывести. Но протягивая ему руку помощи, можно и самому пострадать.

Люди, которые пытаются помочь или просто ради интереса вводят seed-фразу, получают доступ к кошельку и видят на нем крупную сумму средств, например, 5 000 USDT. Все выглядит правдоподобно, кажется, что можно просто отправить эти деньги себе — быстро, гладко и без последствий.

Уловка! Для вывода средств нужно уплатить комиссию — минимум 1-2 доллара. Сложность в том, что оплата предусмотрена в другой криптовалюте, поэтому использовать непосредственно средства аккаунта-мошенника не получится. Например, счет в USDT, а комиссия в TRON, и напрямую конвертировать USDT в TRON невозможно.

Человек решает пополнить счет на недостающую для оплаты комиссии сумму. Но сразу после зачисления валюта исчезает. При повторной попытке внести деньги все повторяется. Так происходит из-за того, что мошенники управляют кошельком через мультиподпись, которая позволяет контролировать его даже при наличии доступа у другого человека.

Важно! Мультиподпись — технология управления криптокошельками, для проведения транзакции она требует нескольких подписей, в отличие от обычных, где достаточно одной — владельца. При настройке пользователь может выбрать количество подписей, которые нужны, чтобы провести платеж. Например, всего есть доступ у 5 людей, а для транзакции достаточно подтверждения от 3. Технология направлена на повышение безопасности кошелька. А все попытки постороннего человека войти в кошелек по seed-фразе и снять деньги оказываются безуспешными.

Может казаться, что 1 или 2 доллара — небольшая сумма, и можно рискнуть. На самом деле мошенники используют прием для большого количества людей. Получая с каждого небольшую сумму, в итоге им удается провернуть крупную кражу.

Такая схема обмана в криптосообществах может принимать разные формы и слегка видоизменяться. Самая распространенная — мошенники маскируются под наивных пользователей, которые не понимают, как выводить средства со старого кошелька. Также могут встречаться сообщения, в которых обещают щедрую награду за помощь с выводом, и другие.

🛡️ Как себя обезопасить

— Не доверяйте seed-фразам, которые вы можете найти на просторах интернета или получить от незнакомых вам людей, особенно если там обещают большие деньги. Со 100% вероятностью это мошенники.

— Не переводите деньги на чужие кошельки. Если для вывода требуется внести средства для покрытия комиссий — скорее всего, это обман.

— Используйте только официальные кошельки и проверенные платформы. Например, Trust Wallet добавил обновление для защиты пользователей и предотвращения мошенничества с мультиподписями.

— Будьте внимательны. Если предложение кажется слишком выгодным — это наверняка обман.

Оставайтесь всегда бдительны и не поддавайтесь соблазну получить легкие деньги.

https://prnt.sc/gI2C2vrvRcCK

https://text.ru/antiplagiat/671b9fd900afa

⚠️ Мошенническая атака с отравлением адресов

В мире криптовалюты уже больше года существует мошенническая атака с отравлением адресов — Address Poisoning Attacks (APA). Любой владелец криптокошелька может попасться на такую уловку. Невнимательность и спешка могут привести к потере значительной суммы средств, вернуть которые не получится.

⚡В чем заключается схема обмана

Мошенники ищут криптоадреса владельцев аппаратных холодных кошельков, на которые с определенной периодичностью совершаются крупные переводы. Например, вы регулярно пользуетесь одним и тем же холодным кошельком и решили отправить какую-то сумму средств другу. Выглядит это как Адрес А, который переводит крупную транзакцию на Адрес В.

Задача мошенников в том, чтобы «запачкать» историю транзакций Адреса А на холодных кошельках. Для этого создается поддельный Адрес С. Он подбирается так, чтобы первые и последние цифры совпадали с Адресом В. Так вы можете легко не заметить разницы, когда захотите повторно отправить другу определенную сумму, ведь не все занимаются поцифровой сверкой данных перед совершением перевода.

УЛОВКА! Мошенники отправляют NFT или небольшое количество монет на Адрес А, например, несколько центов. Такие транзакции обычно выглядят как обычные переводы, получение NFT, уплата комиссии. У получателя не возникает лишних вопросов, а соответственно, и намерений как-то обезопасить себя.

Делаются такие переводы с целью запутать пользователя. Например, если позже начальник будет заходить в книгу транзакций для отправки денег работнику, то есть совершения транзакции с Адреса А на Адрес В, то он может спутать его с мошенническим Адресом С.

ВАЖНО! Зачастую при отправке денег люди сверяют символы адреса, но не все, а только первые или последние. На это и рассчитывают мошенники.

Они повторяют это действие неограниченное количество раз, используя разные адреса, но с совпадающими первыми и последними символами. Таким образом мошенники «отравляют» холодный кошелек, и «поддельные» адреса остаются там навсегда. Дальше все зависит от вас и вашей внимательности.

🛡️ Как себя обезопасить

— Копируйте адреса по специальной процедуре — нажимайте на кнопку «пополнить конкретный кошелек» и используйте этот адрес, а не из истории транзакций. В большинстве из них уже есть встроенная проверка подлинности. Это позволит убедиться в том, что кошелек, куда планируется отправка средств, не поддельный, так как мошенники часто используют адреса, похожие на ваш.

— Скрывайте нежелательные NFT в Ledger Live. Для этого нажмите правой кнопкой мыши на NFT, выбирайте «Скрыть коллекцию NFT».

— Скрывайте нежелательные токены. Для этого нажмите правой кнопкой на токен и выберите «Скрыть».

— Всегда оставайтесь бдительны. Малейшая ошибка может стать причиной потери средств.

🎯От подобных мошеннических атак с отравлением адресом никуда не деться. Можно только обезопасить себя, тщательно сверяя адрес, куда планируется отправка денег. Отослав их мошенникам, вернуть ничего не получится, как и скрыть свои данные. Такова суть работы блокчейна.

И помните, что вы можете пользоваться счетом как обычно. То, что он был «отравлен», не говорит о том, что он взломан. Просто нужно быть внимательнее, аккуратнее и не копировать адреса из истории транзакций.

https://text.ru/antiplagiat/6708c270cd100

https://prnt.sc/1hKFc7uPKZD6

⚠️ Мошенническая схема на P2P-рынке

На площадке Bybit появилась новая мошенническая схема. Она уже коснулась многих пользователей, подобные случаи зафиксированы и на других платформах. При проведении P2P-платежа мошенники отправляют поддельные PDF-чеки, видеозаписи экрана, где якобы отображается подтверждение платежа из банка. И все это выглядит достаточно правдоподобно. Это вводит жертву в заблуждение, что транзакция действительно проведена, и не позволяет сразу распознать обман.

🚨 В чем заключается схема обмана

Рассмотрим схему обмана на примере платформы Bybit. Однако стоит помнить, что используется она на разных ресурсах. Мошенники на площадке Bybit пользуются фальшивыми ПДФ-чеками. Это делается, чтобы отвлечь внимание пользователя, и человек поверил, что перевод средств реальный.

Суть в том, что контрагент создает ордер на платформе, а далее — прикрепляет поддельный PDF-чек. Это создает иллюзию, что средства действительно отправлены, хотя никакие деньги в итоге не поступают. Мошенники приводят аргумент, что транзакция в обработке, но просто задерживается, а чек — подтверждение совершенного платежа. Это уже может указывать на факт подделки. Ранее можно было просто запросить видео из личного кабинета Сбера, и этого было достаточно, чтобы мошенники отменили ордер, а проблема на этом решилась.

Теперь же вместо отмены ордера контрагент скидывает видеозапись экрана, записанную с личного кабинета онлайн-версии банка, например, Сбербанка. На видео достаточно правдоподобно показан перевод в истории. На самом деле сайт ненастоящий. И если уделить внимание деталям, например, расположению элементов, точному URL и др., можно заметить различия. Часто прослеживаются некорректные ссылки, дополнительные переводы, несовпадающие транзакции в случае предоставления сразу нескольких ордеров на разные суммы.

УЛОВКА! Пользователь видит чек и запись экрана, что платеж якобы совершен. Это вводит его в заблуждение. Пользователь полагается на «честность» продавца и «видимость» перевода в чеке и на записи экрана. Затем, пытаясь ускорить процесс, он подтверждает сделку, не проверив фактического зачисления средств. Соответственно, активы сразу же уходят к мошеннику, и выполнить возврат уже невозможно.

Нужно полагаться не на чек, а ориентироваться на фактическое поступление денег на баланс своей карты. Важно проверять зачисление этих средств и только потом подтверждать операцию.

ВАЖНО! Выполнить возврат своих активов не получится. Это невозможно по правилам и площадки Bybit, и любой другой платформы для P2P-торговли. Обращение в службу поддержки с высокой долей вероятности не принесет результата.

🔍 Реальный кейс в качестве примера

Рассмотрим ситуацию, которая недавно произошла на Bybit. Мошенники зашли в две сделки подряд — на 39 700 рублей и 160 000 рублей. Каждую подкрепили поддельными чеками. Пользователь отказался закрывать ордер только на основе чеков. Тогда мошенники записали видео якобы из личного кабинета онлайн-версии Сбербанка. Записано оно было с поддельного сайта, хотя и с высоким уровнем правдоподобности.

Мошенник допустил ошибку в двух разных ордерах. Это можно отследить по видео. На одном из них до якобы совершенной транзакции в 160 тыс. рублей есть на 39 770 рублей, а на другом — уже на 45 тыс. рублей. На самом деле такого не может быть в настоящей истории транзакций. Там отображаются все проведенные платежи, в том числе отменные или забракованные самим банком. Это и позволило выявить, что это не реальный продавец, а мошенник.

❗ Как себя обезопасить?

1. Проверяйте факт проведения платежа. Если приводится PDF-чек и говорится, что платеж ушел в обработку, то с вероятностью 99% это фальшивка.

2. Не закрывайте сделку, пока не дождетесь поступления денег к вам в банк. Ни чеки, ни видео не являются доказательством проведения платежа. Они могут подтвердить только факт мошенничества для службы поддержки площадки.

🛡️ Распространяйте информацию! Делитесь сведениями с другими пользователями. Так о мошеннической схеме будут знать больше людей, которые не окажутся обманутыми и не потеряют свои деньги.

https://text.ru/antiplagiat/671270f6557b1

https://prnt.sc/rp4qau5ijyeS

⚠️ Поддельная служба поддержки на P2P рынке

Одной из самых распространённых схем является мошенничество через поддельную службу поддержки. Особенно часто эта схема встречается на P2P платформах, где сделки происходят между пользователями непосредственно.

В чём заключается схема обмана?

Мошенники находят ваше объявление о продаже криптовалюты на P2P платформе и переходят к этапу сделки.

Вместо того чтобы осуществить реальную оплату на ваши реквизиты, они подтверждают транзакцию на бирже кнопкой «Оплатил». Таким образом, платформа считает, что деньги якобы были отправлены вам. При этом, мошенники не отправляют реальных средств, а ждут некоторое время (обычно 10-15 минут).

По истечении этого времени они подают апелляцию, утверждая, что уже произвели оплату, но не получили криптовалюту. Могут добавить поддельные доказательства, например, скриншот якобы выполненного платежа или фальшивую квитанцию.

УЛОВКА! В момент сделки мошенники начинают писать вам от имени «службы поддержки». Используя эмодзи или изменённый шрифт (например, ⚠️ «Support»:), они пытаются убедить вас в том, что возникла техническая проблема.

Аферисты настаивают на том, что вы должны подтвердить сделку или выполнить дополнительные действия для «разблокировки» вашего аккаунта или средств.

ВАЖНО! Реальная служба поддержки никогда не инициирует разговор через личные сообщения или сторонние чаты. Она связывается с вами только через официальный чат платформы после открытия апелляции.

🛡️ Как себя обезопасить?

— Не поддаваться на провокации! Реальная служба поддержки всегда появляется в чате после открытия апелляции, но вам необходимо дождаться этого момента.

— Не реагируйте на поддельные сообщения от мошенников и тем более не подтверждайте сделку, пока реальный представитель биржи не рассмотрит ситуацию.

🚩 При работе на P2P будьте внимательны, перепроверяйте все этапы выполнения сделки, перед закрытием сделки проверяйте поступления средств. Для консультации по любым вопросам —