ИЗМАМИ И ИЗМАМНИ СХЕМИ С КРИПТОАКТИВИ

БЪДЕТЕ БДИТЕЛНИ И СЕ ПАЗЕТЕ

Бързият растеж на криптоактивите и техните специфични характеристики — глобална достъпност, бързина, анонимност и често необратимост на трансакциите — Ви превръщат в основна мишена за киберпрестъпниците. Измамниците използват сложни тактики, за да Ви измамят, като например „схеми Понци“, фалшиви възможности за инвестиции, безплатни оферти в социалните мрежи и фалшиви съобщения. Те също така използват предложения за романтични връзки с цел инвестиционни измами, както и приличащи си адреси, за да заразят портфейла Ви. Те често се свързват с Вас чрез социални мрежи, приложения за съобщения, имейли и неочаквани обаждания, които звучат реалистично. Може да се сблъскате с рискове като финансова загуба, кражба на самоличност и емоционален стрес.

Бъдете внимателни и следвайте тези ключови съвети, за да сте в безопасност:

Бъдете бдителни за възможни измами и измамни схеми с криптоактиви:
научете повече за различните видове измами и измамни схеми (вж. стр. 5, 6, 7 и 8);

Разпознавайте предупредителните знаци:
научете се да разпознавате подозрително поведение, съобщения или оферти (вж. стр. 2);

Пазете себе си и активите си:
защитете личните си данни (вж. стр. 3);

Научете какво да направите, ако станете жертва на измама или измамна схема
(вж. стр. 4).

Предупредителни знаци

Обещание, което изглежда твърде хубаво, за да е истина.

Непоискана оферта.

Гарантирана бърза и висока възвръщаемост.

Неотложност за действие (напр. предложения за ограничено време, които Ви притискат да действате незабавно).

Искане за плащане чрез непроследими методи (напр. криптоактиви, подаръчни карти, банкови преводи или предплатени дебитни карти).

Покана за кликване върху връзка, сканиране на QR код или изтегляне на приложение.

Искане за изпращане или споделяне на частни ключове и тайни фрази (списък с думи за достъп и възстановяване на Вашия крипто портфейл).

Подозрителен или неправилен URL адрес.

Лого с леки изкривявания — уебсайт, който копира външния вид на уебсайта на истинско дружество или изглежда професионално, но няма потвърдени данни за контакт, информация за регистрацията на дружеството, резултати или потвърдимо присъствие.

Неизвестна платформа за обмен.

Подозрителен прикачен файл, по-специално .exe, .scr, .zip или Office файл с активирани макроси (.docm, .xlsm).

Стъпки за самозащита:

1 Направете пауза и помислете, преди да действате:

Не бързайте да инвестирате, да споделяте информация или да кликвате върху връзки — измамниците умишлено създават усещане за неотложност. В случай на съмнения, дори и незначителни, не действайте или не инвестирайте и проверете източника внимателно.

2 Проверете внимателно източника:

- Винаги проверявайте откъде идват съобщенията, обажданията, имейлите и връзките, дори ако изглеждат официални, изглежда сякаш идват от приятел или Вашето семейство или дори публична личност. Потърсете правописни грешки, странни URL адреси или липсващи индикатори за сигурност, например проверете дали връзката към уебсайта включва „s“ в „HTTPS“, за да се уверите, че уебсайтът е защитен, и проверете за добавени или липсващи букви в името на дружеството.
- Не отваряйте връзки от непоискани съобщения, инсталирайте само официални приложения чрез надеждни магазини за приложения и не сканирайте непознати QR кодове.
- Дори ако дадена оферта изглежда официална, винаги я сравнявайте с уебсайта на дружеството или проверявайте дали профилът в социалните мрежи е потвърден (напр. с официални отметки).
- Използвайте проверени данни за контакт, за да се свържете директно с дружеството или физическото лице и никога не разчитайте на информацията за контакт, предоставена от предполагаемия измамник (напр. потърсете името на дружеството самостоятелно, използвайте проверени бизнес указатели). Измамниците могат да твърдят, че са лицензирани, или да имитират уебсайта на лицензирано дружество. Проверете дали доставчикът на криптоактиви е лицензиран в ЕС, като проверите регистъра на ESMA (↖). Можете също така да посетите уебсайта на Вашия национален финансов орган (https://www.fsc.bg/), за да видите дали са издадени предупреждения или черни списъци или списък I-SCAN на IOSCO (iosco.org/i-scan/).

3 Никога не споделяйте пароли, частни ключове или тайни фрази:

Всеки, който има достъп до тях, може да поеме контрола върху Вашите активи. Лицензираните дружества никога няма да поискат Вашите пароли или кодове за сигурност чрез имейл, текстово съобщение или телефон.

4 Поддържайте устройствата и частните ключове сигурни:

Използвайте силни и уникални пароли за всеки от Вашите крипто профили, пазете паролата си в тайна и избягвайте повторното използване на едни и същи идентификационни данни на различни платформи. Разрешете многофакторното удостоверчване, когато е възможно. Вижте някои съвети за пароли тук (↖). Поддържайте софтуера и антивирусната си защита актуални и активирани.

5 Бъдете внимателни към неочаквани инвестиционни оферти:

Бъдете предпазливи по отношение на инвестициите, които обещават огромна възвръщаемост. Ако звучи твърде хубаво, за да е истина, вероятно не е истина.

6 Помислете, преди да споделяте информация в социалните мрежи:

Чат групи, форуми, публикации в социалните мрежи и снимки могат да бъдат ценни източници на знания за измамниците. Разкриването на твърде много информация за себе си или за Вашите инвестиции може да Ви направи лесна мишена.

Какво да направите, ако сте станали жертва на измама или измамна схема

Незабавно спрете операциите:

За да блокирате всякакви по-нататъшни преводи към подозрителни сметки и да избегнете допълнителни загуби. Прекратете всякакъв контакт с измамниците — игнорирайте техните обаждания и имейли и блокирайте подателя.

Променете паролите си на всички Ваши устройства и приложения/уебсайтове:

Измамниците купуват изтекли пароли онлайн и ги изпробват на множество профили. Промяната само на една парола не е достатъчна; не забравяйте да промените всички пароли, така че измамниците да не могат да ги използват повторно.

Прекъсване и отмяна на достъпа:

Отменете подозрителните разрешения във Вашето цифрово споразумение, които се изпълняват автоматично от блокчейна (интелигентния договор), за да спрете измамниците да харчат Вашите токени без Вашето съгласие. Много портфейли и блокчейн браузери предлагат инструменти, които Ви позволяват да видите кои интелигентни договори в момента имат достъп да харчат Вашите токени. За да направите това, можете:

- да използвате надежден „контрольор на разрешенията“, който проверява дали даден потребител или адрес на блокчейн е упълномощен да изпълнява дадена операция.
- да преразглеждате списъка на одобренията, и
- да използвате бутона „Отмяна“ директно от платформата.

Преместете средствата си:

Ако портфейлът Ви е компрометиран, незабавно прехвърлете останалите си активи в нов защитен портфейл.

Свържете се с Вашия доставчик на криптоактиви:

Информирайте своя доставчик на криптоактиви възможно най-скоро, като използвате официалните канали за контакт, за да проучите потенциалните възможности. Дори ако в повечето случаи не е възможно да се върне операцията в блокчейн, доставчикът все пак може да замрази сметката на измамника (ако тя е на неговата платформа) и да включи в черен списък адреса на портфейла.

Докладвайте и предупреждавайте:

Докладвайте за инцидента на полицията или на Вашия национален орган за финансов надзор (https://www.fsc.bg/) и информирайте Вашата мрежа (напр. приятели и семейство), за да повишите осведомеността. Тези действия са най-добрият начин да защитите себе си и другите.

Пазете се от измами със „стая за възстановяване“ (*recovery room*):

Измамникът може да се свърже с Вас като жертва на предишна измамна схема, като твърди, че е публичен орган (напр. полиция, данъчен или финансов орган и т.н.) и предлага да възстанови загубените Ви пари срещу такса. Това често е поредният опит за измама. Не забравяйте: това, че веднъж сте били измамени, не Ви предпазва от това да бъдете измамени повторно.

Вж. Съвместното предупреждение на Европейските надзорни органи относно криптоактивите, за да научите повече за рисковете, свързани с криптоактивите (↖) и информационния документ „Разяснения относно криптоактивите: Какво значи MiCA за вас като потребител“ (↖).

Европейски банков орган, Европейски орган за застраховане и професионално пенсионно осигуряване, Европейски орган за ценни книжа и пазари, 2025 г.

Люксембург: Служба за публикации на Европейския съюз, 2025 г.

PDF ISBN 978-92-9407-220-7 doi:10.2853/9472615 DZ-01-25-108-BG-N

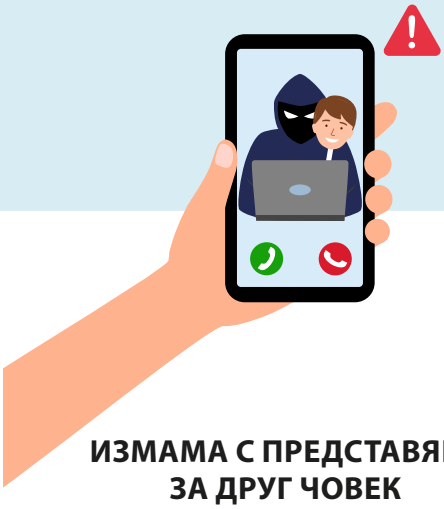
ВИДОВЕ ИЗМАМНИ СХЕМИ С КРИПТОАКТИВИ

СХЕМА „PUMP AND DUMP“ ИЛИ „ИЗДЪРПВАНЕ НА КИЛИМЧЕТО“

Виждате реклама в социалните мрежи или уебсайт, популяризираща „възможност за инвестиции за ограничен период от време“ в криптоактиви, в която се препоръчва да се инвестира в нов крипто токен или проект. След изявен от Вас интерес, се свързват с Вас и Ви пренасочват към платформа за обмен на криптоактиви или канал за съобщения (напр. Telegram, Viber или WhatsApp). Привидно надежден контакт обещава бързи печалби или висока възвращаемост, ако инвестирате бързо. Насърчават Ви да инвестирате малка сума и след това Ви карат да инвестирате повече.

Какво може да се случи:

Откривате, че инвестираният токен е безполезен и контактът, с който сте комуникирали, спира да отговаря. Когато се опитате да изтеглите парите си, уебсайтът вече не съществува, и дружеството е недостъпно. Измамниците изкуствено са надули или надценили криптоактива с ниска стойност, за да увеличат стойността му („pump“), след което са разпродали активите си („dump“), което е довело до срив на стойността и до загуби за инвеститорите. Като алтернатива те могат да закрият проекта и да изчезнат със средствата („издърпване на килимчето“).



ИЗМАМА С ПРЕДСТАВЯНЕ ЗА ДРУГ ЧОВЕК

След като сте публикували въпрос в платформа в социална мрежа или уебсайт за проблем с крипто портфейл, получавате неочаквано лично съобщение (DM) или имейл от някой, който се преструва на доверен контакт (напр. криптоборса, доставчик на портфейл, ИТ поддръжка или дори приятел). Лицето пита за Вашата тайна фраза (т.е. последователност от думи, която служи като централно резервно копие за достъп до Вашия цифров портфейл), пароли или частни ключове (автоматично генериран криптографски код, който доказва собствеността на цифрови активи).

Какво може да се случи:

След като споделите Вашата тайна фраза, пароли или частни ключове, измамникът ги използва, за да откраднe Вашите криптоактиви или други средства. Имайте предвид, че загубата на частни ключове води до постоянна и необратима загуба на достъп и собственост върху Вашите криптоактиви. За разлика от банковите операции, в случай на крипто преводи, след като средствата Ви изчезнат, възстановяването е почти невъзможно.

ФИШИНГ

Получавате неочаквано съобщение по имейл, телефон, изскачащ прозорец или социални мрежи, в което се твърди, че съобщението е от добре познат доставчик на криптоактиви. Съобщението Ви приканва да влезете или да изтеглите ново приложение. Можете също така да получите имейл, който изглежда е от приложението Ви за крипто портфейл, като Ви подканва да разрешите проблем със сигурността, като кликнете върху връзка, предоставена от неофициален източник, или като актуализирате приложението.

Какво може да се случи:

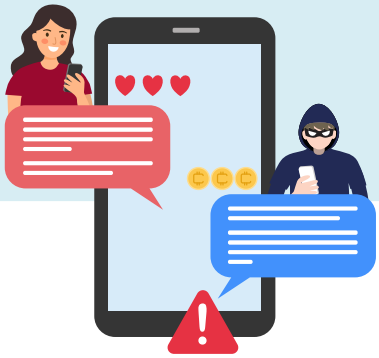
Като кликнете върху връзката, изтеглите приложението или сканирате QR код, Вие всъщност инсталирате зловреден софтуер, който позволява на измамника да има достъп до Вашата информацията и да я използва, за да открадне Вашите криптоактиви или Вашите средства.

ИЗМАМА С ДАВАНЕ НА ПОДАРЪЦИ

Попадате на съобщение в социалните мрежи, в което се твърди, че дружества раздават криптоактиви при условие, че направите малка крипто инвестиция. Тези съобщения съдържат и видеоклип или публикация със снимки на знаменитост или марка — обикновено фалшиви или получени без разрешение — обещаващи да „удвоят криптоактивите Ви“, ако първо изпратите пари. Логото, оформлението, препоръките и използваният език изглеждат професионални и официални, както и уебсайтът, към който сте пренасочени.

Какво може да се случи:

След като изпратите криптоактивите си, не получавате нищо в замяна и сте загубили изпратените пари. Раздаването се оказва фалшиво, а публикацията или излъчването на живо, представящо знаменитости или дружества, са били предназначени да Ви заблудят.



РОМАНТИЧНА ВРЪЗКА С ЦЕЛ ИНВЕСТИЦИОННА ИЗМАМА

С Вас се свързва в социалните мрежи, приложения за запознанства или телефон/ текстово съобщение някой, когото не сте срещнали в реалния живот. Този човек може да участва в чести, лични и романтични разговори, изграждайки доверие, използвайки фалшиви профили. Постепенно насочват разговора с Вас към финансови възможности, претендирайки за огромни печалби от крипто-инвестиции и насърчавайки Ви да инвестирате с обещания за висока възвръщаемост и нисък риск. Те Ви напътстват при създаването на сметка и правенето на малък първоначален депозит, за да изглежда схемата легитимна.

Измамниците създават фалшиви онлайн профили и използват откраднати или генерирани от изкуствен интелект снимки, за да се доближат до Вас.

Какво може да се случи:

Измамникът извлича колкото се може повече пари, след което прекъсва цялата комуникация и изчезва. Измамният инвестиционен уебсайт или приложение е свален офлайн, което Ви оставя без достъп до предполагаемите инвестиции. В някои случаи измамниците могат да използват информацията, получена по време на измамата, за да се насочат към Вашите приятели и семейство, и да извършат кражба на самоличност, която може да има финансови или правни последици за Вас (напр. измамникът може да потвърди откраднати портфейли от Ваше име и може да бъдете подведен под отговорност за дългове или престъпления, извършени от Ваше име, докато не бъде доказано друго).

ПОНЦИ СХЕМА

Поканени сте да участвате в проект, който обещава постоянна висока възвръщаемост от инвестициите в криптоактиви, често подкрепена от препоръки или фалшиви истории за успеха й. Схемата може да бъде представена като маркетингова възможност на много нива, където печелите награди не само от собствената си инвестиция, но и от привличането на други инвеститори. Първите инвеститори изглежда като да получават плащания, което насърчава повече хора да се присъединят и да популяризират схемата.

В действителност не се генерира реален бизнес или печалба. Вместо това средствата идват единствено от приноса на по-нови инвеститори, който се използва за изплащане на възвръщаемост на организаторите и на първите участници в схемата.

Какво може да се случи:

След като новите инвестиции се забавят, схемата се срива и Вие, както повечето участници, губите парите си. Организаторите изчезват, без да оставят възможност за възстановяване на средствата. Многостепенната структура помага на измамата да се разпространи бързо, тъй като жертвите несъзнателно стават промоутъри.

ПОДОБЕН АДРЕС, КОЙТО ЗАРАЗЯВА ПОРТФЕЙЛА ВИ

След като направите крипто операция, забелязвате нов адрес, който се появява в историята на портфейла Ви. Този адрес изглежда подобен на този, с който преди сте взаимодействали. Измамниците могат да накарат фалшивите адреси на портфейла да се появят в историята на операциите Ви, като изпратят малко количество криптовалута от подобен адрес до портфейла Ви. По този начин бихте могли да запазите фалшивия адрес, създаден от измамника, в „скорошната дейност“ на портфейла си или в „автоматичното предлагане“,. Измамниците умишлено създават подобни адреси, като променят само няколко знака, често в средата на адреса, за да избегнат откриването.

Какво може да се случи:

Когато се опитвате да изпратите криптовалута и да копирате грешен адрес от историята на портфейла си, несъзнателно изпращате средства в портфейла на измамника. Тъй като крипто операциите често са необратими, Вашите средства се губят в повечето случаи завинаги. Тази измама разчита на визуална измама и грешка на потребителя, използвайки навика да копирате и поставяте адресите на портфейла без внимателна проверка.