



Воркшоп «Крипта, дропа та безпека: Як не злити всі гроші в мережі»

Що потрібно знати кожному підлітку, який починає працювати з криптовалютою — щоб не втратити гроші назавжди.

Всім привіт! Сьогодні ми поговоримо про те, що люблять усі — про гроші. А точніше про те, як їх у вас намагаються віджати в інтернеті щодня. Хто з вас хоч раз бачив рекламу в ТікТок чи Телеграм у стилі: *"Підними 5000 грн за дві години, схема без ризиків"*? Або *"Розіграш скінів у CS2/Valorant, переходи за лінком"*?

Скамери знають, що підлітки хочуть мати власні гроші та крутий шмот в іграх. І вони цим користуються. Сьогодні ми розберемося, як не стати їхнім спонсором



Інтерактив «Міф чи Факт», Ментіметер,

<https://www.mentimeter.com/app/presentation/alua1kdse6ot2aqb4n/edit?question=96jx4e7a9xn6>

ЧУДОВО!!!!учасники стають в коло. По черзі виходять в центр кола і на якість, талант, уміння. Всі інші учасники, що стоять в колі, хором відповідають



menti.com
3383 0201

Головна помилка новачків

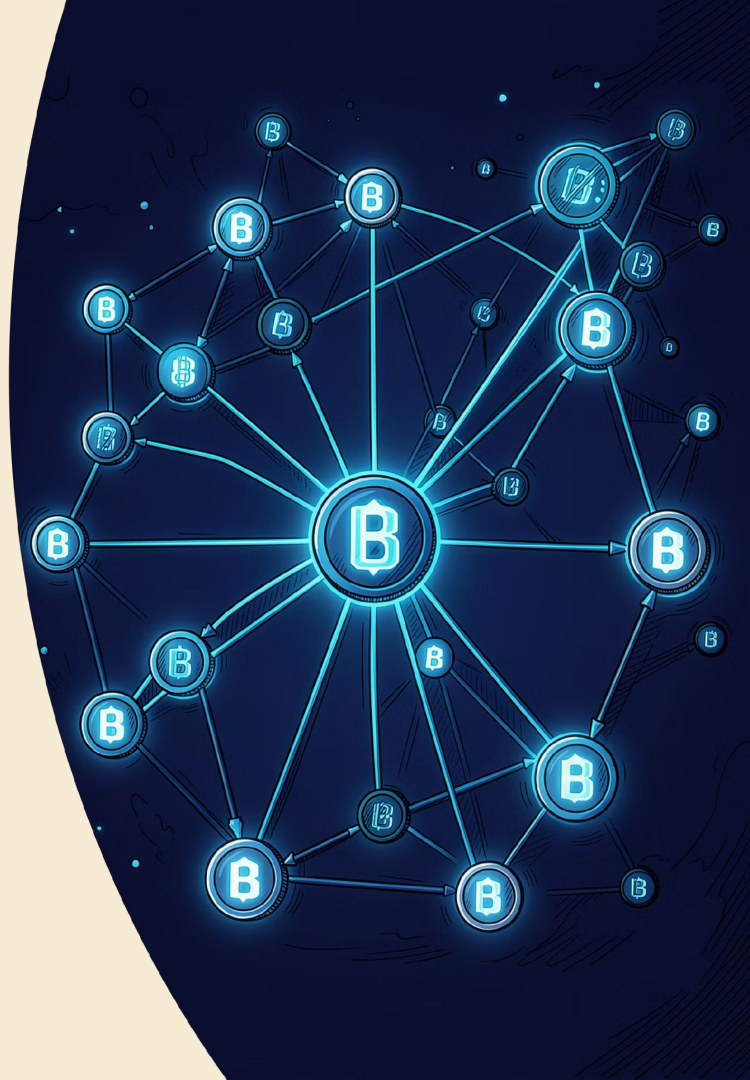
✗ Як здається

Криптовалюта зберігається у додатку на телефоні — як гроші в Монобанк чи Приват24.

✓ Як насправді

Гроші лежать у **блокчейні** — глобальній мережі. Додаток — це лише «віконце», через яке ти на них дивишся.

Якщо додаток зникне — гроші залишаться. Але якщо хтось отримає доступ до твого гаманця — вони зникнуть.



Що таке Сід-фраза?



Сід-фраза — це 12 або 24 випадкових англійських слів, наприклад: *apple, train, window, clock...*

Ці слова перетворюються на **Приватний ключ**, а з нього генеруються всі



Публічний

ключ
Як номер картки — можна давати всім.



Сід-фраза

Ключ від сейфа — дає повний контроль над усіма грошима з будь-якої точки світу.

Аналогія: телефон і сейф

Відновлен
ня
власником

Вводить 12 слів,
кошти повернені
безпечно



Крадіжка на 30
секунд

Невідомий
вводить 12
слів, забирає
монети
МИТТЄВО

Захиститися від крадіжки після передачі сид-фрази неможливо.

Скасувати транзакцію теж не можна — це остаточне рішення

Як шахраї крадуть сід-фразу

1

Сайти-двійники

Сайт виглядає точнісінько як MetaMask. З'являється помилка: **(Фішинг)** "Ваш гаманець заблоковано — введіть Recovery Phrase для верифікації".

2

Фейкова

У Discord/Telegram пише «MetaMask_Support» з офіційною аватаркою. Схиляють сід-фразу, перевірю статус у базі.

техпідтримка

3

Схема

У чатах кидають 12 слів з «200\$ всередині». Щоб вивести — треба закинути \$5 на комісію. Бот миттєво краде їх.

«Загублений гаманець»

Аірдропи та тестнети: де пастка?

Тестнет — тестування нової мережі «іграшковими» монетами.

Аірдроп — безкоштовна роздача tokenів за активність.

Самі по собі — абсолютно легальні та є основою маркетингу у Web3.

Небезпека — у фейкових сайтах аірдропів, які паразитують на бажанні отримати легкий дроп.





Один клік — і гаманець



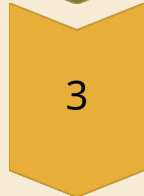
ПЕРШИЙ Connect Wallet

Кнопка безпечна — лише показує адресу



Підпис транзакції

Дрібний шрифт англійською — шахраї маскують шкідливий код



SetApproval ForAll

Підліток думає «забрати \$50», а дає дозвіл безлімітно розпоряджатися грошима



Гаманець очищено

USDT, TON, ETH, BNB, NFT — все вкрадено за секунду

Телеграм-піраміди:



«Сплати податок 10%»,
«верифікація 200 грн» — потім бот

Гучок

гейміфікації
«Орендує майнінг-ферму» або «Купи
гнома за 5% на день»

Ілюзія успіху

Безкоштовний бонус росте, графіки
миготять — система «працює»

Перший внесок

«Купи Супер-ферму за 200 грн» —
невелика сума, підліток ризикує

Реферальне

декло

«Приведи 3 друзів для виводу» —
піраміда затягує інших

Головне правило проти

пірамід
Якщо проект обіцяє фіксований прибуток (1%, 5%, 10% на день)
просто за те, що твої гроші там лежать — це завжди піраміда.



Ознаки

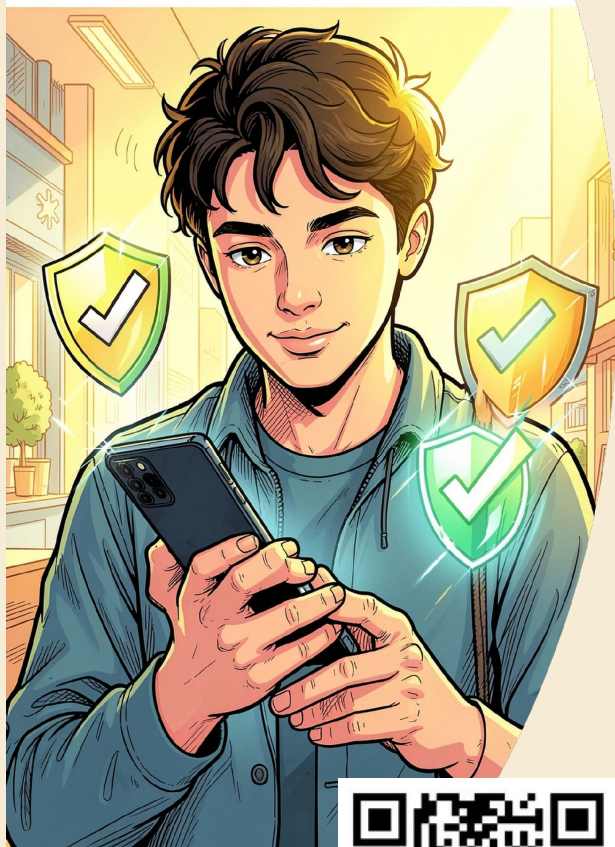
піраміди

- **Гарантований щоденний відсоток**
- **Вивід лише через нових учасників**
- **Тиск «успішними» скріншотами**



Як це працює

Гроші беруться не з «майнінгу» — вони надходять із кишень нових учасників, яких ти привів. Коли нових людей немає — схема розвалюється, а останні учасники втрачають усе.



ПЕРЕГЛЯНЬ!



Пам'ятай ці

Сід-фраза —
нікому.
Навіть

Читай
перед
підписом.

Гарантований
прибуток =
скам.

Офіційні джерела лише. Тільки
перевірені сайти, офіційні

підтвердж
гарантує

Блок 3. Розбір кейсу: прогріви на «Успішний Успіх» в Instagram



nazar_p2p ...

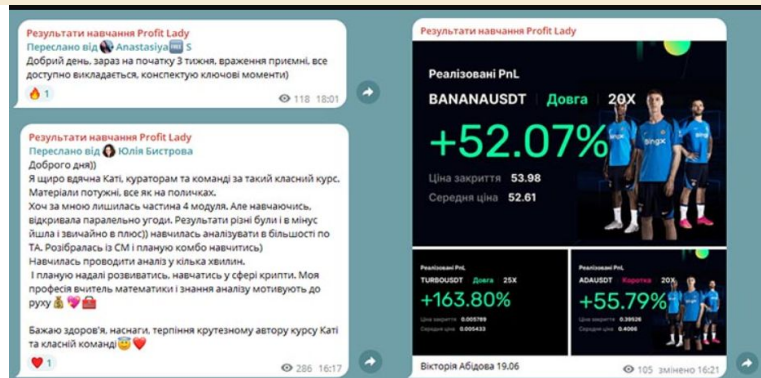
P2P Binance | Арбітраж крипто

9 дописів Читачі: 574 Стежить: 0

Машина з салону за \$45K в 21 📈

Фішки | Схеми | Навчання
+15-20% до капіталу в день 🤖

Допомагаю почати шлях в p2p без злитих бюджетів!!



nikitin.cash ...

📈 NIKITIN CASH І ЗАРОБІТОК | КРИПТА

69 дописів Читачі: 180 тис. Стежить: 54

Блогер

📍 ХАЛЯВНІ 1640UAH для КОЖНОГО ТУТ 📍

(Виплатив вже 565 750 грн (14/79))

🌐 t.me/nikitincash 📞 66 123 533

👤 Стежить kseniia_maliarchuk27 і olga.volkova.1976

Відкрийте додаток Instagram, у пошук слово "P2P зв'язки", Арбітраж крпти або "Signalu crypto" та давайте в реальному часі знайдемо першого-ліпшого "успішного криптана".

https://www.instagram.com/ksu_osypova/

Проаналізуємо його профіль за чек-листом:

Чи є в нього фото з реального життя, чи тільки орендовані машини/готелі?

Чи відкриті коментарі під його публікаціями? (У скамерів коментарі завжди закриті або там лише спам-боти з текстом "Thanks for tips").

Анатомія розводу:

Крок 1. Лампи та Дубай: сторіз із орендованими тачками, пачками грошей, кальянами та дорогим шмотом. Створення картинки: "Я зміг, і ти зможеш".

Крок 2. Псевдо-філантропія: блогер «дарує» підписникам гроші просто так, щоб викликати довіру.

Крок 3. Секретна темка: "Пацани, я знайшов лазівку на криптобіржі, зв'язка дає +20% до депозиту. Викладу безкоштовно в мій ТГ-канал, посилання в шапці".

Крок 4. Фінал: підліток переходить у ТГ, закидає гроші на фейкову біржу за схемою блогера. Гроші зникають, блогер кидає в бан.

Якщо хтось реально знайшов схему, яка генерує мільйони без ризиків, він останній, хто буде кричати про це в Instagram і ділитися з незнайомцями.

Блок 4. Практикум: симуляція фішингової атаки «Знайди 10 відмінностей»



Чек-лист 10 ознак підробки (що мають знайти підлітки):

1. Дивне URL-ім'я: steamcommunity.com (замість і стоїть l) або binance-airdrop-2026.net.
2. Відсутність HTTPS або дивний сертифікат: (хоча зараз і скамери ставлять SSL, але перевірити варто).
3. Неактивні кнопки: на фейковому сайті працює тільки кнопка «Увійти» або «Підключити гаманець», інші посилання (Контакти, Про нас, Політика) ведуть в нікуди або перезавантажують сторінку.
4. Квапливість та психологічний тиск: Таймер зворотного відліку на екрані: "До кінця роздачі залишилось 03:14 хв! Поспішай!"
5. Граматичні помилки: поганий переклад інтерфейсу, помилки в тексті, суміш української та російської/англійської.
6. Fake Live-чат: поп-ап вікно, де «користувачі» в реальному часі начебто пишуть: "Вау, отримав +2500!", але це просто зациклена анімація.
7. Запит надлишкових даних: сайт просить ввести сід-фразу для «верифікації» гаманця (оригінальні сервіси Web3 цього ніколи не роблять).
8. Вікно авторизації всередині вкладки: замість відкриття окремого безпечного вікна браузера для логіну через Steam/Google, вікно малюється прямо на самому сайті (не можна перетягнути за межі вкладки браузера).
9. Занадто щедрі обіцянки: обіцянка подвоїти будь-яку суму, яку ти відправиш на вказану адресу (класичний "Giveaway scam").
10. Поява сайту в Google через рекламу: перше посилання в пошуку з позначкою "Реклама" часто веде на фішинг, який перекупив оригінальний бренд за ключовими словами.

Близнюки Криптобіржі: "Фейковий Аірдроп від Binance" (Трюк з Look-alike доменами)

Тут скамери розраховують на неуважність підлітків, які швидко гортають стрічку новин зі смартфонів. Візуально дизайн сайту повністю завантажується з оригінального брендингу (справжній - <https://www.binance.com/uk-UA>)
ФЕЙК <https://binanceln.com>

Ознака сайту	Справжній Binance 	Фішинговий близнюк 
Адреса сайту (URL)	<code>[https://www.binance.com]</code> <code>(https://www.binance.com)</code>	<code>[https://binance-airdrop.net]</code> <code>(https://binance-airdrop.net)</code> <code>[https://www.binance.com]</code> <code>(https://www.binance.com)</code> (заміна літери i на і з цяткою) <code>[https://binanceln.com]</code> <code>(https://binanceln.com)</code> (заміна букви i на малу l)
Кнопки меню	Усі посилання вгорі та внизу сайту (P2P, Академія, Підтримка, Про нас) клікабельні й ведуть на відповідні сторінки.	Працює лише одна велика кнопка по центру — "Connect Wallet" (Підключити гаманець) або "Claim Bonus". Якщо клікнути на інші розділи меню — сторінка просто перезавантажується або видає помилку.
Елементи тиску	Немає штучного поспіху. Сесія безпечна.	На екрані миготить червоний таймер зворотного відліку: "До кінця роздачі 500 USDT".

Інструменти для перевірки підозрілих лінків

Для миттєвої перевірки репутації домену:
ScamAdviser — сервіс, який аналізує вік сайту, приховані дані власника та відгуки, виставляючи "оцінку довіри" (Trust Score). Якщо сайту всього 2 дні, а він обіцяє роздачу скінів CS2 — це 100% фішинг.

Перевірка файлів та посилань на віруси: VirusTotal — безкоштовний агрегатор, де можна вставити будь-яке посилання на "нову круту інді-гру" або "ТГ-бота" і перевірити його через 70+ антивірусних



URL, IP address, domain or file hash

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Choose file

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#).



Головне правило безпеки в мережі звучить так - якщо пропозиція виглядає занадто ідеально, щоб бути правдою — це розвод. Безкоштовних скінів не буває, легких іксів у крипті без знань не буває, а успішні блогери не хочуть зробити вас багатими просто так. Думайте критично, бережіть свої акаунти та гаманці.

РЕФЛЕКСІЯ



АРТ- ВПРАВА «Думаю критично»,
ліпимо з повітряного пластиліну

ГОЛОВНИЙ ІНСАЙТ СЬОГОДНІ – Хмара слів))

