

Forum:[Hack Forums](#)

Thread: [Anyone getting poison address spam?](#)

Mewtwo - February 13, 2026, 6:11 am

I was looking through my transactions and I've seen that there was someone sending me less than a penny in ETH addresses similar to my Ethereum deposit address.

It went like this: 0xtest....abc
And theirs will be the same but different ...

Kify - February 13, 2026, 9:52 am

Yeah, completely normal.

Think that every address I've ever used that has a balance >1k gets poison spam after every transaction, on Solana more than on Ethereum though. Big transactions can trigger like 20-30 poison spam transactions.

Costanza - February 13, 2026, 9:38 pm

Yeah man i get legit 10+ daily its cooked addy is close to the same too lol

Omniscient - February 14, 2026, 10:39 am

Does this happen on a particular blockchain?

I don't really use much Smart Contract. Mainly Tron and Sui for stablecoins. I see no spam.

Costanza - February 14, 2026, 11:50 am

(Feb 14, 2026 11:39 AM)Omniscient Wrote: [\[CITE\]](#) Does this happen on a particular blockchain?

I don't really use much Smart Contract. Mainly Tron and Sui for stablecoins. I see no spam.
Eth
anytime i send any its gg

Omniscient - February 14, 2026, 11:55 am

(Feb 14, 2026 12:50 PM)Costanza Wrote: [\[CITE\]](#) Eth
anytime i send any its gg

Really, that's interesting. Is it a web3 wallet used on a site or is this like a mobile wallet? Do you just suddenly get a random token?

Costanza - February 14, 2026, 9:15 pm

(Feb 14, 2026 12:55 PM)Omniscient Wrote: [\[CITE\]](#) Really, that's interesting. Is it a web3 wallet used on a site or is this like a mobile wallet? Do you just suddenly get a random token?
Whenever i swap for example changelly and others

Mewtwo - February 14, 2026, 9:20 pm

(Feb 14, 2026 12:55 PM)Omniscient Wrote: [\[CITE\]](#) Really, that's interesting. Is it a web3 wallet used on a site or is this like a mobile wallet? Do you just suddenly get a random token?

Here's an example:

<https://debank.com/profile/0x037c1e88837c3926d1e011b4197c5c2169babfc6/history>

I used the okx wallet for this. As soon as I sent it to the exchange, I started getting those funky ETH spams. 24 txs, at a avg tx cost of 0.005 to send.

It must be really profitable for them if they're doing it on a large scale. 100k tx fees = 12k. One person must be falling a victim.

AI Quote:

There's no single official number, but we can estimate realistically using known phishing-style conversion rates and what blockchain security firms have reported.

Let's break it down logically.

?

? Real-world data (from blockchain security reports)

Security firms like Chainalysis, SlowMist, and PeckShield have observed:

- Address poisoning campaigns hit thousands to millions of wallets
- Only a tiny fraction of users actually send funds to the poisoned address
- But when they do — losses are often large

Typical estimated success rates:

? 0.01% – 0.1% of targeted wallets
(That's 1 in 10,000 to 1 in 1,000)

This is consistent with email phishing, SMS scams, etc.

?

? If scammers send 100,000 poison transactions

Using realistic conversion ranges:

Conservative estimate (0.01%)

- 100,000 targets
- 10 victims

Moderate estimate (0.05%)

- 100,000 targets
- 50 victims

Aggressive / highly optimized campaign (0.1%)

- 100,000 targets
- 100 victims

?

? Why that's insanely profitable

Even if just 10 people fall for it:

If average mistaken transfer = \$2,000

-> \$20,000 revenue

Campaign cost (cheap chain spam) maybe:

-> \$100 – \$500

ROI = massive.

?

? But on Ethereum mainnet specifically...

ETH mainnet users tend to be:

- More experienced
- Paying higher gas
- More careful

So success is usually lower than L2 chains.

More realistic ETH mainnet estimate:

? 0.005% – 0.03%

So for 100,000 poisoning attempts:

- 5 to 30 victims

Still very profitable.

?

? Important psychological factor

Success rate depends heavily on:

- ? Wallet UX (shows truncated addresses)
- ? User behavior (copying from history)
- ? Transaction frequency
- ? Whether victim sends large transfers regularly
- ? Whether they verify full address

High-volume traders and businesses are more valuable targets.

?

? Your personal likelihood (if you're careful)

If someone:

- ? Always checks full address
- ? Uses whitelist / hardware wallet
- ? Never copies from history

Risk becomes extremely low.

Probably:

? Less than 1 in 100,000 per send
(or effectively near zero over time)

Address poisoning mainly catches:

- rushed users
- beginners
- high-frequency senders who rely on history

?

? Simple answer

If scammers send 100,000 poison transactions:

? Expected victims = about 5 to 100 people depending on campaign quality

? Typical realistic range = 10 to 50

?

? If you want deeper analytics, I can show you:

- Real 2024–2025 address poisoning loss totals
- Biggest poisoning scams ever recorded
- Mathematical model of expected profit per campaign
- How often large wallets fall vs small wallets
- How to code a poison-address detector

Just say.

Omniscient - February 14, 2026, 10:26 pm

(Feb 14, 2026 10:15 PM)Costanza Wrote: [\[CITE\]](#) Whenever i swap for example changelly and others Start using Houdini, it's so much better.

Hackers - February 15, 2026, 7:50 am

Yeah unfortunately this is a big problem. People make mistakes and click into recent TX to send to without verifying, so the influx of spam transactions makes sense. It only takes 1 person to pay for the efforts to try to do this to many.

Usually I see a lot more attention spent on the first few & last few of an address.
in a lot of examples they're not even trying to use the same last 4 chars

There are address generators you can make (or use) that will keep hashing until it hits an address w/ a specific string at end. This is how people get cool addresses with their name at the end, but the same can be done to make something look like someone's real, actual address.

Web wallets could make this a lot harder if they started showing first 6 and last 6 instead of

including the 0x in the first 6 and only showing the last 4.

It's not hard to hit a fake address "match" (same end) for only 4... It is harder to nail the first 4 after 0x AND the last 4, but doing it for first 6 AND last 6 would really help....

The more visibility, the better because it's harder to hash a match with 6 compared to 4

Mewtwo - February 16, 2026, 10:41 am

(Feb 15, 2026 08:50 AM)nodes Wrote: [\[CITE\]](#) Yeah unfortunately this is a big problem. People make mistakes and click into recent TX to send to without verifying, so the influx of spam transactions makes sense. It only takes 1 person to pay for the efforts to try to do this to many.

Usually I see a lot more attention spent on the first few & last few of an address.
in a lot of examples they're not even trying to use the same last 4 chars

There are address generators you can make (or use) that will keep hashing until it hits an address w/ a specific string at end. This is how people get cool addresses with their name at the end, but the same can be done to make something look like someone's real, actual address.

Web wallets could make this a lot harder if they started showing first 6 and last 6 instead of including the 0x in the first 6 and only showing the last 4.

It's not hard to hit a fake address "match" (same end) for only 4... It is harder to nail the first 4 after 0x AND the last 4, but doing it for first 6 AND last 6 would really help....

The more visibility, the better because it's harder to hash a match with 6 compared to 4
If I'm not mistaken, a government entity accidentally sent crypto to a poison address. I'm just surprised it's possible to generate something like this, especially first 6 and last 6. That's really a big problem if some people still fall for these.

loadman - February 19, 2026, 12:16 pm

i used to run this bot from a cloud service provider for testing the profitability

rented 100x 4090 costed me around 1.5k\$ per day

Even with all that power, I can only generate 3–6 character addresses, and it takes 3–30 seconds per address.

Second, you have to monitor the mempool to make fast transactions. That also costs money. If you try to run your own dedicated private node for speed, it will cost \$1k per month

also need filters to avoid losing money by sending transactions to hot wallets, contracts, etc.

It's not as simple as "just make a transaction." There's math involved—you have to calculate gas fees, batch transactions, and more.

Sometimes daily cost will be \$1k-5k

but can generate 100k\$-300k\$

Costanza - February 19, 2026, 12:23 pm

(Feb 19, 2026 01:16 PM)loadman Wrote: [\[CITE\]](#) i used to run this bot from a cloud service provider for testing the profitability

rented 100x 4090 costed me around 1.5k\$ per day

Even with all that power, I can only generate 3–6 character addresses, and it takes 3–30 seconds per address.

Second, you have to monitor the mempool to make fast transactions. That also costs money. If you try to run your own dedicated private node for speed, it will cost \$1k per month

also need filters to avoid losing money by sending transactions to hot wallets, contracts, etc.

It's not as simple as "just make a transaction." There's math involved—you have to calculate gas fees, batch transactions, and more.

Sometimes daily cost will be \$1k-5k

but can generate 100k\$-300k\$

So your the type of guy that rapes my wallet with 100 transactions lol

loadman - February 19, 2026, 12:27 pm

(Feb 19, 2026 01:23 PM)Costanza Wrote: [\[CITE\]](#) So your the type of guy that rapes my wallet with 100 transactions lol

not exactly, i just wanted to test the functionality of poisoning transactions, didnt run it for long probably few days, the cost had increased significantly alot, wasnt worth it unless u have 50k-100k\$ to invest

Costanza - February 19, 2026, 12:41 pm

(Feb 19, 2026 01:27 PM)loadman Wrote: [\[CITE\]](#) not exactly, i just wanted to test the functionality of poisoning transactions, didnt run it for long probably few days, the cost had increased significantly alot, wasnt worth it unless u have 50k-100k\$ to invest

Thats crazy it cost that much too , it must work lol

it's not really illegal either is it .

loadman - February 19, 2026, 12:50 pm

(Feb 19, 2026 01:41 PM)Costanza Wrote: [\[CITE\]](#) Thats crazy it cost that much too , it must work lol it's not really illegal either is it .

1.5k\$-2k\$ per day(included rent of private crypto node)

SUI-3183372 - February 19, 2026, 1:11 pm

(Feb 19, 2026 01:16 PM)loadman Wrote: [\[CITE\]](#) i used to run this bot from a cloud service provider for testing the profitability

rented 100x 4090 costed me around 1.5k\$ per day

Even with all that power, I can only generate 3–6 character addresses, and it takes 3–30 seconds per address.

Second, you have to monitor the mempool to make fast transactions. That also costs money. If you try to run your own dedicated private node for speed, it will cost \$1k per month

also need filters to avoid losing money by sending transactions to hot wallets, contracts, etc.

It's not as simple as "just make a transaction." There's math involved—you have to calculate gas

fees, batch transactions, and more.

Sometimes daily cost will be \$1k-5k

but can generate 100k\$-300k\$

What sort of scale were you operating at?

On a singular 5070 Ti I can generate an address that matches the first 4 and last 4 characters of a target address in about 3 seconds using not amazing tooling, which on its own is more than sufficient for a singular poisoning, 3 seconds would be well within your target time frame.

If I had a more powerful card, like a 4090 on a CUDA powered address generator, you could generate probably 3.6 to 4 billion addresses per second. Finding an address that matches the first and last 4 is not that difficult at all, 16^8 for roughly 4B tries, so you'd effectively be generating a valid scam address every second. 100x-ing that to 100 4090's means you're generating 100 addresses per second, which feels like overkill considering ETH rarely exceeds 30 TPS, and even then you wouldn't want to be poisoning absolutely everything.

NoodleBot™ - February 19, 2026, 1:56 pm

I've gotta be honest, in 10+ years of crypto this I've seen like once or twice. Where are you guys posting your addresses that they might be seen? I get it could be random but if you're constantly experiencing it...

SUI-3183372 - February 19, 2026, 2:41 pm

(Feb 19, 2026 02:56 PM)NoodleBot™ Wrote: [\[CITE\]](#) I've gotta be honest, in 10+ years of crypto this I've seen like once or twice. Where are you guys posting your addresses that they might be seen? I get it could be random but if you're constantly experiencing it...

They're simply picking active addresses sending funds, these addresses can be seen on any explorer or indexer.

If you watch an explorer and see address 1 send \$0.10 to address 2, you can reasonably assume, "ok address 1 just sent address 2 a test transaction and will likely follow with a much larger transaction".

The rest you probably know, but for those who don't... If you then generate a brand new address, we'll call it address 3, that has the first 4 and last 4 characters that match address 2, you can then send address 1 a transaction containing just dust. The goal is for your address to appear most recently in address 1's list of wallets that they recently transacted with. Then you just pray that when address 1 goes to send their real full transaction, that they send the funds to address 3 by mistake rather than address 2.

Generally the attackers that do this have some sort of trigger that they're looking for, either transactions that look like they may be a test transaction where they can reasonably assume a follow up transaction will take place, or wallets that send funds to the same address numerous times where you can assume they'll likely send to this address again. You don't normally see wide sweeping poisoning attacks that target absolutely everything and everyone.

Mewtwo - February 19, 2026, 4:57 pm

(Feb 19, 2026 01:41 PM)Costanza Wrote: [\[CITE\]](#) Thats crazy it cost that much too , it must work lol it's not really illegal either is it .

Maybe prosecuted for wire fraud? It'll be super hard to prove intention tbh. There hasnt been any criminal cases with these. Some folks lost millions of dollars from poison addresses. Even the DEA got tricked.

(Feb 19, 2026 02:56 PM)NoodleBot™ Wrote: [\[CITE\]](#) I've gotta be honest, in 10+ years of crypto this I've seen like once or twice. Where are you guys posting your addresses that they might be seen? I get it could be random but if you're constantly experiencing it...
I sent my crypto to OKX and that's when all those spams started happening.

SUI-3183372 - February 19, 2026, 5:23 pm

(Feb 19, 2026 05:57 PM)Mewtwo Wrote: [\[CITE\]](#) Maybe prosecuted for wire fraud? It'll be super hard to prove intention tbh. There hasn't been any criminal cases with these. Some folks lost millions of dollars from poison addresses. Even the DEA got tricked. I don't think a prosecutor would have a difficult time proving intent, their actions paint a pretty clear picture imo. Wire Fraud is probably right.

(Feb 19, 2026 05:57 PM)Mewtwo Wrote: [\[CITE\]](#) I sent my crypto to OKX and that's when all those spams started happening. How quickly did the funds move from your OKX deposit address to a known OKX hot wallet?

Did the spam start before or after that movement.

I'd be curious if they're attempting to detect exchange deposit addresses.

Mewtwo - February 20, 2026, 2:10 am

(Feb 19, 2026 06:23 PM)SUI-3183372 Wrote: [\[CITE\]](#) I don't think a prosecutor would have a difficult time proving intent, their actions paint a pretty clear picture imo. Wire Fraud is probably right.

How quickly did the funds move from your OKX deposit address to a known OKX hot wallet?

Did the spam start before or after that movement.

I'd be curious if they're attempting to detect exchange deposit addresses.

Sent to OKX on: 2026/02/02 10:36:47
OKX sent to hot wallet on: 2026/02/02 10:46:59

The tx spams started happening on: 2026/02/02 11:49:47

<https://debank.com/profile/0x037c1e88837c3926d1e011b4197c5c2169babfc6/history>

There's at least like 24 tx they sent which I just don't understand any purposes why. The wallet is completely empty. Each one has a different address but the same first and last 6 address.

SUI-3183372 - February 20, 2026, 9:16 am

(Feb 20, 2026 03:10 AM)Mewtwo Wrote: [\[CITE\]](#) Sent to OKX on: 2026/02/02 10:36:47
OKX sent to hot wallet on: 2026/02/02 10:46:59

The tx spams started happening on: 2026/02/02 11:49:47

<https://debank.com/profile/0x037c1e88837c3926d1e011b4197c5c2169babfc6/history>

There's at least like 24 tx they sent which I just don't understand any purposes why. The wallet is completely empty. Each one has a different address but the same first and last 6 address.
Yeah, my best guess is they determined that the address you sent to is a deposit address for OKX

and they're hoping they can hijack any future deposits to OKX that you may make.

A lot of transactions, but only coming from 2 actual addresses, each fake address sends 10+ transactions to you.

One group is spending \$0.004132 per transaction to poison

The other group is spending \$0.007308 per transaction to poison

One group gets funded by 0xe206F6650305C05620Fa1753AB24E1c7F5e3E6bE, which is a contract, so they have a nice little system built here. Detect people depositing to exchanges, generate deceptive address, smart contract funds the new address, they send poisoning transactions at a seemingly random interval, numerous times per day. Both groups inexplicably take a few days off before ramping back up at one point, wonder if they're just the same group.

IRLCash - February 22, 2026, 9:23 am

I must be lucky I've never had this happen to me yet but it is starting to become more of a problem in the Crypto world these days.