
CRYPTO
TRACK
CTPRO.IO
ADDRESS
POISONING
ATTACKS

What is Address Poisoning?

An address poisoning attack is a sophisticated crypto scam where scammers create lookalike crypto addresses that closely resemble those frequently used by the victim. They then send small, harmless transactions from these fake addresses to "poison" the victim's address book. The goal is to trick the victim into sending funds to the scammer's address instead of the intended recipient, exploiting the victim's reliance on transaction history for convenience. This type of attack is highly effective and increasingly common in the crypto space.

What is the approach of an Address Poisoning Attack

- Scammers start by analyzing a victim's transaction habits, identifying commonly used addresses.
- Scammers use algorithms to create new crypto addresses that closely mimic the victim's frequent address.
- After creating a convincing lookalike address, the scammer sends a small, innocuous transaction from it, thereby 'poisoning' the victim's address book.

Methods of Attack

Fake Contracts

The fake contract method involves scammers creating a smart contract that sends zero-amount tokens to an address similar to the victim's. This tricks the victim into copying the scammer's address from their transaction history, leading to unintended transfers to the scammer's address.

Breadcrumbing

The breadcrumbing method involves scammers creating a vanity address similar to the victim's and sending small amounts of cryptocurrency to the victim's address. This transaction appears in the victim's history, and the scammer hopes the victim will mistakenly copy the scammer's address, thinking it's their own, leading to unintended transfers to the scammer's address.

Address Poisoning Attack Cases

DEA loses $55K in address poisoning scam

The DEA fell victim to an address poisoning scam, losing $55,000 in seized Tether. The scammer created a lookalike address and sent a small transaction to the DEA's wallet, tricking the agent into transferring funds to the wrong address. Despite efforts to recover the funds, they were quickly converted and moved to different wallets.

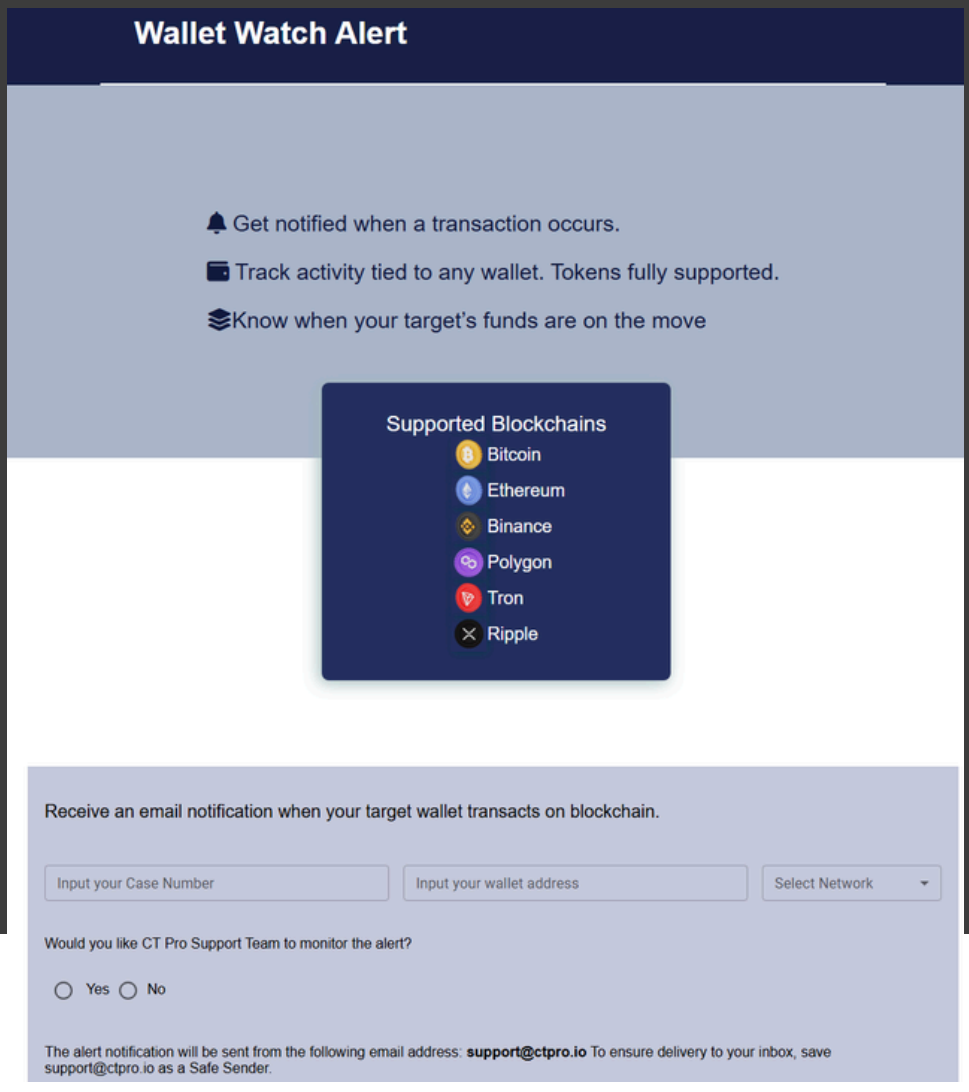
Crypto User Loses $700,000 To Address Poisoning Scam

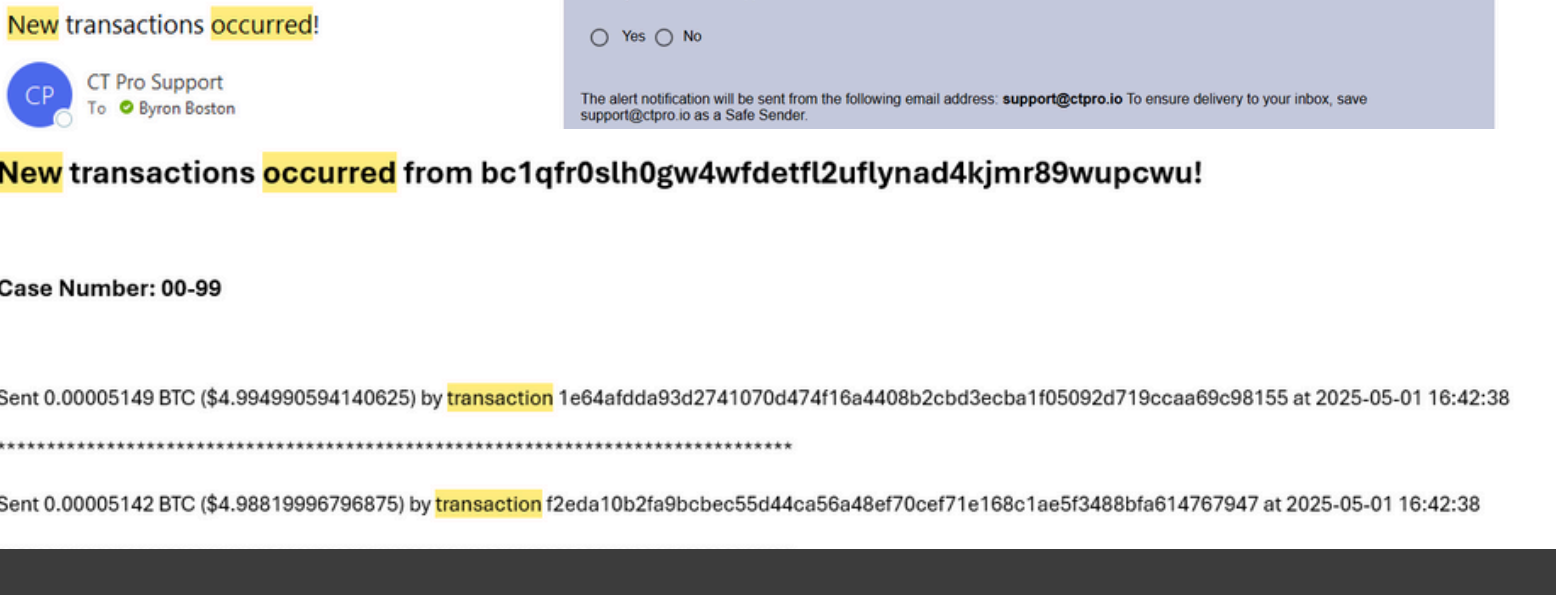
An Ethereum user lost nearly $700,000 in USDT to an address poisoning scam. The attacker created a lookalike address and sent a small transaction to the victim, who then mistakenly copied the scammer's address from their transaction history, leading to the loss. The funds were quickly swapped to DAI and moved through multiple wallets to evade recovery.

How to avoid

Set Alerts

CT Pro enables users to set up alerts for when your agency's wallet address transacts on the blockchain or interacts with specific smart contracts. These alerts can help you verify transactions and ignore others or flag any suspicious activity involving your agency's address.





Crypto Track

Crypto Track PRO is a robust blockchain analytical engine designed to enhance investigative capabilities. As a private forensic firm, we collaborate with U.S. law enforcement as well as international investigators.

We also collaborate with international organizations such as the Cryptocurrency Defenders Alliance which provides us the ability to attempt to quickly blacklist cryptocurrency addresses linked to known criminal activity. This can provide law enforcement with the critical time needed to secure legal documentation and facilitate asset recovery for victims.

Sign up for your free 14-day trial at
https://analytics.ctpro.io/