
ADDRESS
Poisoning
Attacks
CRYPTO
TRACK

ADDRESS POISONING

DEA TARGETED IN LATEST CRYPTOCURRENCY SCAM

THE DEA ACCIDENTALLY SENT $50K OF SEIZED CRYPTO TO A SCAMMER

Address Poisoning is being used to scam people, and no one is safe! Unfortunately, DEA was the latest victim.

The scammer “airdropped” the fake address into the DEA’s account by dropping a token into the DEA account, so it looked like the test payment made to the Marshals.

WHAT IS ADDRESS POISONING?

Address poisoning is a type of phishing scam that has been tricking many crypto users into sending their currency to scammers.

Crypto users use a wallet transaction list, which contains all the incoming and outgoing transfers. Transaction lists provide details about the account, and each address is individualized.
Addresses may show up in short form, showing only the first few digits of the address and the last few digits. It might look something like this: bc1qa.....nhzq.

Scammers “poison” the wallet’s transaction history with addresses that take the same form. However, the tiny dots in the short form are different digits than in the original address, making it easy for users to accidentally send funds to the wrong address. There are two types of address poisoning, fake contract attacks and the breadcrumbing method. Let’s dive into how they work.

Fake Contract

ATTACK

Scammers create a smart contract that send tokens with zero amounts to an address that is similar to the victim's address. This regularly goes unnoticed or without alarm.

The next time the victim tries to make a legitimate transfer, they may copy the phishing address, instead of the intended address - resulting in the transferring of their cryptocurrency to the attacker's address.

Scammers ensure that the address closely matches with the first and last characters. Most people only know and verify the first and last few characters of their wallet.

Breadcrumbing METHOD

In the Breadcrumbing scam the attacker creates a vanity address that is very similar to the victim's address. They then send very small amounts of cryptocurrency to the victim's address, hoping that the victim will check the balance on a block explorer and see the attacker's address in the transaction history.

The attacker hopes that when you see a transaction for a token you typically interact with in your transaction history. You might copy the recipient address think it is your own and then send funds to the address.

sending a small amount of funds to multiple wallets can definitely be expensive, scammers invest millions of dollars paying transaction fees to carry out these address poisoning attacks.

These attacks typically go unnoticed because the transactions appear legitimate and don’t trigger warnings.

STAYING SAFE FROM ADDRESS POISONING ATTACKS

Set Alerts

Adding a tool that will set up alerts to notify when your address transacts with smart contracts and flags suspicious transactions that involve your address – is a great step in protecting yourself.

Create a Contact List

Because the attack works by tricking you into sending funds to a wallet you think is your own or that is trusted. By creating a contact list, you eliminate the risk of the scam.

Use a Trusted Source

Avoid clicking on links or using addresses obtained from untrusted sources. Do not use previous transactions to identify the recipients address without double checking!

Use a Name Service

Name service addresses that are provided by by ENS or BNS will provide additional layers of protection because they are impossible to duplicate, and their short address length makes them much harder to hoax.