Avoiding Crypto Drainers, Approval Phishing and Malicious Smart Contracts

Last Modified on 05/10/2025 2:36 am EDT

Cryptocurrency drainers are malicious smart contracts that allow for wallet to be drained of some or all tokens held in a wallet owner by virtue of the cryptocurrency wallet owner 'approving' the ability for the smart contract to access and send transactions from the wallet. This is also sometimes referred to as 'Approval Phishing.'

As soon as the cryptocurrency wallet owner 'approves' the contract, the attacker can then immediately drain any assets in the wallet that they have approval to send from the wallet; the cryptocurrency wallet owner does not need to enter their seed phrase or wallet password to lose funds to a drainer.

Users can best avoid becoming victims of drainers or approval phishing by carefully authenticating every smart contract they interact with. The vast majority of the time, the wallet owner comes across the malicious approval request from a phishing link that might seem legitimate (i.e. from a seemingly helpful reddit/blog post or youtube video). And users sometimes falsely assume their wallet is safe so long as they don't input their seed phrase.

By carefully authenticating each smart contract you interact with (or avoiding DeFi-related contract interactions entirely) users can help avoid becoming a victim of approval phishing. Also, carefully authenticate each source that provides links that in turn as for approvals.

Apart from that, there are a couple of additional things users can do to mitigate risks:

1. Keep tabs on which approvals you have given from your wallet by using Revoke Cash

2. Utilize multiple wallets rather than just one. Any smart contract approval requests can be performed from a wallet that doesn't hold the majority of your cryptocurrency assets. Consider avoiding approval requests from any cold wallet of yours that stores the bulk of your cryptocurrency assets.