COMMON DeFi SCAMS

A Tactical Guide to
Recognising & Avoiding DeFi Scams

Disclaimer

This playbook is designed to educate and empower you — not to provide financial advice.

Nothing in this material constitutes financial, investment, legal, or tax advice. The examples shared are for illustration and learning, not recommendations to buy, sell, lend, or invest in any specific asset or protocol.

Crypto assets and DeFi activities involve significant risk, including the potential loss of capital. You are solely responsible for your decisions and any actions you take.

Always conduct your own research and, where appropriate, consult a qualified professional before making financial decisions.

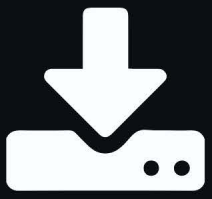
Copyright

THE 3 WAYS SCAMMERS GET IN

Every scam ultimately tries to get you to do just one of three things. If they succeed, they gain access.

Connecting Your wallet to a Scam Site

Signing a transaction on a Scam Site



Downloading Malware onto your system

Scammers are constantly innovating in their approach. In the pages ahead we will see some of their common methods used today.

But no matter how creative the approach becomes, their objective remains to get you to connect your wallet, sign a transaction or download malware.

If you learn to pause before doing any of these three, you dramatically reduce your risk.

Impersonation & Fake Admin Scams

These are commonly found on Telegram, Discord and X, but it's good practice to stay alert across all digital platforms.

Scammers can get VERY pesky. They often copy profile photos, names and even create social handles that look almost identical by replacing letters with characters that resemble them. Some will outright call themselves "admins" or "support."

In most legitimate communities, admins WILL NOT DM you first, unless you have DMed them.

If someone reaches out to you claiming to be support, pause. Verify inside the official community channel before engaging further.

Phishing Links & Fake Giveaways

These scams appear across all platforms and often present themselves as “free gifts,” giveaways, exclusive access, or reward claims. The goal is to get you to download stuff on your device or to sign a blockchain transaction to get a free gift. Once you connect your wallet or sign a transaction, you may unknowingly grant permission for your funds to be moved.

If it looks too good to be true it probably is.

Don’t run after free stuff. If you do believe it could be legitimate, still avoid signing a transaction from your main account. Create a fresh new account that has zero funds. On the Sui blockchain, some known phishing links are flagged on the wallet/explorer, which you can check before interacting. However, proceed with caution — links are typically flagged only after reports from users. The first few victims often encounter the scam before it is publicly marked.

In any case, do not download random stuff from un-trusted sources onto the device that holds your crypto.

Malicious NFT Airdrops

NFTs often appear suddenly in your wallet. Sometimes these are legitimate gifts through partnerships but you want to verify this before signing anything.

Visit the official website and study it. Study their X feed. See if they are endorsed by other credible teams or products on the blockchain.

Even if everything looks legitimate, I highly recommend simply transferring your NFT to a fresh wallet and using that fresh wallet to sign/claim anything you need to claim OR if the NFT claim is account specific, transfer the rest of your assets to another account before signing any transaction..

Even the most seasoned crypto natives have fallen for this so regardless of how reliable it looks, if you don't know what it is, **DO NOT click on it**, do not trust any link it leads to and **DO NOT sign transactions from your primary wallet.**

Fake Calls & Malware Installs

These often come disguised as partnership calls, collaboration proposals or even interview invites.

For the call, the scammer sends a link that looks ridiculously similar to a trusted application like google or zoom. But, the link says you're on an old version of zoom and asks you to update your app. You trust it thinking it is zoom when in fact it is a dubious link installing malware onto your system designed to drain your wallets.

The solution? NEVER download apps through a referred link.

If you need to install or update an app, open your browser yourself and navigate directly to the official website. Download only from there, never from a link someone sends you.

Fake Investment Schemes & Rug Pulls

These can come through many channels — a friend recommending a “great opportunity,” online romance scams, influencer promotions, or private investment groups.

Before investing anywhere, connecting your wallet, or signing any transaction, always consider a few key questions:

- **Is this platform audited?** Can you independently verify the audit from the auditing firm rather than the project’s website?
- **Is this coin a big market cap coin?** How does the value of what you plan to invest compare to the coin’s liquidity? For example, SUI’s liquidity is in the billions so a sale of $1M will barely move the candle for SUI. That’s what you want. Your holdings should be small enough relative to the market liquidity so that your sale doesn’t drastically move the market. So that you can exit your position without crashing the price (thus losing most of the value of your holdings) or getting trapped in an illiquid market.