Common Crypto Scams

Brute Force / Password Leak

This is a scam that originates by Brute Forcing (or social engineering) passwords to one or more of your **online accounts**. If you store your private keys or Seed phrase **in an online account**, you are in serious trouble.

Do Not store your Wallets' seed phrase or private key in online storage. If you absolutely must store it there, make sure you have 2FA enabled on that storage.

Best practice is, when you create a new wallet: Either write down or print out your seed phrase or private key and keep in a very safe place

Risk: Total Loss

Likelihood: Moderate

Avoid:

1. Never store your private key or seed phrase in an online account or digital file that can be read. Key your key/seed offline, hand-written, in a safe or lock box or secure place.
2. If you insist on storing key/seed in online storage, ensure the data is encrypted, that your access password is strong **AND** that you have 2-factor authentication enabled.

Phishing Scam

A fake or lookalike website will prompt you to connect your crypto wallet, then ask you to accept the withdrawal of assets from your wallet.

Risk: Total Loss

Likelihood: Very Common

Avoid:

1. Don't click links that are sent to you or that you see online. Always ensure the URL of the site you are visiting is the expected URL of that site (and not a copy-cat).

2. Never connect your wallet to a website unless you are 100% sure of its authenticity.

Impersonation Scam

Most common on Discord, Telegram or Twitter. Someone will reach out to you, appearing/claiming to be someone else (usually admin of a known group), offering airdrop, support or verification. Eventually with ask for **Seed Phrase/Private Key** or lead to **Phishing site**

Risk: Total Loss

Likelihood: Very Common

Avoid:

1. If someone who appears to be admin of the community you are in, and DMs you. Reach out to them within the group to confirm their identity. 99.9% of the time admins will *NEVER* DM you first.
2. Do not engage DMs that you didn't start yourself, only engage in the main group. Group admins will quickly spot a scammer if they attempt to impersonate within a group chat or channel.
3. If you need support or have a question, use the communities official channels/emails

Airdrop Scam

NFTs or Tokens will appear in your wallet. Usually with a monetary value mentioned ($1000, 2000 USDT, 100 LINK, 100,000 SHIB etc.), They will usually mention a website in the token or NFT (this leads to a Phishing scam site). Once you connect to the site to try and sell your token/nft, they steal the rest of your assets.

If it looks too good to be true, it usually is.

All of my crypto wallets are full of Airdrop scams, best action is no action. If you interact with these airdrops you put yourself at risk of losing everything. Just leave them in your wallet, and do not interact.

Risk: None, unless you try to sell, connect, swap, trade these NFTs or tokens

Likelihood: 100%, once you activate a wallet you are likely to receive airdrop scams

Avoid:

1. If you see a token or NFT that you didn't buy - don't interact with it. Don't transfer, don't try to sell.

2. Expect your wallet to contain some of these trash tokens/NFTs, it's just a fact of crypto. They are worthless though, no matter how valuable they appear or claim to be.

Ponzi / Mutual Fund scams

Projects that claim to give stable % profits no matter what. 90% of the time these are scams. These projects sound realistic on the surface, but in reality, they need new members to buy in, in order to pay the profits of existing members. Generally these project are unsustainable and will eventually fail when new membership slows and their profit mechanism begins to fail

Again - If it sounds too good to be true, it usually is!

Risk: High Risk. People can profit from these scams, but only if you Withdraw your initial investment ASAP. People who invest later, or don't withdraw tend to be left holding the (empty) bag!

Likelihood: Common during Bull markets

Avoid:

1. Don't give your money to people to 'trade' for you.
2. Don't invest in a "sure thing" with "consistent gains", as it's not possible in crypto.
3. Never invest what you aren't willing to lose 100% of.

Pump & Dump / Influencer / Twitter scams

"Hey check out this new meme coin, it's just done 5x but it's gonna be the next 100x coin, guaranteed!"

Wall St. Investors have a saying, that if a guy on the street tells you about a "hot tip" to buy, then it's time to sell. The idea is that, if people are heavily promoting a coin/stock, it usually means they are invested and want **The Public** to buy to pump their investment. And if **The Public** are talking about it, then smart investors are already planning their exit.

The promoter usually has a large holding of the coin/stock and will sell, once people start buying. Remember they already told you they did 5x!

Risk: You will likely buy in at the top, and your investment will tank as the promoter sells everything

Likelihood: Very Common during sideways (boring) markets

Avoid:

1. Trust no-one. High Follower count means nothing, this can be bought on most platforms.
2. If you don't trust them, don't listen. Trust is built over time and by demonstrating integrity and that your goals are aligned. Make someone earn trust, don't give trust blindly.

ICO / New Coin scams

Anyone can create a coin on the blockchain. If you are following a project that plans on releasing a coin, chances are there are scammers watching. If Project A is releasing "Cobra Coin", then you can bet that right around launch time, many different coins with the same name will launch.

The only way to verify the correct coin is via the contract address, which the project team will share with you publicly.

The scammers hope that you mistakenly buy their coin and after a few minutes/hours/days they will pull liquidity, so that you can no longer sell, and they keep any money that was invested

Risk: Lose your investment

Likelihood: Very Common around the time of popular ICO launches

Avoid:

1. Before you buy a coin - verify, verify, verify the contract address.
2. You will not be smarter by trying to watch dexscreener for the new coin to pop up, and beat everyone else to the punch. You will be first on the **WRONG** coin, and you will be stuck holding a worthless bag. Don't do this, wait for the community to officially announce the contract address.

Front-runner Bot scam

You may read articles about how to create a front-running bot to make crazy profits. It will give you code to paste into *remix* (which is an online smart contract editor). It will teach you how to deploy this Contract on the Ethereum blockchain and how to load it with funds. It will suggest you load it with >0.1 ETH to cover gas fees etc.

Once you deploy this contract and send funds to it, the contract will instantaneously send the funds to the scammer.

Risk: You will lose whatever ETH you load the contract with.

Likelihood: Rare, and requires some work on your side to complete the scam

Avoid:

1. Don’t blindly follow YouTube, Medium or Twitter guides on how to create any Crypto bot.
2. If you do follow a guide. Then run the bot on ETH Goerli (test-net) or even use Ganache to run a local ETH chain first to verify that the bot actually does what it says it does.

Man in the middle scam

This is mainly in the crypto marketing space. If you are running a project or community you will very often have “marketers” reaching out offering to promote your project on their socials. There are 3 people involved in this scam. 1 scammer and 2 victims.
The scammer will reach out to you via message and offer promotion services. They will also reach out to a well known promoter and **ASK** them for promotion services for your project. Talking to you they pretend to be the Promoter, talking to the promoter they pretend to be you.

Even if you ask the scammer to verify themselves via another medium (eg. Twitter DM), they will ask the Promoter to DM your twitter account. So you will be none-the-wiser.
The scammer will then ask for payment, and disappear

Risk: You lose the payment you send to the scammer, the promoter loses your potential business

Likelihood: Only common for Community Leads or project Devs

Avoid:

1. This can be hard to avoid as the Promoter here could also be running an Impersonation scam.
2. If you are dealing with someone and ask them to verify via an official Twitter account. Then enquire about payment details on the Twitter DM, rather than on the platform that the interaction began on.