Types of Cryptocurrency Frauds and Scams and How They Work

Last Modified on 05/10/2025 2:39 am EDT

Below is a list of main types of cryptocurrency scams we encounter regularly that lead to a loss of cryptocurrency belonging to a victim. We consider it to be a 'scam' when a victim sends funds, by their own volition, to fraudster(s), typically due to misleading, deceptive, or usually knowingly false information provided to a victim that induces them into sending the funds.

Pig Butchering -- A pig butchering scam or Sha Zhu Pan involves a scammer reaching out to a victim (using a fake name/profile), and working to slowly build up rapport with the victim over weeks or even months. A good portion of this time, the connection is romantic in nature, but not always. Once healthy rapport and trust has been established, the victim will proceed to direct the victim to a fake cryptocurrency trading website, and will suggest the victim invest / trade / use the website. The fraudster will often indicate they use the website as well and have made good money on it -- this is a lie. The fraudster or the 'host' is but a pawn in a large fraud ring -- in some cases the fraudsters themselves are victims of human trafficking by the higher-ups running all the scam operations the ring is part of. The victim is induced into 'investing' more and more through the website, and are comforted by the belief that their new 'friend' has vouched for the website. The investments will often continue until the victim has no money left, and the 'pig' (the victim) has been metaphorically butchered.

Giveaway Scam -- The giveaway scam, involves someone pretending to give away cryptocurrency tokens for free to people who participate. Typically, they will try to get prospective victims to send money first, in exchange for receiving a larger amount back in the future. Example: "Send 1 ETH and get 10 ETH back." As part of the giveaway scam, it is relatively common for the fraudster to impersonate a celebrity, influencer, public figure, or notable company e.g. Tesla, Elon Musk. The scam is relatively simple. Once the victim fulfills the requirements of the scheme, the victim doesn't end up receiving anything back from the fraudster. And there is nothing the victim can do about it to reverse the cryptocurrency transaction they sent to the fraudster.

Malicious Airdrop -- A malicious airdrop is not dangerous, if ignored by the victim. However, often in a quest for free money, a victim will notice an airdrop they were given, and in an effort to realize the proceeds of an airdrop, or in an effort to obtain a new airdrop, they will navigate to malicious websites that will ultimately lead to the wallet becoming compromised, sometimes via approval phishing.

Investment scam -- Investment scams are rife in the cryptocurrency industry. They will often guarantee or suggest that investing through them will be a profitable endeavour. Be very careful anytime you give up control of your cryptocurrency holdings -- when you do, you no longer own that cryptocurrency when you do, and there's no guarantee you'll be able to access that money. Indeed you won't be if it's a scammer you've sent money to.

Fake & fraudulent exchange platforms -- Fraudulent crypto exchanges are incredibly common. Templates for websites, complete with a user registration portal and ability to manipulate gains/losses, are easy to find on the dark web. Users often claim the website "looks legitimate" because they can see the money in their account and all the gains and losses. However, the fraudsters control the platform -- the always make it appear to the victim that a substantial profit has been and is being made in the account in an effort to induce more funds from the victim. The exchange is not real, and the money in the account is also not real. Victims have already lost their money the moment they send money to the fraudulent exchange platform.

Job / Employment scams -- Job and employment scams have become incredibly common, particularly within the past couple of years. Victims are 'hired' and required to deposit money or collateral as part of their 'job', required to pay certain training/license fees, and payments the victims are in turn receiving as part of their job are often

fake/worthless cryptocurrency tokens. Victims are sometimes given various data management tasks to do to make them think it's a real 'job'.

Romance scams -- Romance scams are confidence schemes that delude victims into turning over money for various reasons. Victims are often found on dating apps like Hinge and Tinder. The fraudster operates under a false name and identity, and sometimes false pictures. In some cases, fraudsters will direct victims to a fraudulent investment platform that the fraudster will themselves claim to use. In other cases, the fraudster will claim to be an oil rig worker, miner, or will work in the military (somewhere out of country so that an in-person meeting isn't possible in the near future), and will eventually claim an emergency has come up that they need money for urgently e.g. medical issue.

Ponzi schemes -- A Ponzi scheme involves the operators paying out old investors with money from new investors. In order to keep the investment scheme running, it relies in an ever increasing number of new recruits being onboarded to the scheme so payouts continue occurring. Once that stops or slows down considerably, the scheme collapses. There is not enough money for the scheme to payout everyone's account balances, because much of the money doesn't exist. Any cryptocurrency project, investment platform, or trading platform that offers generous referral fees, guaranteed rates of return, promises 'profitable' investments, has 'downlines', or has other features that are characteristics of Multi-level Marketing (MLM) Schemes, are good indicators of a possible Ponzi scheme.

Impersonation Scams -- Impersonation scams are rife in the cryptocurrency space and come in many forms including:

a) Fake 'customer support' and 'community manager' messages. The fraudster will often pretend to be help/assist the victim under the guise of being a community manager, but instead will direct the victim to a malicious website which will direct the victim to either to input their seed phrase or to "connect" their wallet.

b) Fake social media accounts of cryptocurrency projects, exchanges, wallet providers, etc.. We've seen plenty of fraudsters impersonate us at Cryptoforensic Investigators too!

c) Fake / impersonation websites of crypto projects, exchanges, and wallet providers.

d) Impersonations of notable celebrities, influencers, business leaders, and politicians

Extortion -- Extortion schemes are becoming increasingly more common. While there are real extortion schemes that happen, such as kidnapping and abduction, and Sextortion attempts, there are also fake extortion schemes. In the schemes the fraudster often pretends to be an individual and targets the parents or grandparents of the impersonated individual. The fraudster, pretending to be the victim, will often state they are in some type of trouble and need help e.g. they lost their wallet and phone, or they are traveling and lost their passport, or they were arrested and need money for bail. The goal is to make the parents or grandparents worry about the safety of the person they are impersonating, and get them to send money quickly for their son/daughter or grandson/granddaughters safety. In some cases, fraudsters pretend to be law enforcement officers instead of the victim, and pretend the daughter/son is in jail, in an effort to get the victims to quickly pay 'bail' to get the daughter/son out. These schemes are a bit more research-intensive and targeted since it requires the fraudsters to know names of multiple parties, the relationship these parties have amongst one another, and other background information (e.g. the school the son/daughter goes to), and phone numbers in an effort to seem legitimate.

Fake 'Pro Trader' Scam -- Fake 'Pro trader' scams are relatively common on X/Twitter, Telegram and Youtube. The 'pro trader' will go by a fake name or pseudonym, and will post 'proof' of all their alleged past profitable investments and gains. The profits are fabricated, however. The 'pro traders' , offer to accept money from people who want to invest money with them, in exchange for an alleged commission. The fraudsters will provide with victims with periodic account statements, that include generous purported profits the 'pro trader' allegedly obtained, enticing the victim to invest more. The 'pro trader' does not generate the purported profits they claim --

and often times don't even bother investing or trading the funds at all. When the victim wishes to withdraw their 'account balance' the 'pro trader' declines to send the victim money back.

Address Poisoning -- An address poisoning attack involves trying to get a victim to send money to a visually similar but different address than what they've sent cryptocurrency in the past. This is done by watching user's wallet to see what addresses they send cryptocurrency to. The attacker then sends the victim (sender's) wallet a very small transaction from an address that is very similar-looking to the address the sending wallet has recently sent a transaction to. The hope is that the next time the victim performs a transaction, they simply copy the malicious wallet, thinking it to be a legitimate wallet that they have sent funds to before. This in turn, leads the victim into sending cryptocurrency to the wrong address -- one owned by the attacker. The first few and last few digits of the malicious wallet will likely be the same as the real wallet, thus leading the victim to think the malicious wallet is legitimate.

Comments on Phishing

When victim's inadvertently hand over credentials or permissions to wallets or accounts that allow a third party to take funds, or otherwise get 'hacked' we consider this to be a theft. Phishing, in it's various forms is a great example of this and constitutes one of the Types of Cryptocurrency Thefts, Hacks, and Phishing