Crypto Scams to Avoid


Avoid Crypto Scams

CHICAGO, IL, UNITED STATES, November 10, 2022 / EINPresswire.com/ -- The crypto universe is both fascinating and horrifying, much like the wild west. There are infinite different businesses, games, exchanges, investments, and opportunities available, but there are unfortunately also what appears to be an equal number of dangerous scams that can liquidate accounts before victims even realize what is going on. One bad choice, just a momentary lapse in judgment, can result in rapid and complete account liquidation. The 2022 Crypto Crime Report by Chainanalysis indicates that a staggering $7.8 billion was taken worldwide by crypto scammers in 2020 and $14 billion more in 2021. According to the FTC, in 2021 Americans reported losing $680 million due to crypto fraud. Another $329 million was reported lost in the first quarter of 2022 alone. From the beginning of 2021 through March 2022, over 46,000 Americans reported losses as a result of crypto scams. The team at Best in Crypto developed a reliable crypto directory to help consumers identify reputable crypto businesses in order to help avoid the gut wrenching experience of getting scammed, which is far too common in this developing industry. Several of the most scary and dangerous scams involve hot wallet seed phrase con artists, airdrop phishing, and investment scams including rug pulls.

> I have witnessed many alarming crypto-related scams . These scams can be incredibly deceiving, so learning as much as possible about crypto-related fraud before actually getting involved is critical.”
>
> *Brad Garlin*

Never share seed phrases with anyone! This seems like such a simple rule to follow, but for various reasons, people are far too quick to share this incredibly valuable 12-24 word phrase. There are many examples of criminals attempting to obtain these personal phrases online. In one example on Discord, people were seeking assistance with obtaining the necessary assets in their hot wallets in order to participate in a crypto game. It was admittedly confusing and understandable that people would seek assistance. Help appeared readily available, but from fraud minded individuals who were seeking users’ seed phrases in order to access their wallets in order to "assist." Criminals were disguised behind the illusion of helpful support, but with the ill intent of gaining access to hot wallets in order to drain them. No matter what, do not ever share a seed phrase with anyone. This provides complete ownership access to all contents in a digital wallet. The only place a seed phrase should be shared is on a reliable seed phrase storage device that is stored somewhere incredibly safe and private.

Airdrop phishing occurs in various ways and can deliver devastating consequences, including losing all crypto assets held in a victim's digital wallet. This can be particularly difficult for inexperienced and new investors to identify. Airdrop phishing occurs when random crypto assets are airdropped (meaning to be delivered) to the hot wallets of thousands of potential victims. The real objective of this scam is typically to lure unsuspecting investors to visit a malicious website, posing as a legitimate decentralized exchange, in order to swap or sell these fictitious assets. Don't do it! Never connect a digital wallet to an unfamiliar or untrusted website. With decentralized platforms, there are no safeguards in place to say who is legitimate; it is totally just buyer beware. If investors start granting permissions, or approving any transactions at a phishing website, they are likely unknowingly approving the transfer of all their assets to the scammers and might find their wallet immediately drained. It is up to individuals to ensure that they do not connect their wallets to suspicious websites or simply say "yes" to everything a site asks from them. When a crypto investor feels like something might be a little off, it probably is. There are various versions of the same scam, but the end results in always the same, wallet liquidation.

Crypto investment scams are incredibly common. Rug pulls alone accounted for $2.8 billion in crypto carnage in 2021. Rug pulls involve newly minted coins, or tokens for a game, that are hyped through various means. As demand drives up the price, the original scammers wait for the perfect opportunity to sell all their holdings and disappear. The "Squid Game" crypto scam represents an elaborate rug pull example where the SQUID cryptocurrency token left investors empty handed as the creators disappeared with more than $3 million. In this outrageous scam, the SQUID price skyrocketed more than 300,000% in its first week of trading, rising from less than $0.01 to reach a high of $2,861.80 in just six days. As the developers cashed out, the price literally plummeted back to under $0.01 just ten minutes after reaching its all-time high price, leaving an estimated 40,000 victims wondering what just happened. Nobody is immune; even super-experienced billionaire crypto enthusiast Mark Cuban fell victim as he had an investment in Titan Token that plummeted from $60 to just above $0 the following day. "Even though I got rugged on this, it's really on me for being lazy," Cuban said in an email to Bloomberg.

Sadly, there are countless other crypto scams to lookout for, including blackmail scams, new ICO scams, romance scams, or scammers impersonating celebrities, government agencies, law enforcement, or utility companies. Social media is the most common culprit responsible for initiating these scams, so users must be extra vigilant when engaging web-based crypto opportunities that appear too good to be true. It is likely best to simply ignore them, or prepare for potentially undesirable consequences. Crypto losses have skyrocketed in recent years with losses from crypto fraud in 2021 skyrocketing 56 times higher than they were in 2018. Do not be the next victim, but if it happens, immediately report fraud and other suspicious activity involving cryptocurrency to the FTC at ReportFraud.ftc.gov, and contact a reputable crypto recovery service. Hot wallets are convenient, typically hosted online, and ordinarily secure, but can be susceptible to hacking and scams compared to cold wallets, where crypto is stored offline on a hardware device that is much more secure. Crypto scams are abundant and constantly evolving, so participants in the crypto economy must do their research and prepare wisely for their crypto journey.

Brad Garlin
Best in Crypto
+1 312-219-5510
email us here
