CTPRO.IO

CRYPTO AIRDROPS & ILLICIT ACTIVITY

What Are Crypto Airdrop Scams

A legitimate crypto airdrop is purely promotional and doesn’t require investment. In contrast, scams may involve sending small amounts of cryptocurrency to unsuspecting users, known as dusting scams.

Many airdrop scams trick users into connecting their wallets to phishing sites, often using popular services like MetaMask. Once users enter their secret keys, the scam is complete.

Some scams also entice investors by promising airdrops for holding specific assets, like NFTs. While the airdrop might be real, the project creators could manipulate the market to sell their NFTs at higher prices.

Types of Crypto Airdrop Scams

Phishing scams are a prevalent form of airdrop fraud. In these scams, fraudsters set up fake websites or social media accounts that look like real projects. They often send emails or direct messages with links to these counterfeit sites, tricking users into entering their private keys or other sensitive information. Once they have this data, the scammers can steal the victim’s cryptocurrency.

Advance payment airdrop scams are fraudulent campaigns that pretend to be legitimate. Scammers create fake social media accounts, websites, and promotional content to promote these airdrops. They often ask participants to send a small amount of cryptocurrency to confirm their wallet address or cover transaction fees. Once the payment is made, the scammers vanish, and the promised tokens are never received.

Types of Crypto Airdrop Scams (cont.)

In a malware airdrop scam, people are deceived into downloading harmful software disguised as an airdrop app or wallet. This malware can steal private keys, track keystrokes, or even take control of the victim’s device, resulting in major financial losses.

Impersonation airdrop scams are when scammers pretend to be famous figures in the cryptocurrency world or real project teams to promote fake airdrops. They may use hacked or fake social media accounts to announce these airdrops, tricking users into participating and sharing sensitive information.

How to Avoid Airdrop Scams

To avoid an airdrop scam, it is important to always verify the authenticity of the website or platform projecting the promotion. A legitimate promotion will always have clear information with a clear track record. Also, never share your private keys, seed phrase, or any authentication factors. A legitimate airdrop will never ask for this personal information. Before engaging with any project or promotion make sure to research it to ensure its legitimacy. A legitimate project or promotion is very clear in stating their goals and who’s involved. Be wary of unsolicited messages, emails, or social media posts about airdrops. It may also be beneficial to install and regularly update a security software on your devices. When checking out airdrop-related websites, make sure they use HTTPS and have a valid SSL certificate. Remember, if something seems to good to be true, it most likely is. Trust your instincts and avoid any airdrops that seem unrealistic.

If You Have Been Scammed

If you've been scammed, act quickly. Report the scam to relevant authorities and change passwords for any compromised accounts, using strong, unique ones. Revoke any wallet access granted through the scam and monitor your accounts for unusual activity. If you notice unauthorized transactions, contact your wallet provider or exchange. Consider seeking help from a cybersecurity expert for guidance on securing your assets. Finally, learn from the experience and share your knowledge to help others avoid similar scams.

With access to CT PRO, law enforcement officers can effectively track stolen funds and issue freeze warrants to facilitate the recovery of assets from individuals who have been scammed. For a free 14-day trial sign-up here!

https://analytics.ctpro.io/