Twitter Airdrop Scam Highlights Crypto Phishing Threat to MongCoin Owners

Crypto owners are quickly realizing the threat of airdrop scams happening on social platforms like Twitter.

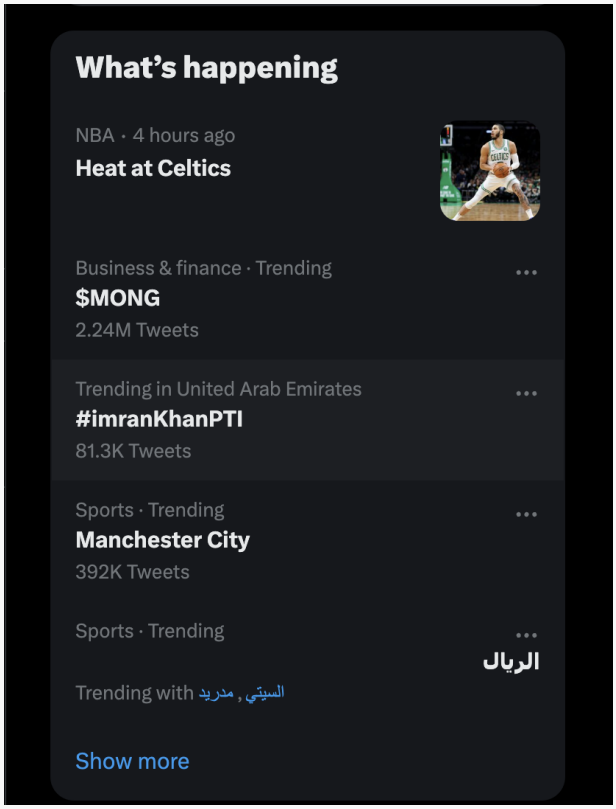
MongCoin

UNITED STATES, May 22, 2023 /EINPresswire.com/ -- Cryptocurrency airdrops were conceptualized as a marketing strategy and during the early days, these drops were associated with people receiving large quantities of coins or tokens for reciprocating a gesture that could drive a crypto brand's value. However, free airdrop tokens that entice users with the promise of getting free coins also come with the threat of millions of crypto funds being stolen. Twitter airdrops started with a simple system where an emerging virtual currency is sent to the crypto wallets of people in the blockchain community who can retweet and help to spread the word about a newly launched currency. A novel idea to market crypto, an airdrop is used by the leading crypto brands to boost outreach, engagement, and awareness levels but when this circulation of airdrops comes with the malintent of scamming the crypto owner—a scan, such as that related to illicit Twitter airdrops, happens.

> There is nothing I won't do for the #MongArmy □□□□□□. There are thousands and thousands of people like me ready to do whatever it takes for $MONG"
>
> *Crytpo Bitlord*

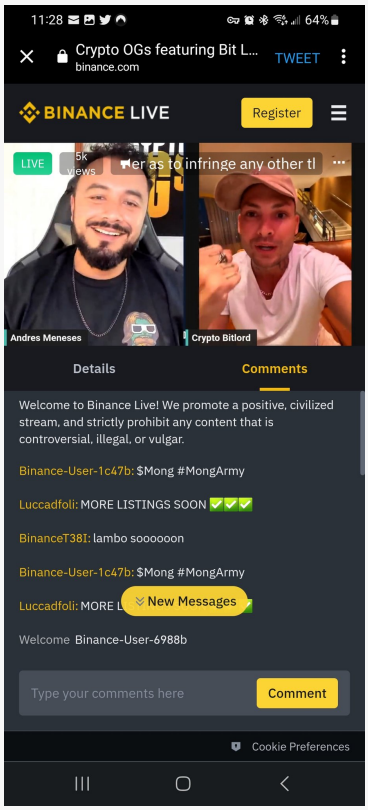
For years, 2018's Coincheck breach was the biggest cryptocurrency hack with a loss of $470 million but it has since been beaten three times, with the 2022 Ronin Nework breach leapfrogging it by almost a third where around $620 million was stolen, which is about the same as the combined GDP of Colorado and Oregon in 2022.

Crypto history suggests that the first cryptocurrency airdrop was attempted by AuroraCoin (AUR) in 2014 and it was geographically specific, for Iceland, aimed at the permanent residents. The drop had a simple confirm-and-reward process where crypto owners who submitted their national ID were slated to receive the goodies. Not just brands but nations, like El Salvador, have executed Bitcoin airdrops since then. As a marketing tool, these drops managed to boost Bitcoin adoption in some way and often drove novel ideas like encouraging the adoption of government-built wallets. The trend has gathered momentum since then and by the end of 2021, token distribution of various types had been attempted as airdropping took a more definitive shape, it also caught the attention of scammers for whom getting access to well-stocked, eligible wallets was perhaps a lure too big to resist.



Business & finance - Trending

The cryptocurrency space has always been about start-up enthusiasm. Harvesting this, digital marketers are always on the lookout for ways to boost a crypto's recognition and hence, its value. Crypto airdrops provide a legit way to do this but the promotional service presents a risk of the trader's or crypto owner's coins being hijacked. These scams are well-dressed, and often choreographed with verified and serious-looking Twitter profiles. When airdrops are announced in Twitter's global space, it becomes hard to identify whether these are fake or genuine tokens appearing on Twitter. This is why the sentiments regarding airdrops have continuously oscillated from being beneficial to fraudulent and the threat is not just to the crypto wallet but also the personal, and often financial, information of the airdrop recipient being illegally accessed and used for bigger financial mishaps.



Crypto Bitlord Interview on Binance Live

A Twitter airdrop can really help a bootstrapped project. If an airdrop manages to get trending, the trading volumes can get a serious boost. However, scammers go to great lengths to ensure the design of the scam is perfected. Such airdrops don't try to raise a conflict with the secured

realms of blockchain-enabled crypto and instead, find ways to get illegitimate access to a crypto owner's wallet. Airdrops are promoted using credible-looking accounts and often, with websites and across multiple social media handles. Further, some airdrops come with a condition where the recipient should hold a minimum quantity of crypto coins in a wallet.

While posting about a currency on a social media platform does not open the door to data phishing, malicious crypto drops can lead to data leakage, as seen, in a recent episode of a PSYOP airdrop scam on Twitter, which lead to massive amounts of the MONG cryptocurrency being wiped away in seconds from the owner's MetaMask wallet. The Mongoose coin, #Mong, while not associated with such scams, has been trending for many weeks on Twitter and its owners seem to be one of the phishing airdrop targets due to its popularity among cryptocurrency enthusiasts. Mong is a decentralized cryptocurrency, riding on the principles of trust and transparency, and the MONG community, #MongMob has been vocal about the worth of static rewards that the platform offers. Mongoose helps to create tokens that can be swapped for funds, and this tokenized environment is gathering momentum with its ability to generate passive income.

Still, phishing attacks were planned using social platforms like Twitter, realizing that stringent data security standards and blockchain at work in the MONG space do not provide any real scope to phish data or tokens—so phishers took advantage of the security loopholes in social handles like Twitter. While the Mongoose Coin community remains strong and is also showing signs of having a conscience with its social initiatives, such phishing attacks are getting smarter and more regular.

For more information about #Mong follow Crytpo Bitlord on Twitter.

Yes, a legitimate, well-intended airdrop helps to stand out and get noticed in an extremely competitive space. A part of CoinDesk's advisory board and an advisor at MIT's blockchain research, Michael Casey, once said that cryptocurrency needs some degree of marketing to succeed and genuine airdrops are doing a job. A schedule of regular and controlled airdrops also means spreading out crypto ownership as more people are likely to explore a new coin on account of getting freebies.

Cryptocurrency phishing grows by 40 percent in one year. Kaspersky's anti-phishing systems have prevented 5 million cryptocurrency-related phishing attacks in 2022, increasing by 40 percent compared to the previous year

Recently, there has been some talk about the threat of Redeeming airdrops. This happens when airdrops want the person claiming the drop to connect a wallet. Here, the wallets can be connected to websites that are part of a scammer's network. Crypto airdrops done in such a way carry a big risk of existing crypto coins being stolen easily and this is why crypto watchers have started warning about the lure of free currency. Similarly, Holder crypto airdrops seek more information about the receiver. The crypto world is big on transparency. A person's existing

tokens cannot be hidden with blockchain data being accessible as a part of the public ledger. While blockchain inspires more visibility of crypto wallets, the tokenized technology also presents an issue as some token owners might be targeted. This is seen in Holder-conscious airdrops where scammers can make the airdrops possible for the highly invested people only, opening up the chances of the biggest wallets being wiped away in an instant.

Perhaps, the best way to keep away such threats is not to go around hunting for crypto airdrops. If an airdrop seems to have the credentials of a genuine offer, it would be a good idea to check out the official company website and branding literature that supports it, such as press releases. Accepting an airdrop armed with such factual data is better than getting washed away in the general excitement regarding free tokens. Another aspect is the status of trading the airdropped tokens—if the gifted tokens cannot be traded, do they serve the wallet holder a real value besides some degree of satisfaction?

Tony Peacock
LinkDaddy®
+1 305-399-9423
email us here