
The Airdrop Gold Rush: Free Money or Fraud Traps?

by *Avi Kamath*, Associate Director, Delta Consulting Group

– July 29, 2025 –

The promise of ‘free money’ makes cryptocurrency investors especially vulnerable to increasingly sophisticated scams.

When Uniswap, a decentralized cryptocurrency exchange, distributed \$6.43 billion¹ worth of its tokens for free in September of 2020², it was capitalizing on a lucrative trend among cryptocurrency enthusiasts. The distribution of crypto coins to ‘people in the know’ through what are commonly referred to as **airdrops** has become a common marketing strategy among blockchain startups and new cryptocurrency networks.

Since airdrops were first introduced in 2014, it is estimated that more than \$26.6 billion has been airdropped³ to lucky users, but where did these billions of dollars of ‘free money’ come from? More importantly, how can you get your share?

Even though everyone has heard the old adage, ‘*If it sounds too good to be true, it probably is,*’ the promise of easy money can compromise the judgment of even the most reasonable and sensible among us. As a result, airdrop events are prime targets for fraudsters. In fact, there are

numerous recent examples of people losing substantial amounts of crypto assets in an effort to get some of this ‘free money.’

What is an ‘Airdrop’?

In simple terms, an airdrop is a free distribution of any crypto asset. While established crypto assets (like Bitcoin and Ether) can be airdropped, it is far more common to see new assets without established market values be distributed for free. Given how easy it is becoming for anyone to issue and distribute their own crypto assets, many airdrops will remain valueless. Increasingly, however, even legitimate and well-established companies in this space are making use of these free distributions.

¹ All dollar amounts referenced herein are in US dollars.

² <https://www.coingecko.com/research/publications/biggest-crypto-airdrops>

³ *Ibid.*

Crypto companies use airdrops as a way of connecting with new users and growing the underlying user base for their platform by leveraging the word-of-mouth recommendations and media attention that these events generate.

There are several different types of airdrops, each requiring a different set of actions in order to receive the ‘free’ crypto asset. The most common types of airdrops used today are:

- Airdrops for using a company’s platform or service
- Airdrops in exchange for completing simple tasks, such as sharing a referral link on one of your social media platforms (e.g., Instagram, X/Twitter, etc.)
- Airdrops for signing up to a newsletter by providing your email
- Airdrops for individuals who hold specified tokens (for example, Ether) in their various crypto wallets as of a certain date, the purpose of which is to quickly attract a tech-savvy userbase (in this example, Ether holders) to their platform or service
- Airdrops for VIP/loyalty members who contribute to a specific project or community

To date, the Uniswap airdrop (the “UNI Airdrop”) is the largest on record, making it a useful example for understanding some of the more common fraud schemes associated with airdrops more broadly.

UNI Airdrop

While the majority of crypto assets are traded on centralized exchanges (i.e., an exchange run by a particular company that is based out of a specified location), people are increasingly using ‘trustless’ alternatives called decentralized exchanges. Decentralized exchanges, such as Uniswap, are considered ‘trustless’ as they require no middlemen or custodians to facilitate trading.

The mechanics underlying Uniswap can quickly become very complicated and are beyond the scope of this article. However, there are some key characteristics that make Uniswap unique. Unlike most exchanges, Uniswap has neither a traditional ‘order book,’ nor does it take custody of any assets in order to facilitate trading. Instead, it allows certain users (referred to as “liquidity providers”) to put crypto assets into liquidity pools, against which other users (referred to as “traders”) can directly swap their crypto assets. The less intuitive aspect is that the crypto assets held in these liquidity pools are secured by computer code rather than an institution like your bank or a centralized exchange.

Liquidity provision is a decentralized finance (or “DeFi”) innovation that is very exciting to crypto enthusiasts due to the income generating potential it brings to assets otherwise held for speculative purposes only. However, it comes with associated risks that once again are beyond the scope of this article.

The qualification requirements for the UNI Airdrop were extremely simple: be a Uniswap user (liquidity provider or trader) prior to September 1, 2020.⁴ Simple enough, so what is the catch? As expected, this unannounced and valuable airdrop created quite the media buzz. While there was no time limit for claiming the UNI Airdrop, there was a ‘mad rush’ to claim and sell these free tokens, which had an approximate value of \$1,376 USD (400 UNI Tokens X \$3.44 USD) on September 17, 2020, the day after the UNI Airdrop became available to be claimed⁵.

In the frenzy to claim the free UNI tokens offered by the UNI Airdrop, scammers and fraudsters were ready to take full advantage. Even in a ‘simple’ airdrop such as the UNI Airdrop, countless things can – and often do – go wrong. Let us look at two real-world examples of fraud schemes that targeted the UNI Airdrop.

Fraud Example 1: “Verify Your Address” Scam

One of the most common types of crypto fraud schemes we’ve seen over the lifespan of cryptocurrencies is essentially an advance fee scheme, whereby the victim is persuaded to pay a small sum of money up front with the promise of a much larger repayment in return.



Image No. 1 – Screenshot of a UNI Airdrop “Verify Your Address” Scam

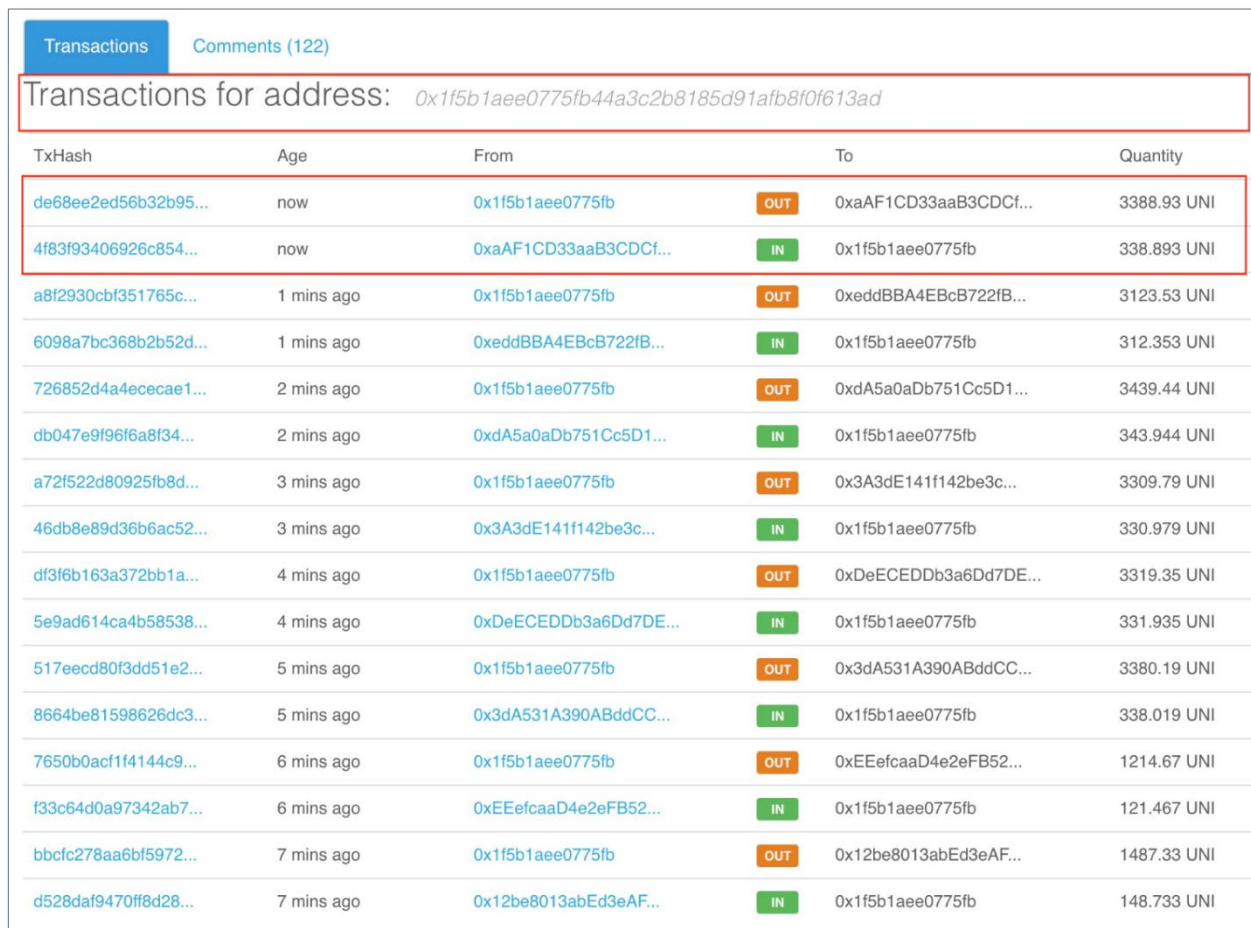
⁴ <https://web.archive.org/web/20210205013100/https://uniswap.org/blog/uni/>

⁵ https://www.coingecko.com/en/coins/uniswap/historical_data?start=2020-09-15&end=2020-10-08

The image above shows a ‘UNI Airdrop’ scam, which gives the impression that 10 million UNI tokens are being given away, as indicated by the red/black bar at the bottom of the picture. This visual depiction conveys a sense of urgency as it implies that a majority of the finite available UNI tokens have been claimed.

In order to ‘claim’ these purported UNI tokens, users were required to ‘verify their address’ by sending between 40 and 4,000 UNI to the address [0x1f5b...613ad](#), and in return, they would be sent back between 400 and 40,000 UNI. The fraudulent promotion states, “1. To make a transaction, you can use any wallet or exchange that supports UNI. 2. Send a small amount you want multiplied by the promotion from your wallet. For example, to get 3000 UNI, send 300 UNI. You can use any wallet or exchange of choice to send UNI. 3. Once we receive your identifying transaction, we will immediately send the requested amount back to you.”

These scammers even go as far as to show you the purported transaction history of the [0x1f5b...613ad](#) address on the Ethereum network, depicted in Image No. 2, which falsely shows that they have returned 10x to other users as promised, thereby giving a degree of confidence to the victim.

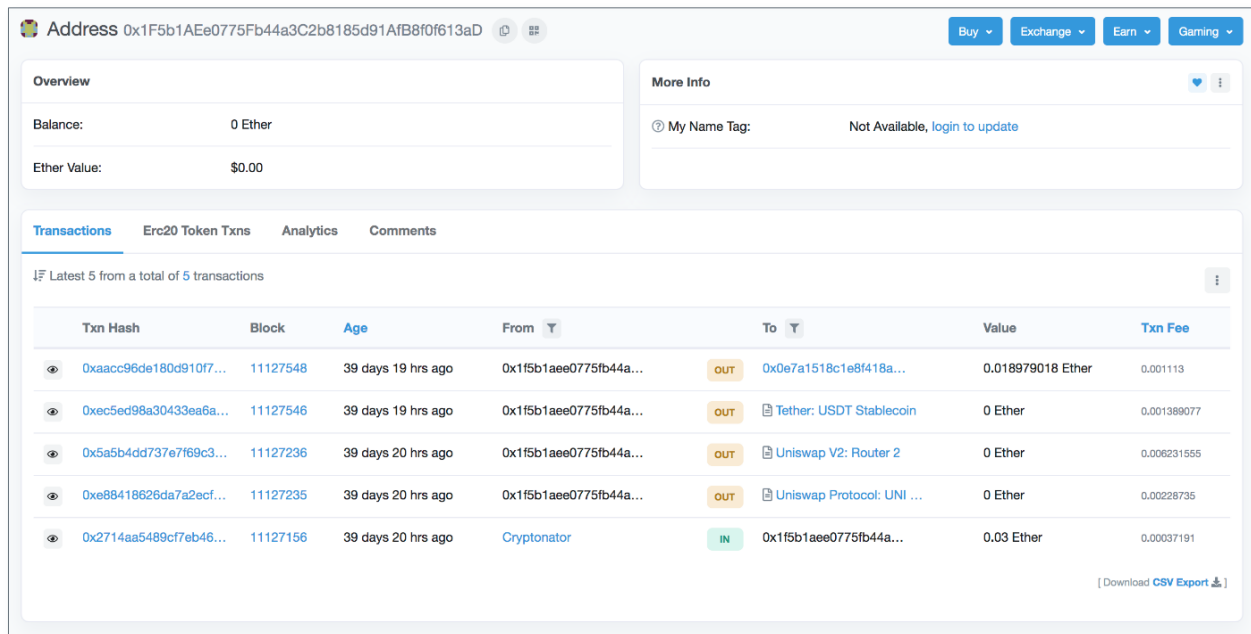


TxHash	Age	From	To	Quantity	
de68ee2ed56b32b95...	now	0x1f5b1aee0775fb	OUT	0xaAF1CD33aaB3CDCf...	3388.93 UNI
4f83f93406926c854...	now	0xaAF1CD33aaB3CDCf...	IN	0x1f5b1aee0775fb	338.893 UNI
a8f2930cbf351765c...	1 mins ago	0x1f5b1aee0775fb	OUT	0xeddBBA4EBcB722fB...	3123.53 UNI
6098a7bc368b2b52d...	1 mins ago	0xeddBBA4EBcB722fB...	IN	0x1f5b1aee0775fb	312.353 UNI
726852d4a4ececae1...	2 mins ago	0x1f5b1aee0775fb	OUT	0xdA5a0aDb751Cc5D1...	3439.44 UNI
db047e9f96f6a8f34...	2 mins ago	0xdA5a0aDb751Cc5D1...	IN	0x1f5b1aee0775fb	343.944 UNI
a72f522d80925fb8d...	3 mins ago	0x1f5b1aee0775fb	OUT	0x3A3dE141f142be3c...	3309.79 UNI
46db8e89d36b6ac52...	3 mins ago	0x3A3dE141f142be3c...	IN	0x1f5b1aee0775fb	330.979 UNI
df3f6b163a372bb1a...	4 mins ago	0x1f5b1aee0775fb	OUT	0xDeECEDDb3a6Dd7DE...	3319.35 UNI
5e9ad614ca4b58538...	4 mins ago	0xDeECEDDb3a6Dd7DE...	IN	0x1f5b1aee0775fb	331.935 UNI
517eecd80f3dd51e2...	5 mins ago	0x1f5b1aee0775fb	OUT	0x3dA531A390ABddCC...	3380.19 UNI
8664be81598626dc3...	5 mins ago	0x3dA531A390ABddCC...	IN	0x1f5b1aee0775fb	338.019 UNI
7650b0acf1f4144c9...	6 mins ago	0x1f5b1aee0775fb	OUT	0xEEefcaaD4e2eFB52...	1214.67 UNI
f33c64d0a97342ab7...	6 mins ago	0xEEefcaaD4e2eFB52...	IN	0x1f5b1aee0775fb	121.467 UNI
bbcf278aa6bf5972...	7 mins ago	0x1f5b1aee0775fb	OUT	0x12be8013abEd3eAF...	1487.33 UNI
d528daf9470ff8d28...	7 mins ago	0x12be8013abEd3eAF...	IN	0x1f5b1aee0775fb	148.733 UNI

Image No. 2 – Purported Transaction History on Scam Website

As we can see from Image No. 2, address [0x1f5b...613ad](#) appears to have received 338.893 UNI tokens and then immediately sent back 3,388.93 UNI tokens, giving the impression that the scammer is sending the user back 10x the amount they originally sent. It is noteworthy that the other transactions in this transaction history reflect this same ratio (i.e., immediately sending back 10x the UNI tokens received).

However, if you were to actually look up the address [0x1f5b...613ad](#) on a blockchain explorer (a basic due diligence step you should always do), you would see a very different picture painted:



Txn Hash	Block	Age	From	To	Value	Txn Fee
0xaacc96de180d910f7...	11127548	39 days 19 hrs ago	0x1f5b1aee0775fb44a...	OUT 0x0e7a1518c1e8f418a...	0.018979018 Ether	0.001113
0xec5ed98a30433ea6a...	11127546	39 days 19 hrs ago	0x1f5b1aee0775fb44a...	OUT Tether: USDT Stablecoin	0 Ether	0.001389077
0x5a5b4dd737e7f69c3...	11127236	39 days 20 hrs ago	0x1f5b1aee0775fb44a...	OUT Uniswap V2: Router 2	0 Ether	0.006231555
0xe88418628da7a2ecf...	11127235	39 days 20 hrs ago	0x1f5b1aee0775fb44a...	OUT Uniswap Protocol: UNI ...	0 Ether	0.00228735
0x2714aa5489cf7eb46...	11127156	39 days 20 hrs ago	Cryptonator	IN 0x1f5b1aee0775fb44a...	0.03 Ether	0.00037191

Image No. 3 – Actual Transaction History of Scammer’s Wallet Address⁶

Image No. 3 tells the real story – the account in question has a total of five transactions, none of which match the transactions displayed on the scammer’s website. This should leave no doubt in your mind that someone is trying to defraud you out of your crypto assets.

If this scam sounds familiar, it is because a variation of it was in the news back in 2020, when we saw a host of well-known business giants (including Jeff Bezos, Bill Gates, Eric Schmidt, Steve Wozniak, Daymond John and Elon Musk) peculiarly appear to promote what turned out to be fake Bitcoin (“BTC”) giveaways that required users to first send some BTC in order to receive a larger amount back⁷.

⁶ <https://etherscan.io/address/0x1f5b1aee0775fb44a3c2b8185d91afb8f0f613ad>

⁷ <https://news.bitcoin.com/elon-musk-bitcoin-giveaway-scam-millions-dollars-btc/>

For example, the ‘Elon Musk Bitcoin Giveaway’ asked people to send BTC to an ‘Elon Musk’ address provided by the scammers and promised to return twice as much BTC immediately. Needless to say, no BTC was returned to the victims and the scammers made off with at least 214 BTC⁸, which, as of July 2025, is worth in excess of \$21.4 million USD. The mechanics of this scheme are almost identical to the UNI scheme outlined above.

While most seasoned crypto users would have immediately recognized this ‘advance fee scheme’ as one of the most common forms of crypto fraud, there were many other more complicated scams relating to the UNI Airdrop that savvy fraudsters perpetrated.

Fraud Example 2: “Phishing” Scam

On September 16, 2020, most people who received the UNI Airdrop were looking to claim and sell their UNI tokens quickly, as these tokens were trading for considerable value. Both novices and seasoned crypto users rushed to claim and sell their UNI tokens, and the price of “gas” (the transaction fees required to complete a transaction on the Ethereum network) skyrocketed. This steep rise in gas, coupled with the inherent price volatility of crypto assets in general, further perpetuated the sense of urgency.

In fact, this rush to claim and sell the UNI tokens had a quantifiable impact on the Ethereum network, resulting in an increase in transaction costs by a factor of almost 5. This is due to how priority is given to transactions on the Ethereum network. Since transactions are prioritized by the amount of gas the user is willing to pay per transaction, users looking to have their transactions processed quickly can rapidly bid up the transaction costs for all users. Image No. 4 below demonstrates the fluctuation in gas prices between June and September 2020.

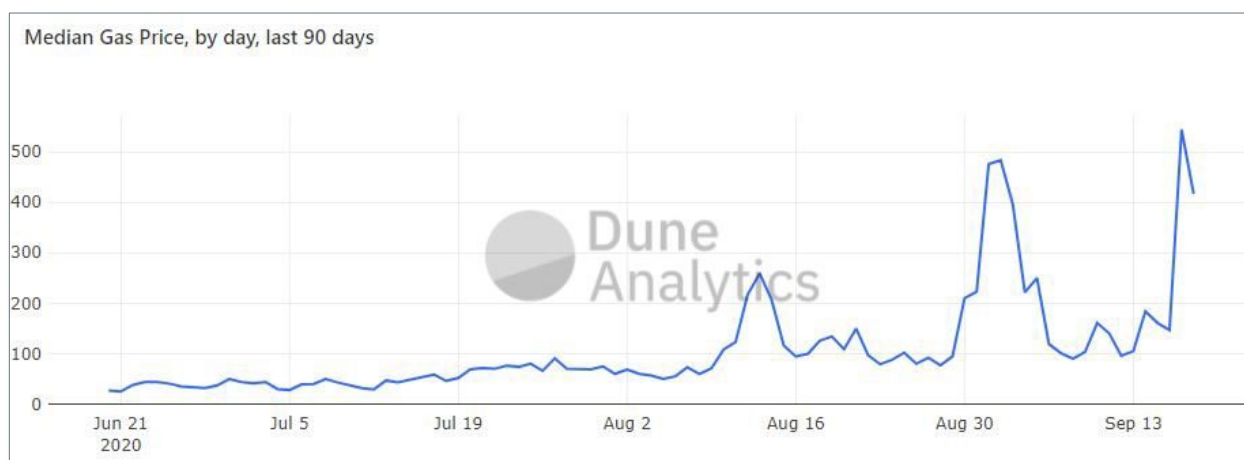


Image No. 4 – Ethereum Network ‘Gas’ Price (June to September 2020)⁹

⁸ Ibid.

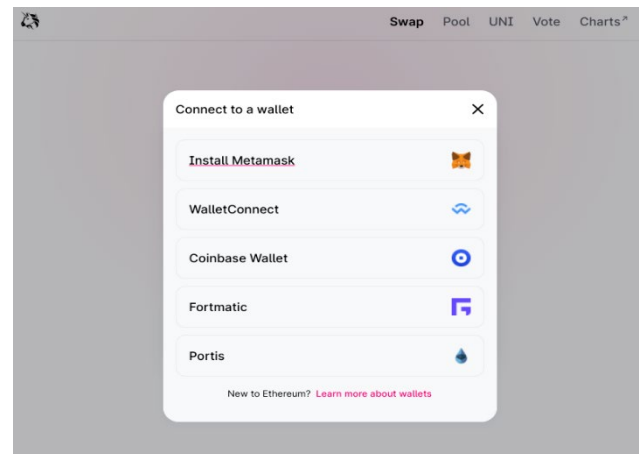
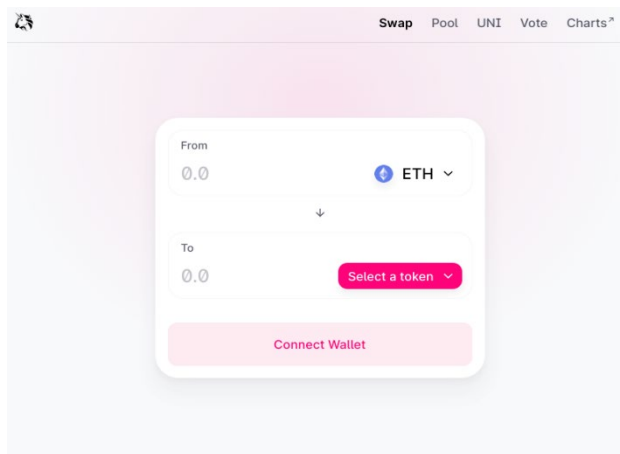
⁹ Source: Dune Analytics

Volatile token prices and transaction fees create the perfect conditions for even seasoned crypto users to make errors that could cost them far more than the free money they hoped to gain.

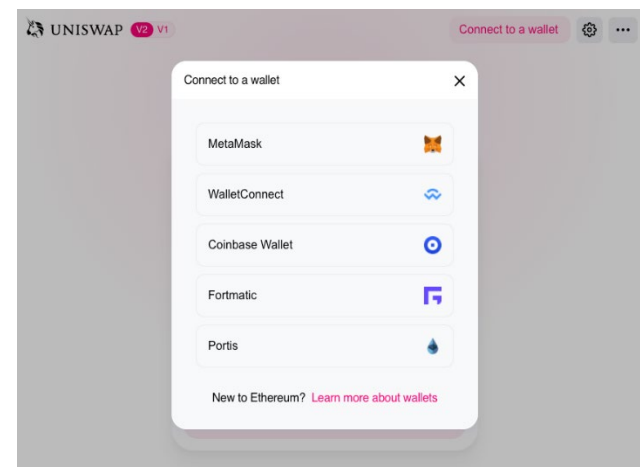
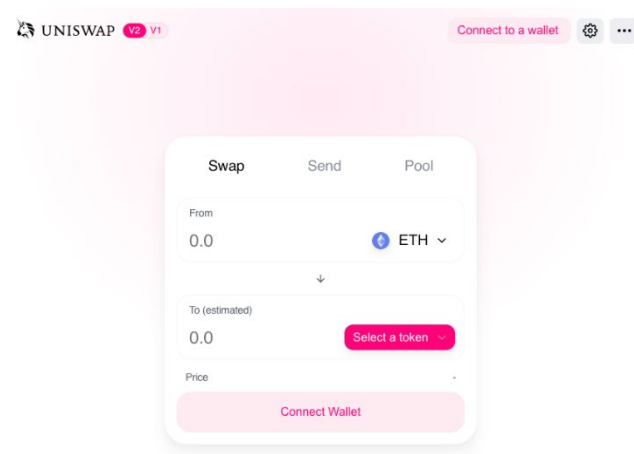
An extremely common malicious tactic used by criminals is to set up ‘phishing’ websites that request your seed or private key, which are the underlying credentials that give users access to their cryptocurrency (comparable to login information to an online bank account).

For example, take a look at the series of screenshots below. Series 1 is taken directly from the Uniswap website and Series 2 from a fraudulent site trying to pass itself off as Uniswap.

Series 1 (From Uniswap Website):



Series 2 (From Fraudulent Website):



Could you have identified which one is legitimate, and which one is not? The two series look almost identical, from the branding to the website’s user experience. The only real difference is that upon trying to connect with the malicious website, users are prompted with an error message as follows:

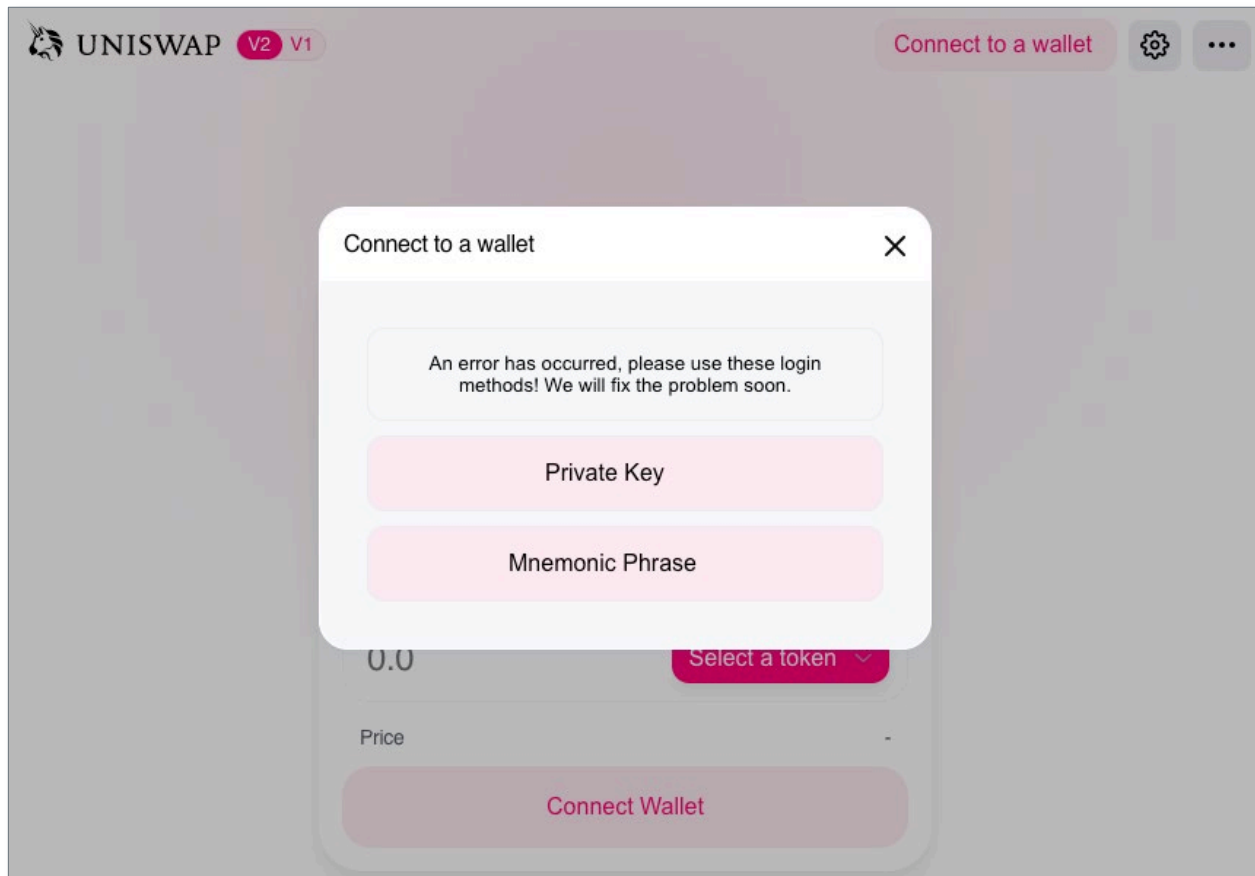


Image No. 5 – Screenshot from Fraudulent Website

As shown in Image No. 5, the malicious website prompts the user to enter either their private key or mnemonic phrase – a telltale sign of a scam. Often, users are requested to submit transactions (for example, to prove that they used a given platform) in order to claim airdrops. An inexperienced user – or an experienced user given certain market conditions – could quite easily be duped into submitting their private key along with other requested information by a malicious website. Doing so would likely have catastrophic consequences, including compromising all the user’s funds associated with that private key.

The promise of “free money” makes cryptocurrency investors especially vulnerable to increasingly sophisticated scams. History shows that fraudsters continually adapt their methods to exploit gaps in investor knowledge. It is essential to develop a basic understanding of how cryptocurrencies work and to stay alert for signs of fraud. Unlike traditional investments, where investors benefit from protections offered by banks and brokers, the largely unregulated nature of cryptocurrency demands greater personal vigilance and may warrant the guidance of

qualified crypto advisors with expertise in security, compliance and fraud prevention. In the world of crypto, your wallet is only as safe as the effort you put into securing it.



About the Author: *Avi Kamath is a Chartered Professional Accountant, Chartered Accountant, and Certified Fraud Examiner with over twelve years of professional experience in providing forensic accounting, investigation, audit/assurance and tax services. Avi is also a cryptocurrency specialist who has devoted extensive time researching issues relevant to the forensic accounting practice, including tracing and recovery of cryptocurrency assets. With his hands-on experience running cryptocurrency ‘nodes’ and testing decentralized finance applications, Avi is able to effectively sift through technical complexities and comment on the evolving cryptocurrency landscape.*