AIRDROPS:

BILLIONS OF DOLLARS OF 'FREE MONEY'

Part 1 of 3 – The Uniswap Airdrop

AVI KAMATH
JONATHAN B. ROSEN

nagel + associates
FORENSIC AND INVESTIGATIVE ACCOUNTANTS

Over the past several months, the entire crypto community has been buzzing with excitement. Since March 2020, several billion dollars' worth of cryptocurrency has been freely distributed to 'people in the know' through what is commonly referred to as **airdrops**. Where did these billions of dollars of free money come from? More importantly, how can you get your share of this free money?

Even though everyone has heard the old adage, '*If it sounds too good to be true, it probably is*', the promise of free money can compromise the judgement 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'?

To get started, what exactly 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 that have no or negligible 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. However, increasingly, even legitimate well established companies developing in this space are making use of these free distributions.

Why, you may ask, would these organizations offer free distributions of their crypto assets? There are many benefits to these crypto companies providing the airdrops, the most notable of which is market exposure. 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 such 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:

(i) Airdrops for using a company's platform or service;

(ii) Airdrops in exchange for completing simple tasks, such as sharing a referral link on one of your social media platforms (e.g., Facebook, Twitter, etc.);

(iii) Airdrops for signing up to a newsletter, by providing your email;

(iv) Airdrops for individuals who hold certain specified tokens (for example, Ether) in their various crypto wallets as of a specific date, the purpose of which is to quickly attract a tech-savvy userbase (in this example, Ether holders) to their platform or service; and

(v) Airdrops for VIP/loyalty members who contribute to a specific project or community.

With that basic understanding of airdrops, let's introduce the three airdrops that we will be profiling over this three-part article series:

(i) Part 1 (Uniswap airdrop) – Intro to airdrops and associated fraudulent schemes;
(ii) Part 2 (Yearn Finance airdrop) – Decentralized finance (DeFi) and associated risks; and
(iii) Part 3 (Reddit 'community points' airdrop) – Big Tech is airdropping! What's the catch?

In part 1 of this article series, we will be examining the Uniswap airdrop of UNI tokens (the "**UNI Airdrop**"), some common fraudulent schemes that have been associated with it, and the specific conditions that one needs to meet in order to qualify to receive it.

UNI Airdrop

The UNI Airdrop is a great place to start, as its qualification requirements were extremely simple. In order for an individual to be eligible to claim the 400 free UNI tokens offered by the UNI Airdrop, they simply had to use the decentralized crypto asset exchange platform Uniswap, prior to September 1, 2020. That's it.

So, your first question right now is probably, 'how many UNI tokens got distributed and how much were they worth?'. However, before we get into that, let's take a step back and quickly unpack what exactly Uniswap is. 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, let's address some of the key characteristics that make Uniswap unique. Unlike most exchanges, Uniswap doesn't have an '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 unintuitive part 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.

We will discuss liquidity provision and its associated risks in greater detail in part 2 of this article series. But continuing on with the UNI Airdrop, the only requirement needed to enjoy this Airdrop of 400 UNI tokens was to be a Uniswap user (liquidity provider or trader) prior to September 1, 2020[1]. Of the 150 million UNI tokens marked for the UNI Airdrop, over 126 million (84%) have been claimed to date[2]. Between September 16, 2020 (the date of the UNI Airdrop) and December 8, 2020 (the date this article was published), the value of the UNI token reached a high of $8.44 USD[3]. That means each user's UNI Airdrop of 400 UNI tokens was potentially worth in excess of $3,300 USD, which translates to over 1 billion dollars being distributed for free, from this one airdrop! Not bad for free money!

So, what's the catch? There's always a catch, right? As expected, this unannounced and valuable airdrop created quite the media buzz. While there was no time limit for claiming the UNI Airdrop, given how volatile crypto prices are, there was a 'mad rush' to claim and sell these free tokens, which had an approximate value of $1,375 USD (400 UNI Tokens X $3.44 USD) on September 17, 2020, the day after the UNI Airdrop became available to be claimed[4].

This chaotic 'mad rush' to claim the free UNI tokens offered by the UNI Airdrop didn't go unnoticed by scammers and fraudsters alike. Even in a 'simple' airdrop such as the UNI Airdrop, countless things could and often do go wrong. Let's 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.

[1] https://uniswap.org/blog/uni/
[2] https://explore.duneanalytics.com/public/dashboards/sjtVoKOXmA0sidtzg7cuatCfDz15SQsX5B6lIoeG
[3] https://www.coingecko.com/en/coins/uniswap
[4]https://www.coingecko.com/en/coins/uniswap/historical_data/usd?__cf_chl_jschl_tk__=1d936d74aeb4be17cce90bea58fcb2e0ea565128-1607452915-0-Ad5eFxfaFOWOfJYXUi9tZRhzZN5uQ-FFT0tVk_KfUoF6fUXI6FI1oT-6NR8MkcgmF_mGp6j1ohHnphN-MZoxcrYYJo0D5gBVSpT0Ik8pJwpOflyULpPkoh6hs-5Wtpaa3f1bklTe6ZV9J-czYAxbugOLxetxt46Dnkdhjyg2D7nWEbNVEBvor1OeltTBhYGfeW4fsF-X9NCJKB-BRR7MnBQLA287ImdUevEB6psRRv1xCc6h_1lqLftVs2cjUHRMaIn8O0CHFMgxxSY7HPC-M6zyQDv_WJBohBvw323S6wn1Byh3qilVItYsMDauij2mz6ZrqQeq1yoJXoxQQyzyJ4hCr1W2byX0RxwrrOMBLFG5&start_date=2020-09-13&end_date=2020-09-21#panel

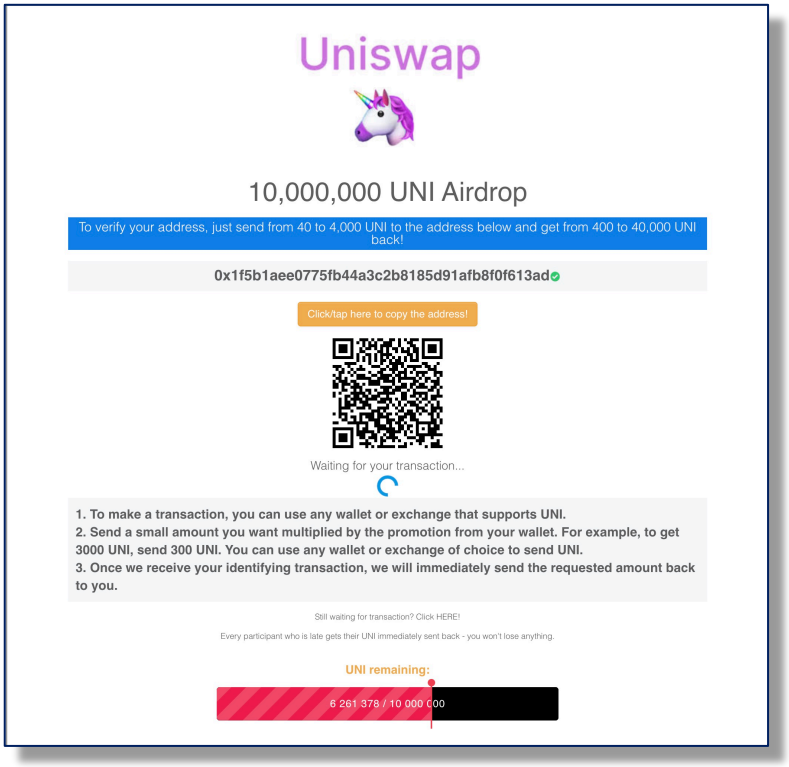


Image No. 1

Image No. 1 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 comfort to the victim.

Transactions | Comments (122)

Transactions for address: 0x1f5b1aee0775fb44a3c2b8185d91afb8f0f613ad

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
bbcfc278aa6bf5972...	7 mins ago	0x1f5b1aee0775fb	OUT	0x12be8013abEd3eAF...	1487.33 UNI
d528daf9470ff8d28...	7 mins ago	0x12be8013abEd3eAF...	IN	0x1f5b1aee0775fb	148.733 UNI

Image No. 2

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:

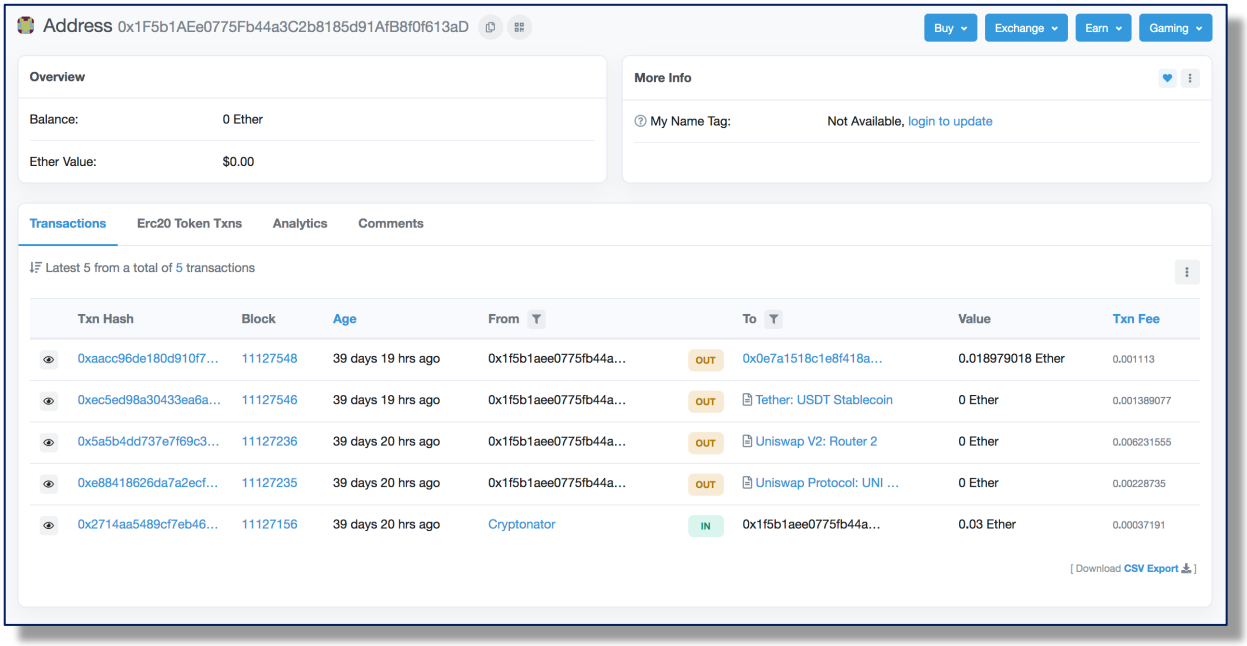


Image No. 3

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 somewhat familiar, it is because a variation of it was in the news recently, when we saw a host of celebrities (including Jeff Bezos, Bill Gates, Eric Schmidt, Steve Wozniak, Daymond John and Elon Musk) peculiarly appear to promote what turned out to be fake BTC (Bitcoin) giveaways that required users to first send some BTC in order to receive a larger amount back.

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 BTC, which, as of the writing of this article, is worth in excess of $4,000,000 USD[5]. The mechanics of this scheme are almost identical to the UNI scheme outlined above.

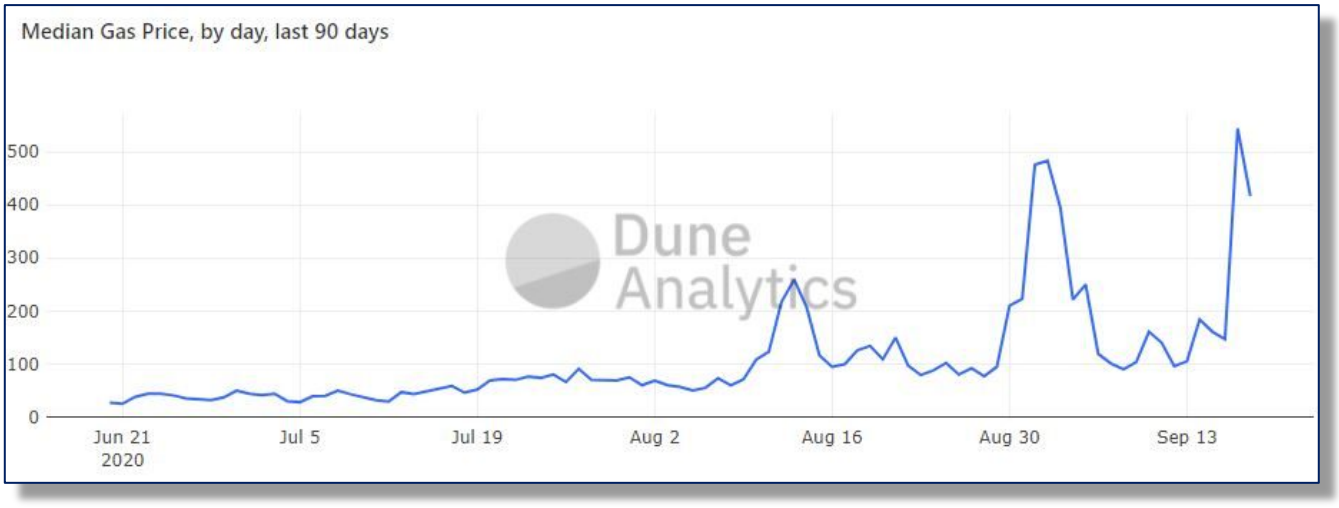
[5] https://news.bitcoin.com/elon-musk-bitcoin-giveaway-scam-millions-dollars-btc/#:~:text=A%20Youtube%20video%20of%20an,as%20much%20as%20you%20sent.&text=He%20tracked%20down%2066%20addresses,used%20by%20hackers%20and%20criminals.

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, one of which is described below.

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. As crypto users – both novices and seasoned users alike – rushed to claim and sell their UNI tokens, 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.



Source: Dune Analytics

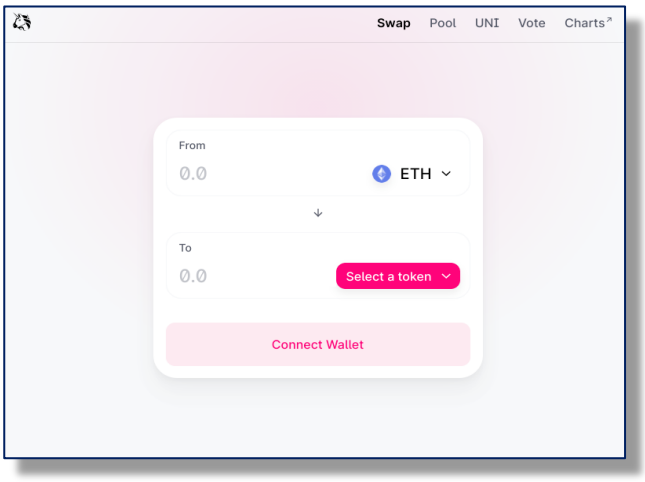
Image No. 4

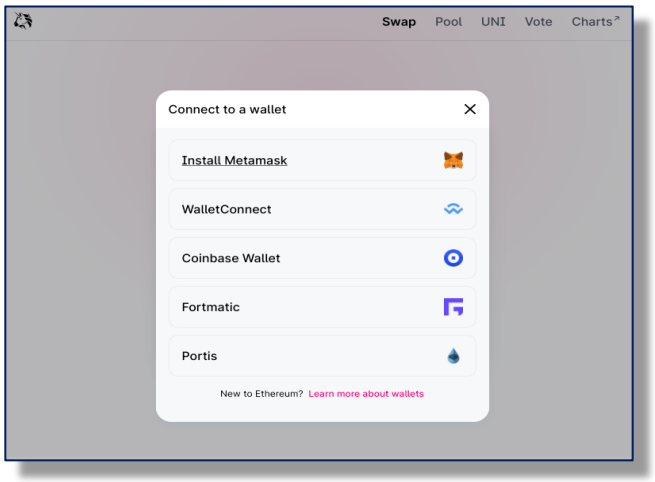
Volatile token prices and transaction fees create the perfect conditions for even hardened crypto users to make errors that could cost them far more than the free money they hoped to gain.

An extremely common malicious tactic used by criminals is to set up 'phishing' websites that request your seed or private key (*if you don't know what a seed or private key is and you are interested in learning more, click here to be directed to Nagel Academy's Introduction to Cryptocurrency course*).

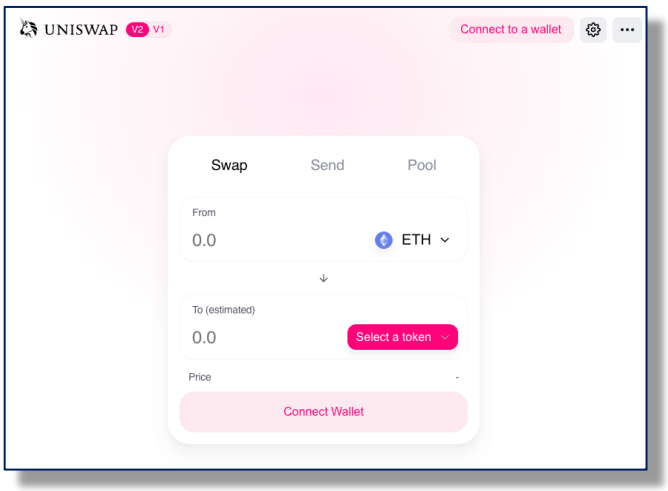
For example, take a look at the series of screenshots below. Series 1 is taken directly from the Uniswap website and Series 2 from a fraudulent site trying to pass itself off as Uniswap.

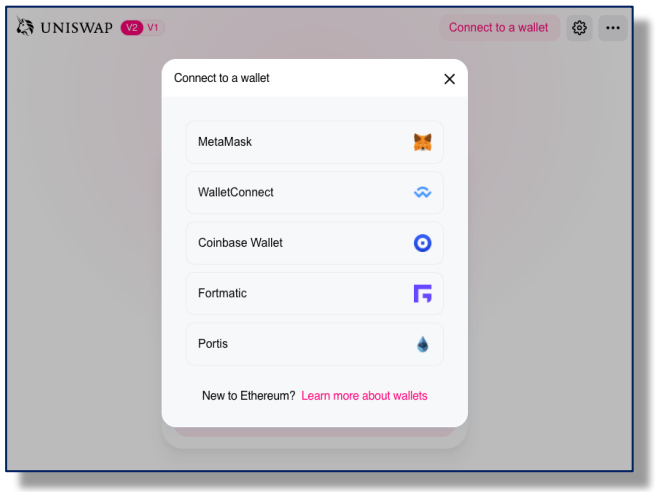
Series 1:





Series 2:





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:

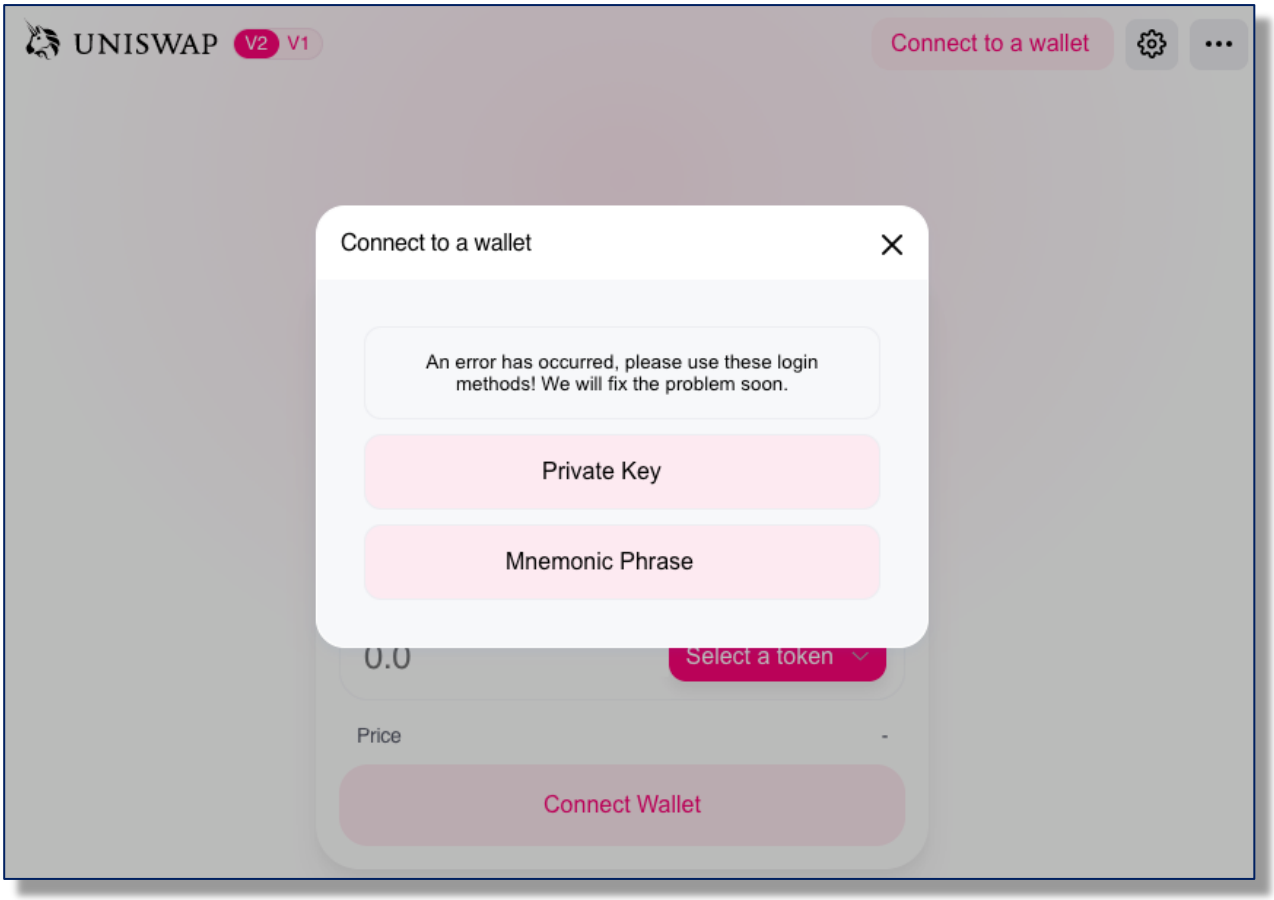


Image No. 5

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 times, 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 such as this. Doing so would likely have catastrophic consequences, including compromising all of the user's funds that are associated with that private key.

How can nagel + associates help?

The nagel team can assist in providing due diligence on any crypto related offers you may have received, in order to help you avoid ones with malicious intent. We can also provide you with a safe a reliable service that will allow you to securely claim any non-malicious airdrop you may have been awarded.

The nagel team can offer various crypto-related services, including:

a) Conducting due diligence to explain risks and help avoid malicious offers;
b) Confirming or dispelling allegations relating to investment fraud;
c) Identifying unreported crypto assets;
d) Tracing and recovery of crypto funds;
e) Providing consultation services on token implementation;
f) Providing consultation services on policy making and/or policy compliance;
g) Reviewing security, privacy, and asset safeguarding protocols and methodologies;
h) Assisting in locking/unlocking assets into liquidity pools;
i) Assisting in staking/unstaking liquidity provision tokens (yield farming); and
j) Assisting in securely claiming all entitled airdrops.

While nobody can be sure what the future holds for crypto, past experience and current trends would appear to suggest that this is only the beginning…

Stay tuned for part 2 of 3 of this article series, where we will address the Yearn Finance Airdrop, decentralized finance (DeFi) and associated risks.

About Our Firm

nagel + associates is a Toronto-based boutique forensic accounting firm that focuses exclusively on Forensic Accounting, Investigations and Disputes, Anti-Fraud Training, Anti-Fraud Consulting and Crypto Advisory. For more information about our services, please visit nagel-forensics.com.