



**VivekRamachandran.eth** @vivekramac Sat Mar 26 11:47:12 +0000 2022

After changing my profile to read "Web3 Junkie" and "Top 200 ENS Holder", and tweeting routinely about web3, NFT and crypto, I have become a target of NFT phishing/scam attacks ■

Anatomy of a scam I was sent (read on)



Step 1: Typically begins with a Twitter account with a high number of followers or a verified account + profile which claims to be co-founder of an NFT project e.g. Bored Apes, Mutant Apes etc.

These might be hacked/purchased/fake followers built up. <https://t.co/zdSYMJKyfy>





The image shows a Twitter profile card for a user named 'crystal.eth'. The profile picture is a simple grey silhouette of a person's head and shoulders. To the right of the profile picture are three icons: a three-dot menu, an envelope icon for direct messages, and a black 'Follow' button. Below the profile picture, the name 'crystal.eth' is displayed in bold black text with a blue verification checkmark, followed by the handle '@crystalhaynes'. The bio reads 'Angel Investor & Co-Founder at @BoredApeYC @YugaLabs | #BAYC #MAYC #BAKC' with a 'Translate bio' link below it. The location is 'Boston, MA', the website is 'apecoin.events', and the join date is 'Joined June 2009'. The follower statistics show '2,437 Following' and '5,380 Followers'. At the bottom, it says 'Not followed by anyone you're following'.

Step 2: These then post an opportunity to still be able to mint a Bored Ape or some other valuable NFT.

The sheer number of Retweets and Likes shows how flawed and fake social validation as a "security test" can be!  
<https://t.co/ZvZ8FgP5yc>

Pinned Tweet

**crystal.eth**   
@crystalhaynes

Launch of Ape Coin has been a big success! We have collectively decided to airdrop some more to active NFT Traders/Holders! If you don't currently own NFTs, you can claim with a 0.33 ETH fee!

For more details visit:


 [apecoin.events](https://apecoin.events)

[\\$APE](#)  
[#ApeCoin](#)  
[#BAYC](#) [#MAYC](#)



9:51 AM · Mar 26, 2022 · Twitter Web App

697 Retweets 53 Quote Tweets 28.4K Likes

     Tip

 **Who can reply?**  
People @crystalhaynes mentioned can reply

Step 3: These accounts or ones in their control TAG users who are active crypto/NFT enthusiasts - probably based on twitter profile or their tweets.

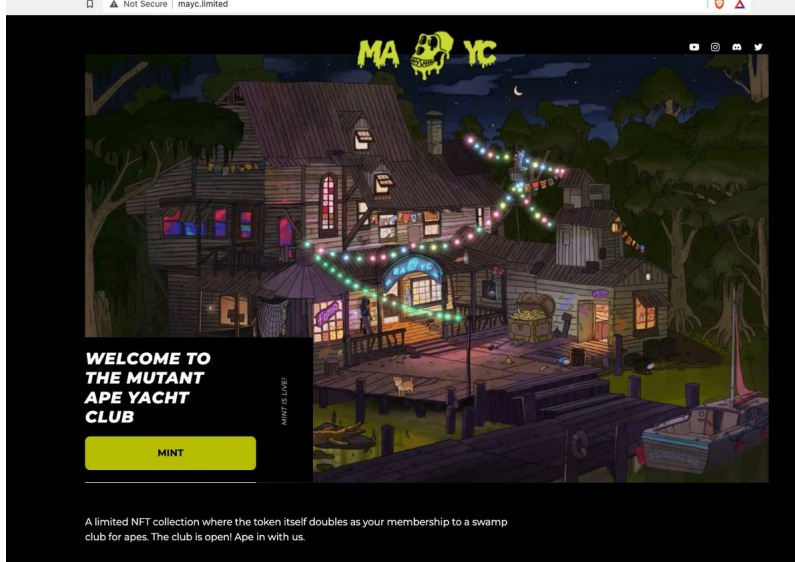
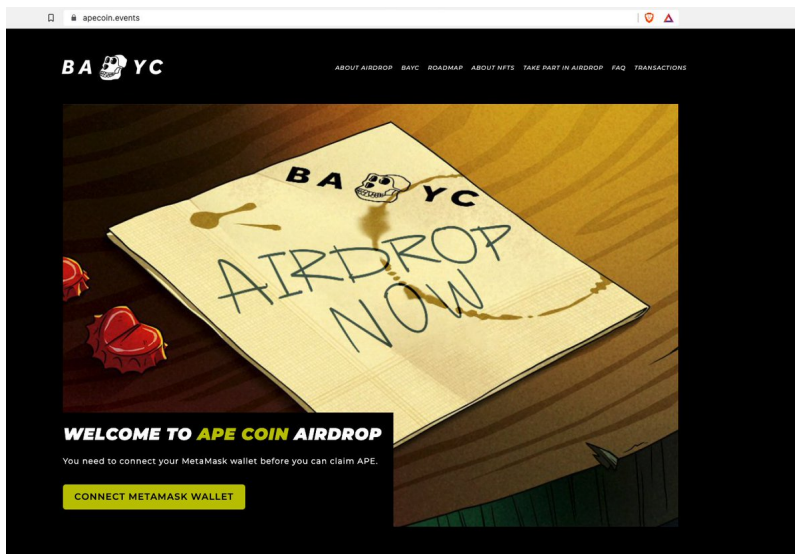
Here is my "good friend" Toni trying to help me get rich quick :) The account was created today. <https://t.co/IF0nwRa7ZI>

**Toni Fortner** @ToniFortner2 · 6h  
Replying to @NFT0007club  
I love it @YW\_jo6k @AnubisGemsx100 @Bestrauss604 @harianlepas\_ @fred\_advimob @arryy12345 @Nuxes1212 @boltasdpoitw @huonglan2021 @GotNXT @awinisawin1 @eddyisboring @vivekramac @youbie7 @thaasty

**Toni Fortner**  
 @ToniFortner2  
 Joined March 2022  
 0 Following 0 Followers  
 Not followed by anyone you're following

Step 4: Once a gullible user lands on the website - they try to make it as legitimate as possible!

<https://t.co/6Q6uchWQMG>



If you have Metamask installed -- the scam site almost immediately triggers a connection.

I will play along and connect a test account.

[PLEASE DO NOT FOLLOW THESE STEPS IF YOU DO NOT KNOW WHAT YOU ARE DOING]

<https://t.co/PbqKj7QDvW>





http://mayc.limited

## Connect With MetaMask

Select the account(s) to use on this site

Select all ⓘ

[New Account](#)

-  Account 1 (0x0f0...  
[Redacted])
-  Test Accou...  
0 ETH [Redacted]

Only connect with sites you trust. [Learn more](#)

Cancel

Next


< Back



http://mayc.limited

## Connect to Account 1 (0x0...)

Allow this site to:

-  See address, account balance, activity and suggest transactions to approve

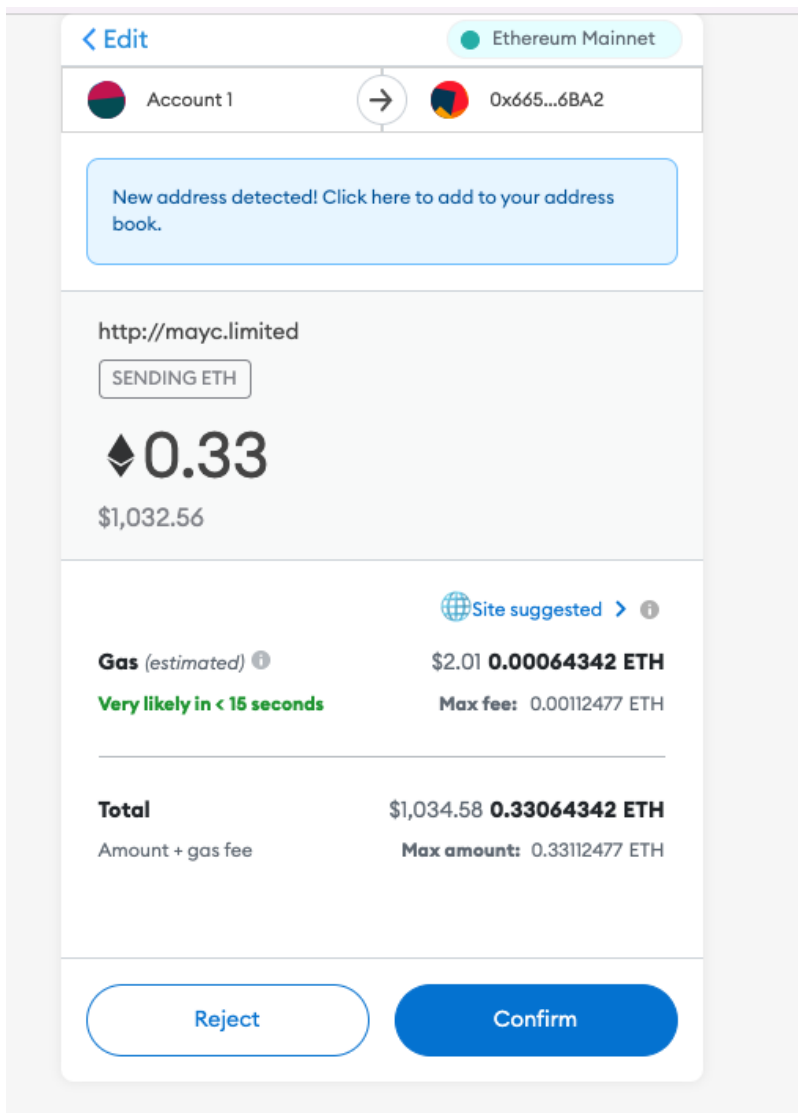
Only connect with sites you trust. [Learn more](#)

Cancel

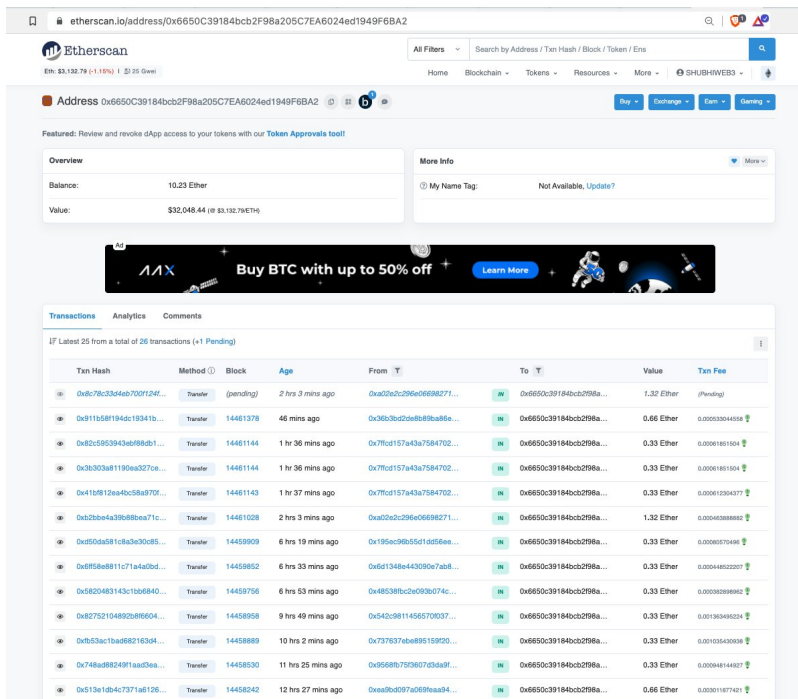
Connect

After the account is connected - it tries to trigger a ETH transaction to send crypto to the scammer's address .

You are not minting anything - just sending money to the scammer if you continue. <https://t.co/aU8LqN3PYS>



Copying the Scammer's address from the top right of the screenshot above, we can see that they have already made over USD 32K (10.23 ETH) as of this writing: <https://t.co/a36tKPAvfq> <https://t.co/rwO1uL1uGx>



If you look closely at the scammer's account - you will see that there are only "IN" transactions i.e. money sent to it and nothing was withdrawn.

This is typical - the scammer might keep this account active for some time and then withdraw to other mule accounts /

use mixers

Unlike having to give KYC when opening a bank account, you don't even have to write anything to the blockchain to create a wallet!

Here is a simple python script to create wallet addresses for the curious - it's that easy! It's entirely offline!  
<https://t.co/CO1mNovpMe>

```
>>> import secrets
>>>
>>> wallet_private_key = "0x" + secrets.token_hex(32)
>>>
>>> wallet_private_key
'0x9df77bb9cc6b1aea2db0f7b6c65c75081de5bb8e1c8b931f9d3c385b9ee74998'
>>>
>>> from eth_account import Account
>>>
>>> wallet_account = Account.from_key(wallet_private_key)
>>>
>>> wallet_account.address
'0x17C6Aa99a749858aD9C461f1769BC9C7E5dcCEA6'
>>>
>>> █
```

Moral of the story -- Web3, Crypto transactions etc. are in their nascency and security awareness has a long way to go.

Web2 phishing and social engineering attacks work just as well on Web3, if not better! So be cautious and vigilant!

Thank you - have a great weekend! ■