NFT Security Concerns

CSC301-01

Michael Burns, Brett Domenick, Adib Ahasan

What is an NFT?

- NFT stands for Non-fungible token.
  - Fungible (in terms of an asset) means that it is able to be replaced or swapped with another identical item, or interchangeable.
  - Non-fungible means that an asset cannot be replaced or interchanged with another item.
  - This is a crucial aspect of NFTs.

What is an NFT? (Cont.)

- An NFT is a digital asset that represents real-world objects.
- This can be virtually anything imaginable, but the most popular NFTs being sold are art, music, video game items and collectible items.
- Anyone can create an NFT and sell it for whichever price they would like.

Importance of NFTs

- Since all NFTs are virtual (most being art), critics would say that you can just save the image and claim it as yours. You can post it wherever you want to, and no one would really know you don't have the ownership to that item.
- The importance of NFTs are that they are expanding on the security measures that cryptocurrency has in place, instead of creating "virtual money" there can now be "virtual items".
- Owning an NFT means the owner is able to do with that item whatever they want (sell it again or hold on to it), and can be proved its their item because it is securely stored on a blockchain, like cryptocurrency.

Purchasing an NFT

- There are numerous marketplaces where users can buy and sell their NFTs.
- The most popular marketplace is called OpenSea, and NFTs can be purchased using cryptocurrency.
- After the NFT is purchased, it is stored on a secure ledger called the blockchain.

Blockchain

- A blockchain is a decentralized, distributed ledger that records the provenance of a digital asset.
- A blockchain uses cryptography to encrypt, protect and make data stored on in the ledger immutable to changes or modifications.
- Every piece of data (or a block) gets created, and encrypted.
- The individual blocks are then attached to each other, and added to the “chain”.

Decentralized Ledger

- A decentralized ledger is used in blockchains and distributed to every node on the network.
- This includes all transactions made on the blockchain (purchases, withdraws, transfers made between accounts).
- Everything is logged on the blockchain, and the ledger is updated every time a new purchase, withdraw or transfer is made.

Decentralized Ledger Benefits

- A decentralized ledger, such as the blockchain, makes it nearly impossible for someone to create a fraudulent transaction.
- Every block is encrypted with a hash, and the hash for every block is reliant upon the block previous to it.
- If one change is made to the data stored in a block, it will not only change the hash of that block, but every block after that.
- The hacker would have to change the data in the block and rehash every block after that on every node that has a copy of the ledger, which is nearly impossible.

Private vs Public Blockchains

- **Public Blockchain**: network where anyone can join, contribute and see any part of the ledge they want to.
  - Ex: Ethereum (cryptocurrency) is a very large public blockchain.
- **Private Blockchain**: a blockchain where only a single organization over the network.

Benefits of Public Blockchain

- •**High security**: blockchains offer many security protocols to ensure the protection of assets stored on the blockchain. Companies and organizations deal with online attacks everyday, totaling billions of dollars of lost year after year.
- •**Open environment**: everyone has a copy of the ledger. If a hacker tried to change a piece of data on the ledger, they would have to hack every computer with the ledger and change it.

What are Blockchains being used for?

- **Cryptocurrency**: runs off blockchain technology, there are more than 10,000 cryptocurrencies now, with the largest being Bitcoin and Ethereum.
- However, many companies have started implementing blockchains for uses outside of cryptocurrency.
- **Healthcare**: providers can use private blockchain solutions to securely store their patient's medical records. When new documents are added to the blockchain, they are encrypted and can be accessed only by certain individuals using a secure private key.

What are Blockchains being used for? (Cont.)

- **Smart Contracts:** (computer code that can be built into the blockchain to verify a contract agreement) can be stored directly onto a blockchain where the a copy can be distributed to both parties, as well as a lawyer/attorney for legal purposes.
- **Supply Chain:** especially within the food industry, companies are increasing the use of blockchain to track the path and safety of food from the farm to the grocery store.
- **Voting:** using blockchain when it comes to voting would make it nearly impossible to tamper with any votes.

Large Companies using Blockchains

- Walmart
- Pfizer
- AIG
- Siemen
- Amazon
- Microsoft
- Nvidia
- 81 of the top 100 companies are using blockchain technology.

Largest Public Blockchains

- When an NFT is purchased, it is stored on a public blockchain.
- The Ethereum blockchain is the most popular for storing NFTs.
- One issue with the Ethereum blockchain is that to store NFTs on it, a user must pay a gas fee (the fee to store an NFT on the blockchain) has become very expensive.
- Due to this, other blockchains such as Binance Smart Chain and Cardano have gained popularity.
- One thing Ethereum, Cardano and Binance have in common is that they are all cryptocurrencies.

Cryptography used for Blockchain

- Blockchains use 2 types of cryptography: asymmetric (2-key) cryptography and hash algorithm.
- Asymmetric cryptography uses a key to encrypt the data, and a separate key to decrypt the data.
- Hash algorithms do not use a key, the data that is hashes is not meant to be decrypted.
- The only way to decrypt hashed data it to know the original data before it was hashed.

Cryptography Example

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Security Risks of NFTs

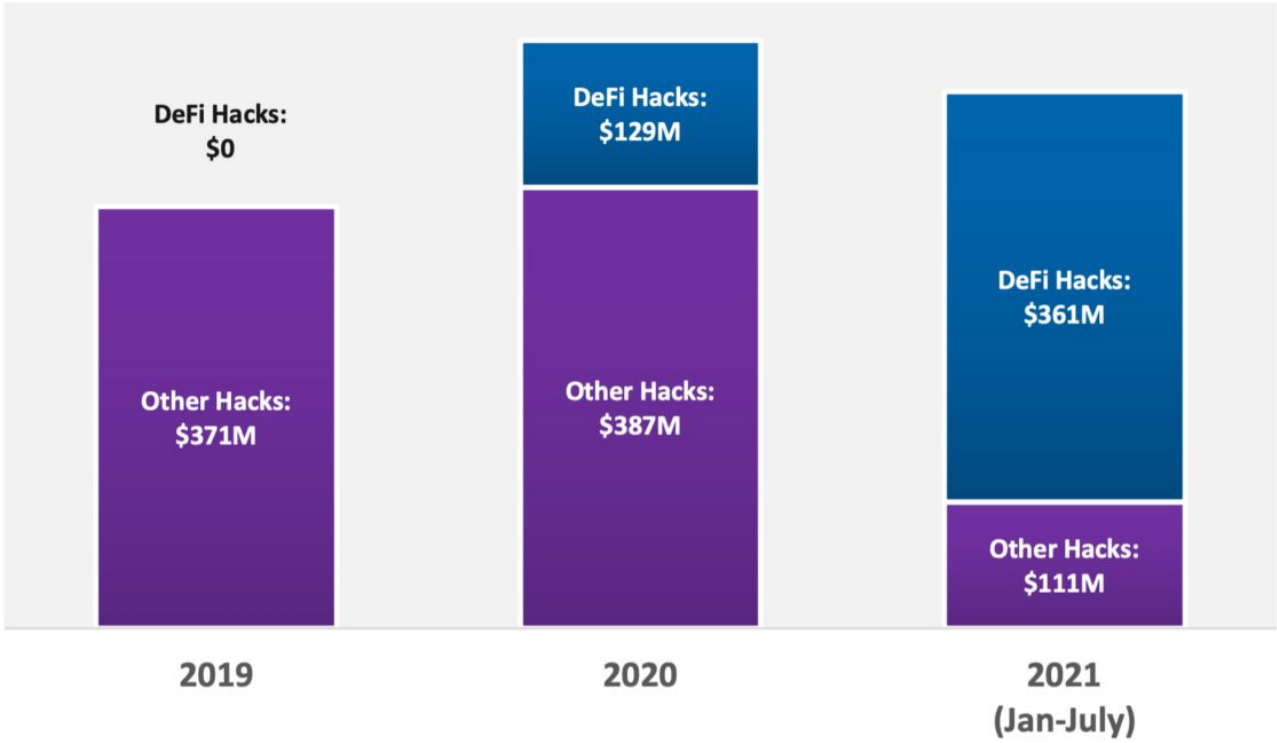
Social Engineering and Phishing

- A Decentralized platform means nobody is there to rescue users when things go wrong
- Attackers can use social engineering to gain access to accounts
- What's gone is gone on the blockchain
- NFT and crypto accounts are just as susceptible to data leaks and are now a prime target
- Stolen NFT from Phishing attack

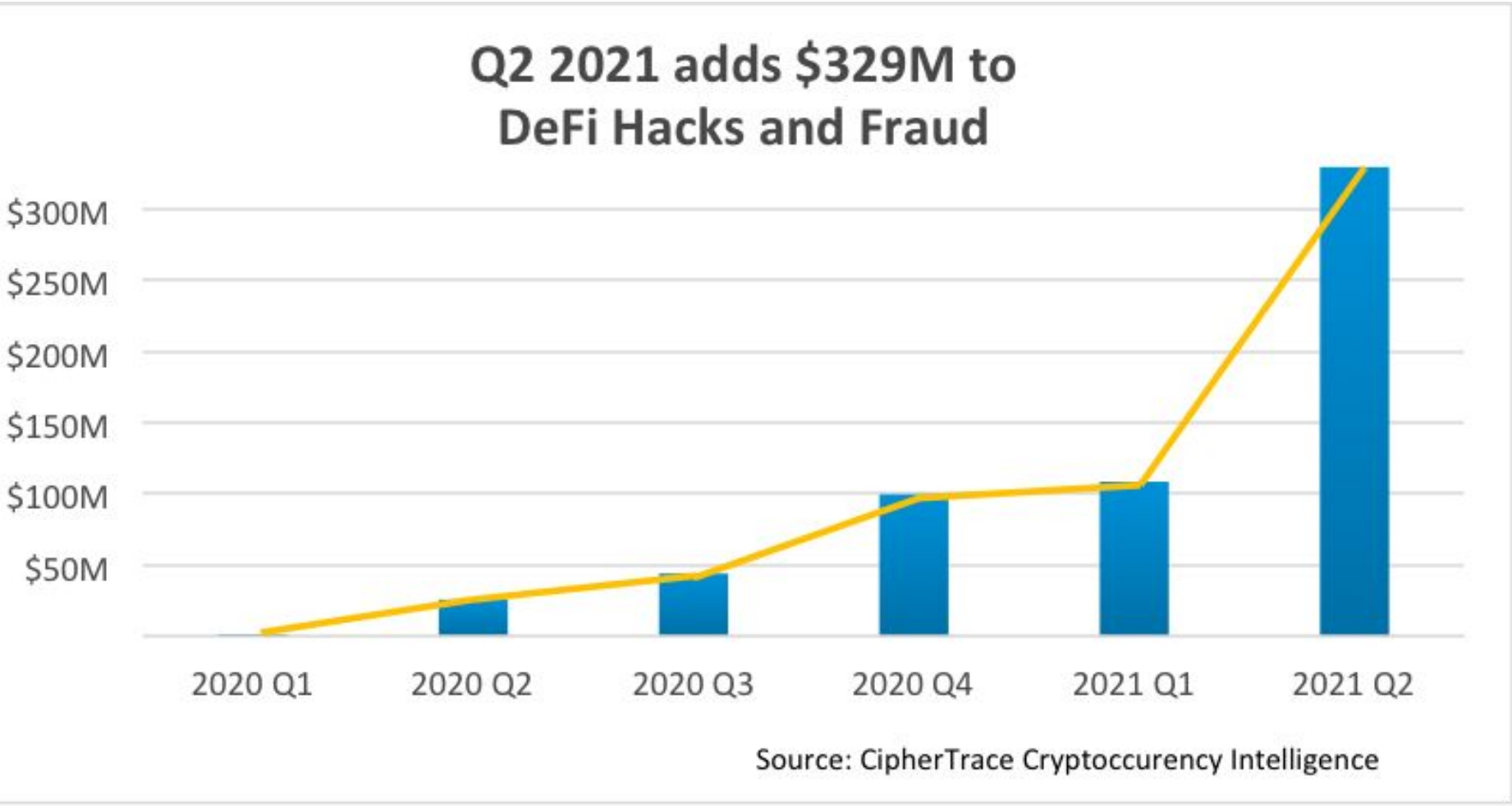
Hacks

- Crypto and NFTs are susceptible to network hacks where users can lose everything
- https://www.forbes.com/sites/emilsayegh/2022/04/11/reflecting-on-the-biggest-crypto-hack-ever/?sh=6e7333ce753c
- Blockchain will always need traditional “web 2” endpoints which could always have vulnerabilities
- 51 percent attack
  - When someone owns more that 50 percent of the computing power on a chain they can control the chain

DeFi related hacks already make up 76% of major hacks in 2021



Source: CipherTrace Cryptocurrency Intelligence


Q2 2021 adds $329M to DeFi Hacks and Fraud
$300M
$250M
$200M
$150M
$100M
$50M
2020 Q1
2020 Q2
2020 Q3
2020 Q4
2021 Q1
2021 Q2
Source: CipherTrace Cryptoccurency Intelligence

Scams

- Decentralization makes NFTs and crypto prime targets form scammers
- Transactions are harder to track and there are less safe guards to prevent fraudulent or nefarious transactions
- Scams are easier to pull of as users often are not as knowledgeable about the platform
- https://web3isgoinggreat.com/?tech=nft

NFT SCAMS

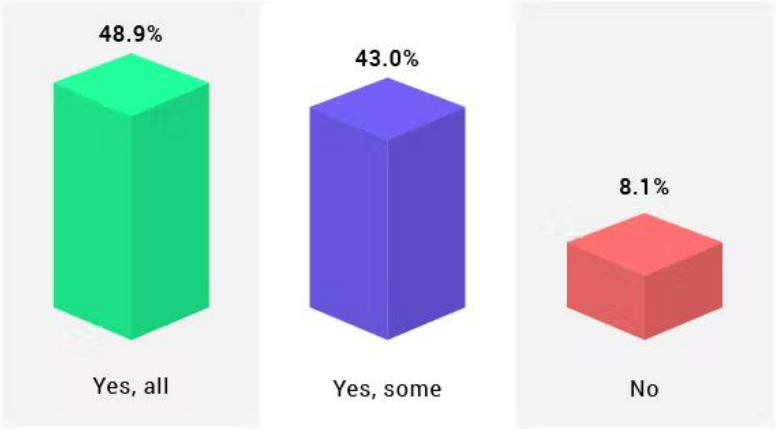
Two out of 3 respondents had **paper hands and panic-sold** NFTs in the past.

Only 1 in 10 NFT owners had never **experienced a scam**.

Half of respondents said that they had **lost access** to their NFTs before.

Most Commonly Experienced NFT Scams

Did you recover the NFTs you had lost?



Source: Survey of 1,008 NFT owners

PrivacyHQ

Rug Pulls

- Term coined to describe when crypto project creators abandon their projects to run away with the funds or sell off their “pre-mined” holdings
- Becoming increasingly common in crypto and NFT
  - Anyone can create an NFT project
  - No governance over creation of projects
- Similar to the investing term “pump and dump”

Other NFT scams

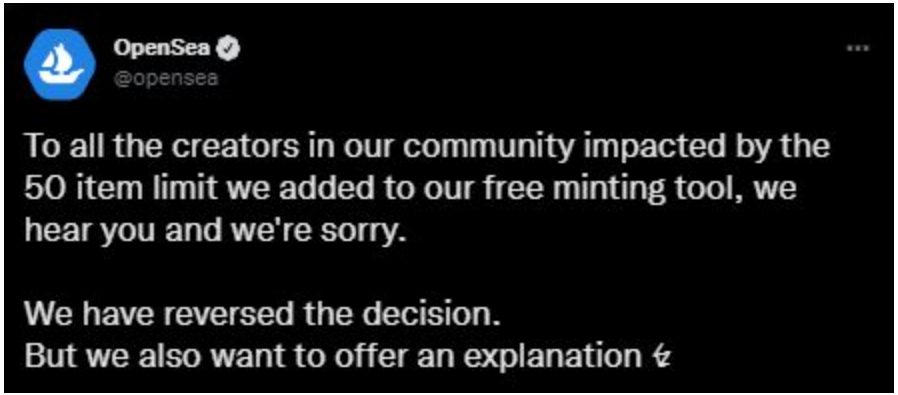
- Wash Trading
  - Trading with yourself to falsely increase value
- Sleepminting
  - Minting an NFT to a notable wallet and transferring it back to the real creators wallet. Makes faxes seem genuine
- Tokenomics Loophole
  - Distributing non randomized NFTs under the idea that they are randomized. (Mekaverse)
- Fake Minting Websites
  - New NFT releases are targeted by fake minting websites that look like real ones to deceive buyers

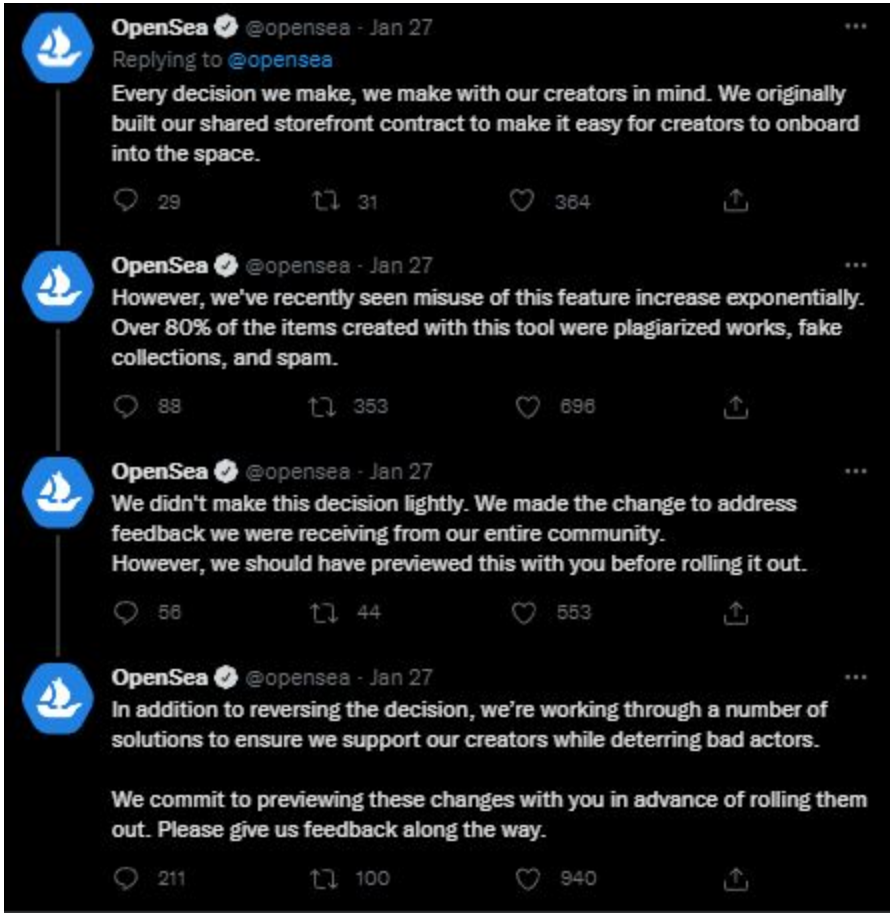
Not as popular as they seem

- About 360,000 total individuals own all the NFTs
  - 0.1% of 300 million total crypto owners
- 80% of the total value associated with NFTs is owned by only 9% of the community
  - About 2.7mill NFTs owned by only 32,400 users
  - Possibly lower as users are counted by unique wallets
- Many high value NFT’s are believed to be traded to multiple wallets owned by the same person or group

Ownership

- Owning an NFT does not necessarily mean ownership of the item
- Blockchain only stores a hash or url, Image is stored:
  - Http server
  - IPFS(decentralized storage)
    - Node is run by company that sells NFT
- NFTs are still subject to copyright
  - NFT ownership does not give copyrights
  - Can be sued for creating NFTs of stolen work


OpenSea
@opensea
To all the creators in our community impacted by the 50 item limit we added to our free minting tool, we hear you and we're sorry.
We have reversed the decision.
But we also want to offer an explanation ↯


OpenSea @opensea · Jan 27
Replying to @opensea
Every decision we make, we make with our creators in mind. We originally built our shared storefront contract to make it easy for creators to onboard into the space.
29 31 364
OpenSea @opensea · Jan 27
However, we've recently seen misuse of this feature increase exponentially. Over 80% of the items created with this tool were plagiarized works, fake collections, and spam.
88 353 696
OpenSea @opensea · Jan 27
We didn't make this decision lightly. We made the change to address feedback we were receiving from our entire community.
However, we should have previewed this with you before rolling it out.
56 44 553
OpenSea @opensea · Jan 27
In addition to reversing the decision, we're working through a number of solutions to ensure we support our creators while deterring bad actors.
We commit to previewing these changes with you in advance of rolling them out. Please give us feedback along the way.
211 100 940

Environmental Impact

- Most NFTs are traded on the Ethereum blockchain
  - Ethereum uses “proof of work” to validate transactions
- Estimated that every transaction has a carbon footprint of about 30kg CO_2 - 50kg CO_2
  - 14x the footprint of mailing a physical piece of art across the US.
  - 74,000 visa transactions
- Average usage of the bitcoin network evens out to about 2000kwh per transaction(new york times)
  - Enough to power the average us household for 73 days

Risk Management & Security

(What to do when someone screenshots your NFT)

Before you buy…
For the first time NFT buyer.

- Does the project have real followers on Social Media?
  - If they have a lot of followers, are people engaging with them?
    - It is **easy to fake** a popular and active social media account.
- Find out more about the NFT seller, artist, vendor, and marketplace.
  - What do similar NFTs go for?
  - Check their reputation (history).
  - Verify their identity/branding.
  - Engage in a dialogue to understand their vision/mission.

Twitter

Man who paid $2.9m for NFT of Jack Dorsey's first tweet set to lose almost $2.9m

Crypto entrepreneur Sina Estavi made headlines in March 2021 when he paid $2.9m for an NFT of Twitter boss Jack Dorsey's first tweet. But his efforts to resell it have run aground, with a top bid of just $6,800 as of Thursday.

The initial purchase was at the time among the most expensive sales of a non-fungible token, or NFT, and came amid a flurry of interest in the niche crypto assets.

Estavi put the tweet up for resale on the popular NFT marketplace OpenSea last week, initially asking for $48m.

That price tag was removed after offers in the first week were in the low hundreds of dollars. As of Thursday, the highest bid was 2.2 of the cryptocurrency ether - equivalent to about $6,800.

Congratulations! You are now a proud owner of an NFT!

Well… Now what?

Follow Basic Security Principles

- Use strong security measures
  - Strong passwords
  - Change passwords frequently
- 2-Factor Authentication
  - Enabled and secured backups
- Prevent unauthorized access to your data
- Do not click on Untrusted links
- Avoid connecting to Untrusted networks (Public Wifi)
  - Use a VPN to help enhance security

Safeguarding your NFTs

- Stay up to date with the latest news for where you store your NFTs (e.g. OpenSea)
  - This will alert you to any new security issues, or new security features.
- Be informed of who you are dealing with
  - Users - Can compromise your security in many ways (phishing, social engineering, etc)
  - Marketplaces - Only use trusted and verified vendors or user
- Be informed of what you are dealing with
  - What NFT you have, where it is stored, your proof of purchase, etc.

Safeguarding your NFTs

- Use a Hardware Wallet - Give you better control over your security
- Ignore unsolicited messages, especially unknown messengers.
- Double check URLS, Usernames, and addresses.

Q&A

Works Cited

- https://www.merriam-webster.com/dictionary/non-fungible%20token
- https://www.forbes.com/advisor/investing/nft-non-fungible-token/
- https://www.forbes.com/advisor/investing/what-is-blockchain/

Works Cited (contd.)

https://privacyhq.com/news/nft-and-wallet-security/

https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/

https://phemex.com/academy/what-is-a-rug-pull

https://www.csoonline.com/article/3655745/10-security-concerns-cisos-should-have-about-nfts-and-cryptocurrency.html#:~:text=%2010%20NFT%20and%20cryptocurrency%20security%20risks%20that,While%20NFTs%20are%20based%20on%20blockchain...%20More%20

https://www.independent.co.uk/tech/nft-ownership-metaverse-crypto-bitcoin-b1986530.html

https://www.cbr.com/fewer-nft-owners-than-you-think/

https://www.linkedin.com/pulse/crypto-101-nft-scams-ezreal-kung/

https://earth.org/nfts-environmental-impact/

Works Cited (contd.)

- https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft
- https://coinmarketcap.com/alexandria/article/how-to-protect-your-nfts
- https://medium.datadriveninvestor.com/how-to-protect-your-nfts-and-avoid-getting-scammed-7a5733410188
- https://www.theguardian.com/technology/2022/apr/14/twitter-nft-jack-dorsey-sina-estavi
- https://bitcoinmagazine.com/business/we-tested-new-trezor-cryptocurrency-wallet-what-we-found
- https://bitcoinmagazine.com/culture/bitcoin-hardware-wallet-keepkey-launches-begins-shipping