Web3 Security 101

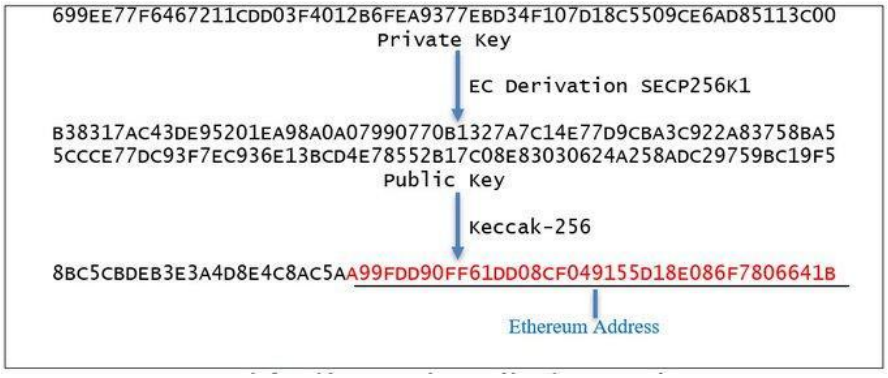
Keeping your NFTs and Crypto assets safe can seem impossible. Let's change that. This is a guide to give you a strong foundation to use on your Web 3 journey.

Basic Terms & Concepts

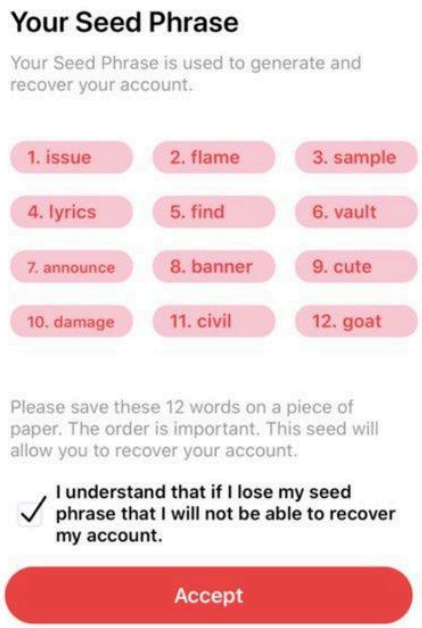
ADDRESS - a string of characters that represents a wallet that can send and receive cryptocurrency It's like a real-life address or email. Each address is unique and marks the location of a wallet on the blockchain.

PUBLIC KEY - a string of characters that allows you to receive cryptocurrency transactions It's paired with a private key. Anyone can send transactions to your public key. You need the private key to unlock them. Your ADDRESS is a shortened form of your public key.

PRIVATE KEY - gives you the ability to prove ownership and unlock assets linked to your public address While your Public Key encrypts the transaction. Your Private Key decrypts the transaction. Ethereum Private Keys are 64 random hex characters or 32 random bytes.



SEED PHRASE - a series of words that links to your private key Your seed phrase is like your bank account number, your social security number, date of birth, home address, and ATM pin—all in one. If someone gets it, they can take all your Crypto assets. May look like this:



HOT WALLET - or software wallet A form of digital storage for your private keys that you can access on your computer or mobile and is connected to the internet. Because of the internet connection, hot wallets are not as secure from hackers as their counterparts—cold wallets.

COLD WALLET - or hardware wallet A physical device that stores your private keys offline. Cryptocurrencies are never stored within the hardware wallet itself. They always live on the blockchain. The hardware wallet stores your private key. There is no back up to this form of storage. If you misplace your cold wallet, you lose access to your investments. Cold wallets can cost between $60 and $200 and look like a USB drive.

Choosing Your Wallets

You should utilize both a hot (online) wallet and cold (offline) wallet.

For ETHEREUM transactions: Use Metamask for the online transaction. Then store the key offline with Ledger. How to use Metamask with Ledger. Walkthrough on how to use Metamask with Ledger.

For SOLANA transactions: Use Phantom for the online transaction. Then store the key offline with Ledger. How to use Phantom with Ledger. Walkthrough on how to use Phantom with Ledger.

The DO's

- DO start with small transactions and only increase the size when you get the hang of it.
- DO your own research before any transaction.
- DO segregate your accounts by use - long term storage of coins, free airdrops, minting NFTs etc.
- DO store your seed phrase offline on paper, or on a secure steel plate or capsule (more on this below).
- DO use the mobile app versions of your wallet/s. Mobiles are more secure environments than laptops.

The DON'Ts

- DON'T send assets to a wallet that does not support your crypto. You will lose it.
    - For example: DON'T send Solana assets to a Coinbase wallet.
- DON'T keep the keys to your valuable assets in a hot (online) wallet, instead transfer them to a cold (offline) wallet
- DON'T back up your seed phrase on your Google drive or iCloud. It's hackable. Store your seed phrase OFFLINE.
- DON'T take a picture of your seed phrase.
- DON'T click on links sent to you via DMs or email. Ever!

Protecting Your Seed Phrase

Protecting Your Seed Phrase **NEVER SHARE YOUR SEED PHRASE WITH ANYONE**! That gives them full control of your assets. Store your SEED PHRASE offline on paper, or preferably in a Cryptosteel Capsule.

A scammer's main goal is to steal your seed phrase or the private key to your crypto wallet. With it they can log into your wallet from their own device and move all your funds and NFTs to their own wallet. Once that happens, there is absolutely no way to get it back.

It’s vital that you keep your seed phrase safe and not share it with anyone, or on any site. You will NEVER, EVER need your seed phrase or private key for any transaction. If any site or person asks you for either, leave immediately! More on protecting your seed phrase HERE.

Avoiding NFT Scams

Do your due diligence before buying into a collection. During NFT minting make sure you are connected to the correct website. Scammers frequently clone websites by making a slight change to the original domain name.

Double check the name of the project. Always look for the verified badge. Check the number of items, the volume, and the floor price. Use reverse image search on Google or Fingible for counterfeit detection. More information on avoiding NFT scams can be found HERE.

Phishing Attacks

One of the most common ways scammers can target NFT collectors is via phishing attacks. They may lure you with fake airdrops to trick you into claiming or interacting with tokens.

When you proceed with the claim, you interact with a malicious smart contract that secretly seeks permission to take your assets. If you inadvertently grant permission to the contract, it can drain the assets in your wallet. Don't trust—verify everything!

Scams on Discord

Discord is important for info and community, but it can also be risky. Look out for: Servers with FAKE NFT projects. DMs with links. ANYONE who says they need your seed phrase. Free Discord Nitro subscriptions. More information on avoiding Discord scams can be found HERE.

The Blind Signing Problem

When you sign a smart contract without key contract details being fully extracted and displayed that is blind signing. This is a vulnerability that can be exploited. More details HERE.

OpenSea Hack Lessons

Revoking permissions. Avoiding blind signatures. Not mixing web3 and emails. More details about the OpenSea hack can be found HERE.

The New Web3 Mindset

Best practices and options for securing crypto including practical approaches ranging from passwords to crypto wallets and more. THIS is a good podcast to listen to about crypto security and having a Web3 mindset.

In the Head of the Scammer

I highly recommend watching THIS video from Ledger that will help you get in the head of a scammer. In watching this you will learn more about:

- Why to never give out your recovery phrase
- What scammers look for
- The main traps
- Phishing device scams
- Bad link scams
- SIM swaps
- And more

Knowing how to secure your assets is key to thriving in Web3. Take it from me, 2 years ago I had my Metamask completely drained in seconds because I screenshotted the recovery phrase on my phone, and it was backed up to my OneDrive account that got compromised. Don’t take any of this lightly, hacks happen daily, stay protected!