

How to Secure Your Crypto and NFTs: Hot and Cold Wallet

This guide is for people who already have a Web3 wallet and want to secure their purchased NFTs or crypto after hearing a lot about people losing all their assets to scammers.

Setup two wallets, a Hot Wallet and a Cold Wallet, to secure your crypto and NFTs.

“Assume every message you get is a scam,
even if it is from someone you know”

@snarls4651 (Had STOLEN Sept 20, 2022,
\$300,000 worth of NFTs: BAYC #4651 BAKC
#4259 KODA #345 & #2185 MEEBIT #1034)

- @Snarls4651



<https://twitter.com/Snarls4651/status/1612131786259333120>

How to Use a Hot and Cold Wallet

| | Hot Wallet | Cold Wallet |
|-------------------------------------|--|---|
| Primary Use | For minting or buying NFTs only. Keep very little \$ in it. | For storage only. Never for minting or connecting to a website. Transact with your hot wallet only, nothing else. |
| Mindset | If I lose everything here, I will be fine. | If I lose everything here, I will be ruined. |
| Wallet Type | Software Wallet (Metamask, Phantom, TrustWallet, Coinbase Wallet, etc.) | Hardware Wallet (Ledger, Trezor, etc.) |
| Value of Items Stored in the Wallet | Small \$ amount | High \$ amount |
| Seed Phrase Weakness | Seed Phrase touched the Internet or touched your computer | Seed Phrase never touched the Internet |
| Seed Phrase Input Method | Electronically (manually typed or copy-paste) | Rarely used as you manually input a PIN physically on your hardware wallet. |

Bonus Level Wallet Security

Add a third wallet, a Warm Wallet. A warm wallet lets you use your hot wallet as if it owned the assets in your cold wallet.

Check out delegate.cash, warm.xyz, tokenproof.xyz, and other similar services.

Hot Wallet Vs. Cold Wallet

What makes a wallet hot or cold is NOT the hardware.

It is related to signing transactions or connecting to websites.

| | Hot Wallet | Cold Wallet |
|------------------------------------|------------|-------------|
| Signed a transaction previously? | YES | NEVER |
| Connected to a Website previously? | YES | NEVER |

Even if you have a hardware wallet (Ledger, Trezor), it does not mean it is a Cold Wallet.

If you connect your Ledger Wallet to a website or sign a transaction, the Ledger Wallet becomes a Hot Wallet.

If you store your Ledger Wallet Seed Phrase on your computer, password manager, or take a picture of your Seed Phrase, then the Wallet is a Hot Wallet.

If you go to a website of a project you are excited to mint, click the mint button, and sign using your hardware wallet, you have now given approval for that smart contract to mint the NFT or to transfer away all your NFTs from the hardware wallet.

“There is no crypto in a Ledger. Ledger is an authentication mechanism. It does not store valuable items.

The valuable items are still on the blockchain. Instead of a Chrome plugin, Ledger is a hardware device that makes it much more difficult for someone to steal stored information.”



-Kyle Thornton - U.S. Head of Customer Success of Ledger During GaryVee's @VeeCon 2022

The Flow of Assets Between the Wallets

You bought an NFT and want a role on Discord, or do you need to show proof of ownership on the project's website?

Buy (or mint) the NFT using your hot wallet, connect to Discord or the project website to get your role, and then move the NFT to your cold wallet.

If you have an NFT in your cold wallet, and your favorite project wants to airdrop something to holders, how do you do so securely?

Option 01: Use a service such as delegate.cash, warm.xyz, tokenproof.xyz, or others.

Option 02: Transfer NFT temporarily from the cold wallet to the hot wallet, connect to the site you want and transact, then move the NFT back to the cold wallet. As if you removed the valuable item from a valuable safe to show it to someone. You are not compromising the whole safe in case they steal that NFT from your hot wallet.

“Use a cold and hot wallet setup! Preferably a ledger for your cold wallet.

The cold wallet should only ever transact with the hot wallet. And the hot wallet should only have a balance necessary for day-to-day use. Phishing is the most likely way that you lose all your crypto.

No matter how smart you are, everyone is susceptible to phishing. It’s just a matter of time before you will get phished, so keep the value at risk at a minimum.”

Toly – Co-founder of Solana Labs

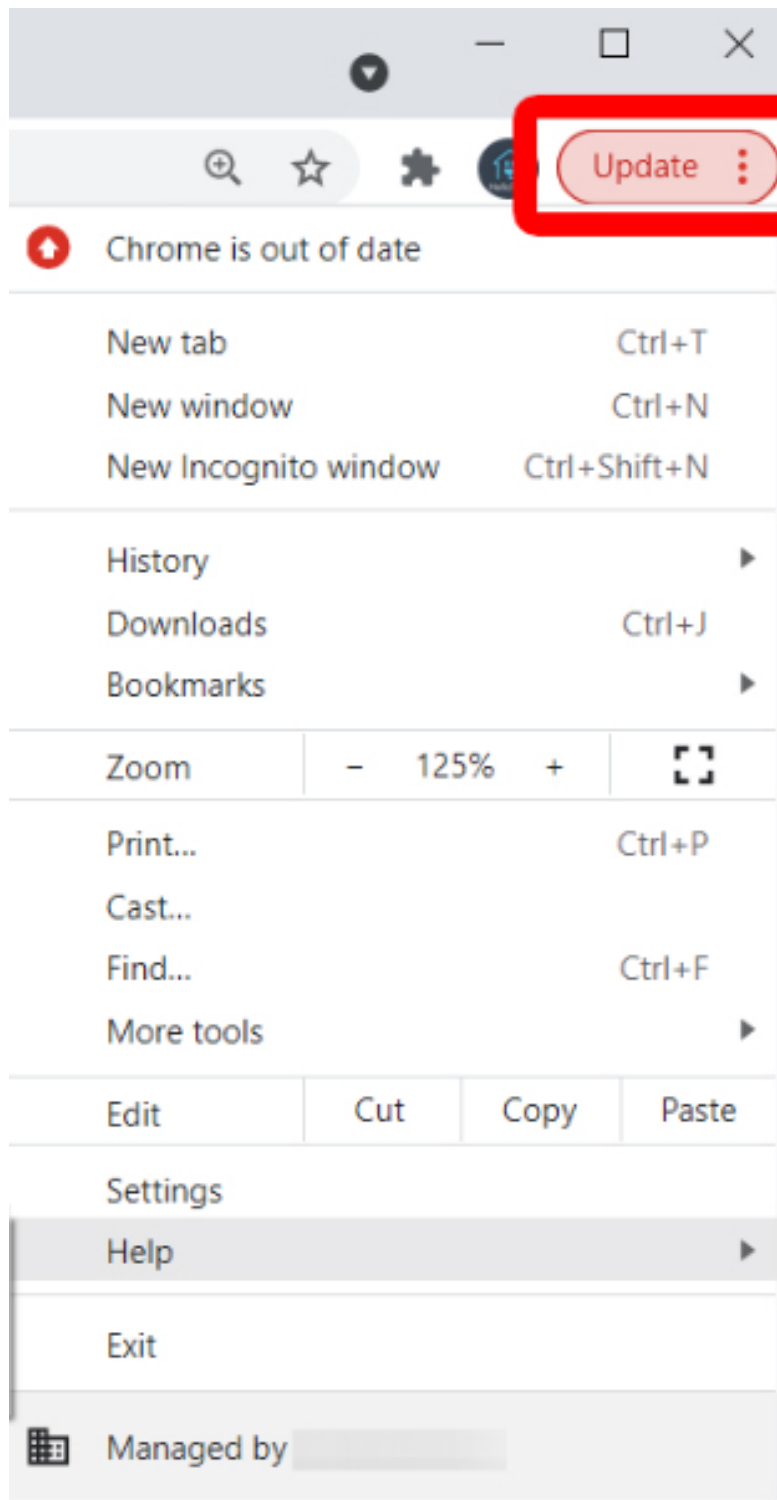
<https://twitter.com/aeyakovenko/status/1610986082992095232>

“It is all about what you can afford to lose. Move assets from your hot wallet to your cold wallet until what is left in it are assets you don’t care if you lose.”

-Fouad Itani – Co-founder of @nftpowerup



Make sure you always keep your Chrome browser updated



“Your New Year’s resolution should be to go full self-custody and practice using a hot and cold wallet setup.”

-Toly – Cofounder of Solana Labs

Tools that could help

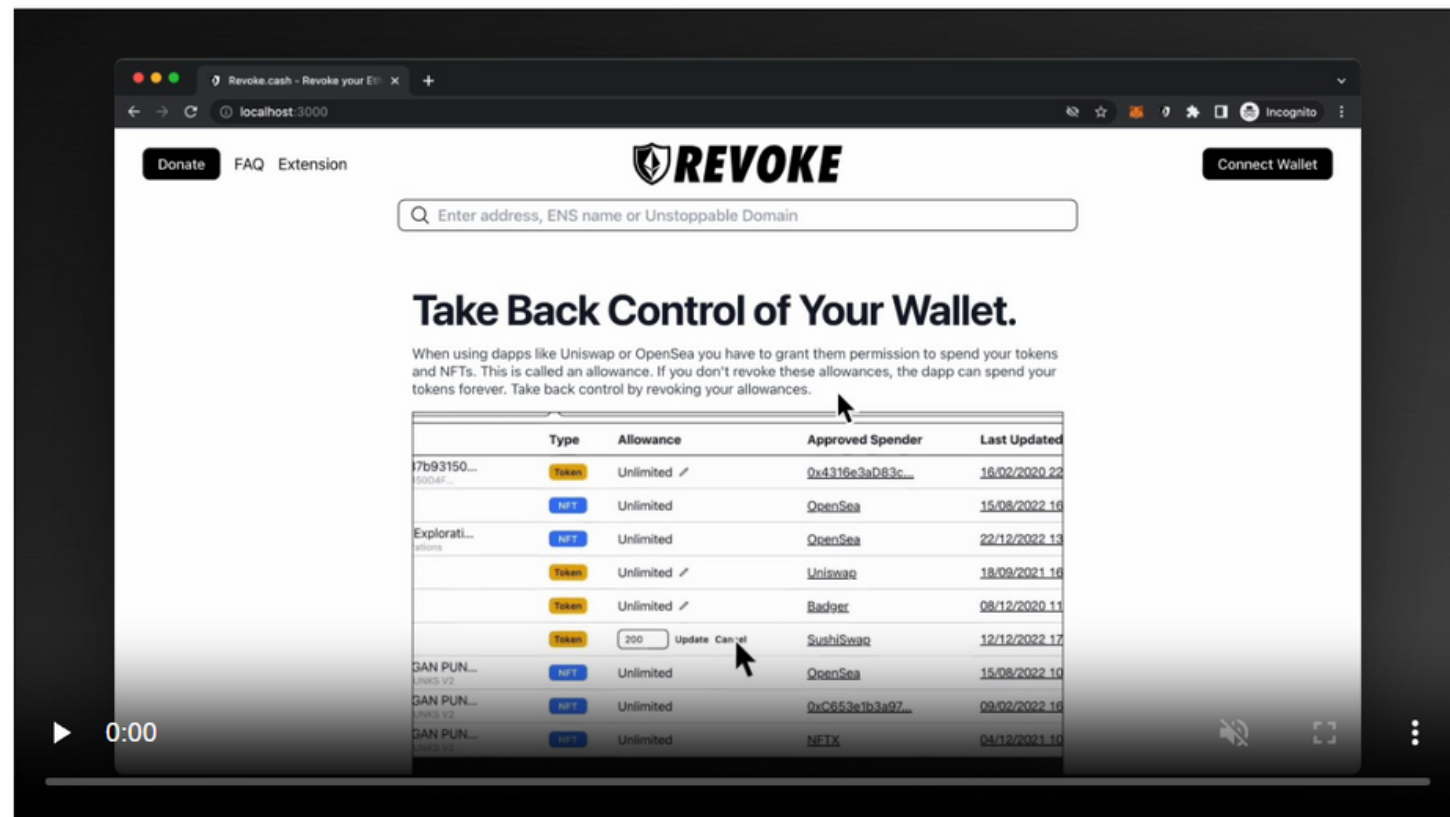
revoke.cash



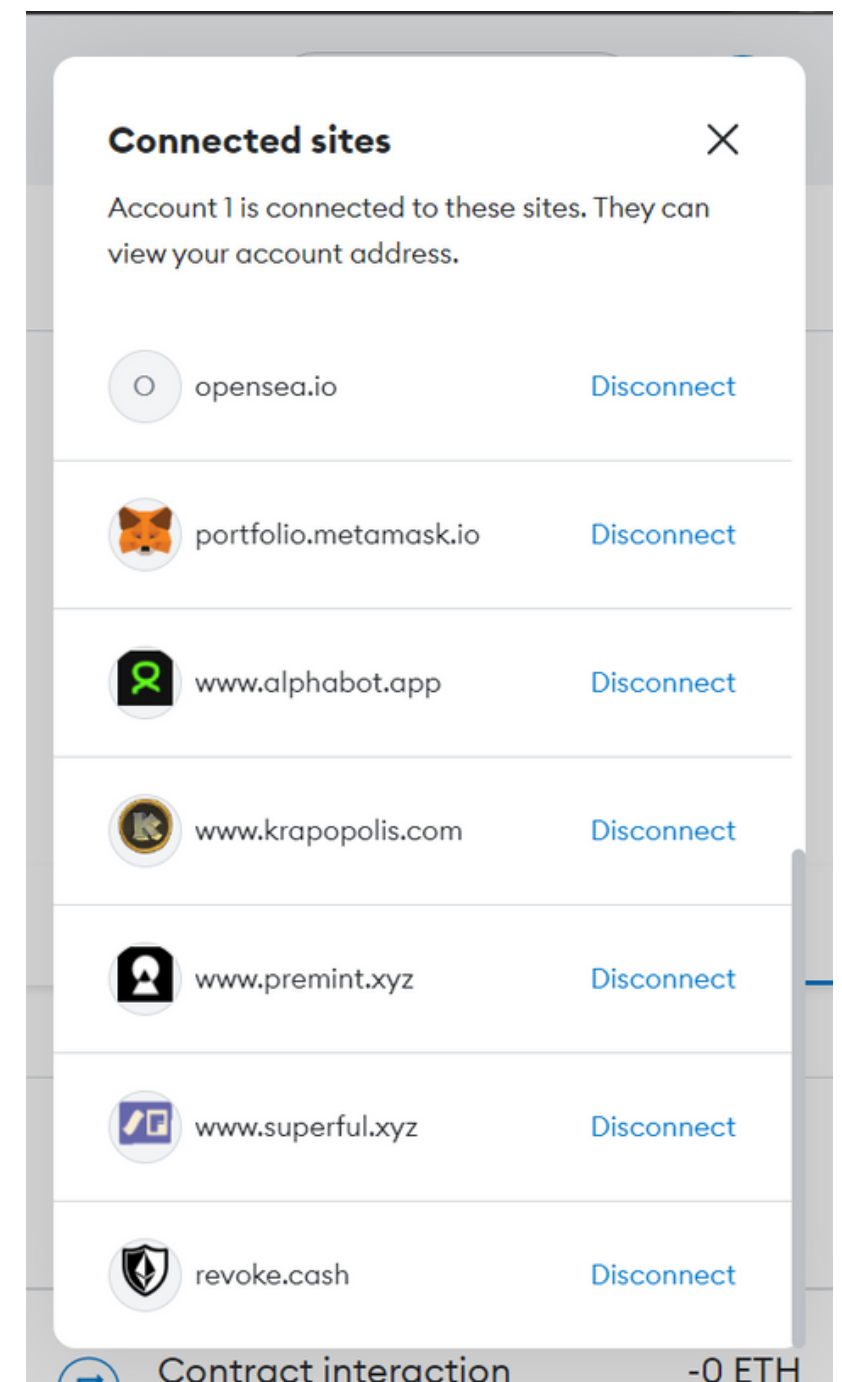
Search accounts by address or domain

Take Back Control of Your Wallet.

When using dapps like Uniswap or OpenSea you have to grant them permission to spend your tokens and NFTs. This is called an allowance. If you don't revoke these allowances, the dapp can spend your tokens forever. Take back control by revoking your allowances.



MetaMask Website Disconnect

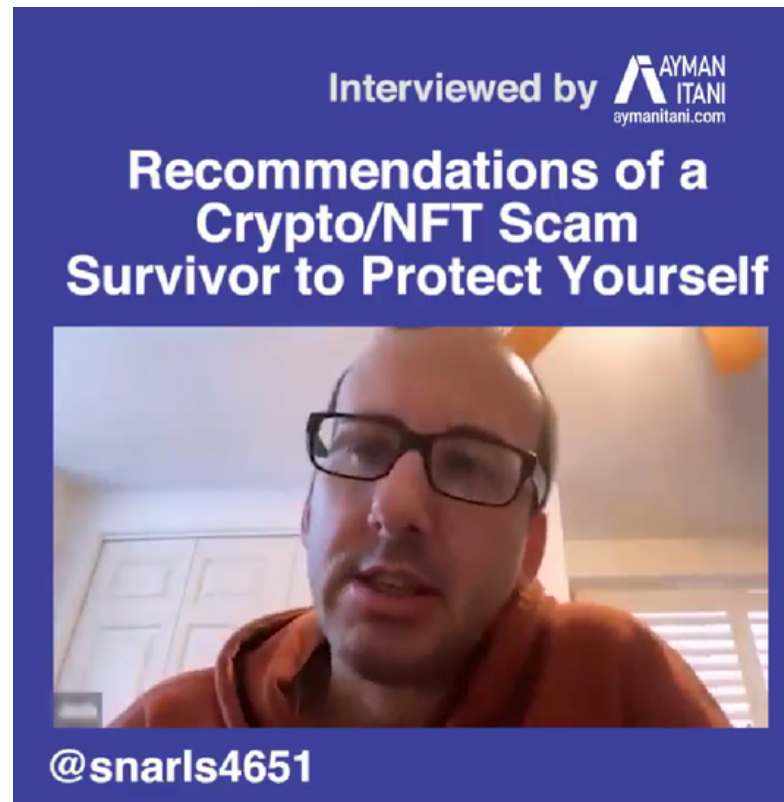


The crypto and NFTs are not stored on the hardware device itself. You use the hardware wallet to authenticate moving crypto or NFTs out of your wallet. It makes it much harder for scammers to move your assets out of a wallet.

The hardware wallet is not a USB crypto NFT storage! You can lose your hardware wallet, buy a new one, connect it to your hardware-protected wallet, and carry on as if nothing happened.

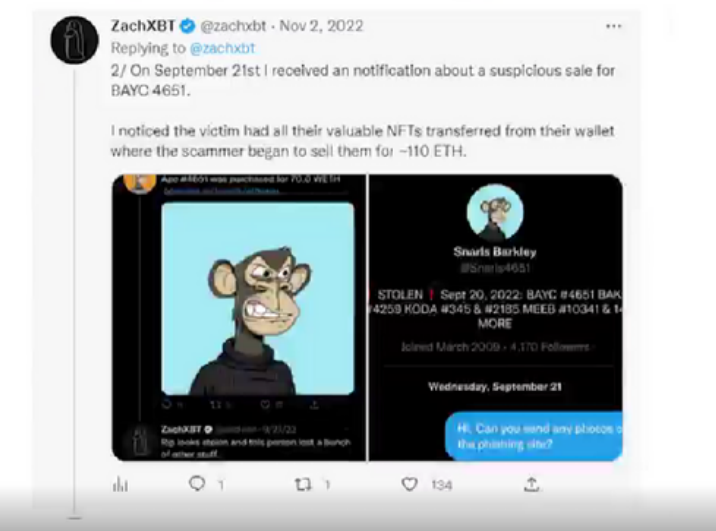
If you are building a project in Web3, you may need an additional wallet, a “Utility Wallet.” It holds the NFTs that give you access to tools (such as @premint_nft). The Utility Wallet has no \$ in it, and the Seed Phrase touched the Internet or is on a computer.

Letting a family member or a your loved one know where you store your seed phrase so that god forbid something happens and you have assets in your wallet, they can get the help of a trusted Web3 person who can help them navigate restoring your assets.



1. Buy and set-up a cold wallet
2. Store your Seed Phrase offline
3. Never click links
4. Turn off DMs
5. Assume everything is a scam

[Recommendations of a Crypto/NFT Scam Survivor to Protect Yourself](#)



[How the Web3 Community Comes Together to Stand with Crypto/NFT Scam Victims](#)



[In Web3, Assume Everything is a Scam](#)



[The Psychological Impact on a Victim of a Crypto/NFT Scam.](#)

The Safest Way to Use MetaMask With Ledger Hardware Wallet:

<https://www.ledger.com/academy/security/the-safest-way-to-use-metamask>

Found a random NFT in your wallet?
Interacting with it could be a big mistake -
Morganlinton.com

<https://www.morganlinton.com/found-a-random-nft-in-your-wallet-interacting-with-it-could-be-a-big-mistake/>

The guide was prepared by Ayman Itani, Web3 Founder and Content Creator after he was this close to becoming a scam victim and could not easily find information on how to protect himself from future scams.

Disclaimer: This is meant to be a guide. There is no liability. Do your own research.

