

Deposit to earn rewards

Sign up and deposit to receive up to **10,055 USDT** in bonuses.
Exclusive for new users only.

Get it now

Ways to Keep Your NFTs Safe and Avoid Getting Scammed

Original:

<https://www.btcc.com/en-US/academy/crypto-basics/ways-to-keep-your-nfts-safe-and-avoid-getting-scammed>

If the recent OpenSea bug has taught us anything, you don't need to be explicitly robbed to lose your NFTs. So here are a few ways to keep your NFTs safe! Read more!

As NFTs gain increasing exposure and value, this has unfortunately drawn the attention of no-gooders that would like to get their hands on your assets — by any means possible.

Fortunately, digital assets are incredibly secure at the blockchain level. This means it's highly unlikely that anybody will lose their assets due to a blockchain-level hack or attack.

Instead, the vast majority of NFT thefts and losses occur due to asset holders falling victim to one of a growing number of scam attempts or failing to adequately secure their assets.

If you're a fan of digital collectibles or have exposure to NFTs, it's important to take the time to understand how to properly protect this rapidly emerging asset class. Here are some ways that you may find helpful.

Use a [Cold Wallet](#) (Hardware Wallet)

If you're currently storing your NFTs on a custodial wallet solution — don't. Centralized platforms can, and sometimes do, get hacked.

Instead, consider purchasing one of the numerous hardware wallets that are now available. These are (generally) small physical devices that are used to isolate your cryptocurrencies and other digital assets from the internet and other potentially dangerous situations. These generally require you to manually sign each transaction, preventing anybody from stealing your assets remotely. But they do require you to take full control of your security, which generally involves backing up and storing your seed phrases/private keys in a safe place.

There is now a huge range of hardware wallets on the market, including options that suit practically any budget, and they're generally considered an essential accessory for the savvy crypto investor.

Hardware wallets can vary dramatically in their form and function, as well as their overall security, but in general, even the most basic options generally provide dramatically better security than most centralized wallet providers.

That said, you will need to ensure that the wallet you choose supports the blockchain(s) you intend to store your NFTs on and also that it supports the specific NFT token standards — since not all will.



[Download App for Android](#)

[Download App for iOS](#)

Use a Different Platform

If the recent OpenSea bug has taught us anything, you don't need to be explicitly robbed to lose your NFTs — you might end up inadvertently selling them at a frustratingly low price instead.

Depending on your NFT marketplace of choice, you may or may not have access to the controls necessary to adequately protect your NFTs against attacks or bugs.

In most cases, NFT marketplaces are non-custodial platforms, which means that you always control your assets even while they're listed on the marketplace or simply presented in your portfolio. However, they do require that users authorize their smart contracts to interact with their assets, e.g. to transfer them to the correct buyer upon sale.

If these smart contracts have bugs, this can leave your NFTs vulnerable.

Because of this, it's important to ensure that the marketplace you use is both highly secure and well-reputed. One of the simplest ways to check this is by looking at their public audits — which essentially check that their smart contracts do not contain any bugs or vulnerabilities, and are overall safe for the public to use.

This might be challenging with newer platforms like LooksRare, which hasn't yet provided a public audit. That said, it's important to balance opportunity with risk, which can make newer platforms worth trying if there are significant incentives or opportunities available.

Remember, not all NFT marketplaces are built equal. Do your due diligence before selecting a platform — doubly so when it's new or hasn't been battle-tested by the masses.

Defend Against Viruses

Computer viruses, though relatively rare, can be devastating to the NFT collector — since they can allow an attacker to exfiltrate data (including your private keys) from your computer in various ways, or potentially even take your system over remotely.

Protecting yourself against viruses is usually a relatively simple task, which begins with knowing how to avoid places that might be looking to install virus-laden code onto your machine. Some of the usual suspects include copycat websites, sites that offer dubious/illegal content, torrents, and other P2P file-sharing services and chat rooms.

In any case, never install a program or open an attachment sent to you by a suspicious source — the vast majority of viruses require you to manually open a file before it can be installed.

Beyond this, consider outfitting your computer with robust antivirus software and ensure your firewall is turned on. This will help to avoid drive-by exploits and may alert you to suspicious files that may already be on your machine.

Macbooks are generally considered to be less vulnerable to viruses due to their built-in runtime protection, but it's not a silver bullet — you'll still need to be cautious since macOS viruses are still a potential threat.



[Download App for Android](#)

[Download App for iOS](#)

Avoid Scammers

Unfortunately, the cryptocurrency industry is riddled with scammers and fraudsters who would like nothing more than to part you from your NFTs and other digital assets.

Avoiding these scams can be a challenge, particularly if you are less experienced since they almost invariably target the least experienced users — since they make the easiest marks.

But in general, it's possible to avoid the vast majority of scams by sticking to a handful of simple rules.

- **Always doublecheck:** When purchasing an NFT, transferring it, using an NFT marketplace, or performing any other task that requires you to log into a website or service that can access your NFTs, always double-check that you have the correct URL. Cross-reference this on their socials for certainty and bookmark the link to prevent you from falling for a fake link.
- **Be wary of imitators:** One of the most common ways NFT holders get scammed is by falling victim to a copycat — i.e. somebody impersonating a reputable individual, entity, and organization, or even a phishing. Only use official lines of communication when dealing with NFT transfers or trades, and always make sure the person you're talking to is who they say they are.
- **Be careful about unsolicited emails and messages:** Telegram, Discord, Twitter, and even your email inbox can be prone to spam, scams, and various types of fraud — particularly if you were caught up in a database leak. If you receive unsolicited messages from anyone over any of these (or other) platforms then odds are it's a scam. Never hand over your private keys or recovery phrase to anybody, regardless of their reasons or status, and absolutely never authorize smart contracts you're not familiar with.

By following these key rules above, you'll be able to avoid the vast majority of risks to your NFTs.