Tips for a Safe Non-Fungible Tokens (NFTs) Experience

2022 Public-Private Analytic Exchange Program

A non-fungible token (NFT) is a cryptocurrency token that is indivisible and unique. One NFT cannot be interchanged with another NFT, and the whole cannot be broken down into smaller parts and used. NFTs are a niche market and a very new commodity. Some NFTs may be valuable, which can make them a target for fraud, counterfeiting, and/or theft. NFTs have been utilized for purposes such as creating digital or crypto-collectibles, managing ownership of digital items within blockchain-integrated games, and proving authenticity of digital art while allowing artists to retain their intellectual property—and in some cases, are used for items such as event tickets.

For a safer experience, ensure you understand Non-Fungible Tokens (NFTs) and key related terms, such as the below, before you invest.

- Smart contract
- Blockchain
- Contract address
- Token ID

The NFT market is a new and evolving market. As with any new investment, there are risks involved. The below chart is designed to assist you in better understanding some of the red flag scenarios you should be aware of.

✓	✗
Website is a known NFT marketplace with good reviews and reputation.	Website has limited or negative reviews or reports indicating customers have been victims of fraud.
Seller has an external site with the NFT road map, history of sales, good reviews, and information about their art.	Seller has an external site with limited or no reviews or other information.
The time, place and price of the NFT sale is widely publicized.	NFT sale information is shared in a limited manner or sent via DM or individual communication.
The cost of the NFT is reasonable in comparison to the rarity and popularity of the NFT.	The cost of the NFT is significantly higher than others of the same popularity or significantly lower than others of the same rarity.
The purchase is conducted on an open-forum website which charges fees.	The purchase is conducted in a private setting to avoid paying any fees.

Common Scams Involving NFTs

Impersonation/Phishing: Scammers can replicate popular NFT websites and marketplaces to trick users into logging into a counterfeit website. These scams can result in account login information being compromised, or trick users into spending money on counterfeit digital artwork on the fake page. Scammers posing as legitimate trading platforms can also send phishing emails containing fake NFT offers, with the aim of obtaining your login information.

To avoid this scam: Always verify the URL of the NFT marketplace website you are using and the sender address of any related email you receive before attempting to login or make purchases.

Rug pull scams: In this type of scam, a criminal promotes an NFT to investors which appears legitimate, but turns out not to be resellable, and then disappears with all the funds, leaving victims with an asset that has little to no resale value.

To avoid this scam: Verify the credentials of any NFT investment project you are pursuing, including researching the background of the project owners.

Counterfeit NFTs: Counterfeit NFTs are copied from someone else's genuine work. Scammers selling counterfeit NFTs trick victims into believing they are buying a unique NFT; however, just like with physical counterfeit goods, the counterfeit NFT has no genuine value.

To avoid this scam: Always confirm the seller's credibility and stick to reputable marketplaces.

Pump and dump scheme: Scammers use these schemes to artificially drive up the price of an NFT by making several bids within a short time span to make it appear as though the NFT is popular. Once the selling price is inflated, the scammers will cash out and sell it to the highest bidder for far above its true value.

To avoid this scam: Review the transaction history of the desired NFT. Several transactions centered around one date could indicate a pump and dump scheme.

Smart Contract scams: Scammers can include hidden fees or clauses in smart contracts designed to steal your money—such as 99% buy or sell fees—and cybercriminals can also exploit vulnerabilities in legitimate smart contracts.

To avoid this scam: Ensure that you review a token's smart contract before purchasing, and engage a trusted resources to help you understand it if necessary.

Tips to Keep You and Your NFT Safe

There are simple steps which can be taken to safeguard your online information as well as your NFT when participating in cryptocurrency markets.

- NEVER invest money you cannot afford to lose.
- Use 2-Factor Authentication (such as a password and a phrase, a fingerprint, or a confirmation text).
- Safeguard your passwords and seed phrase, and do not repeat them or share them.
- When possible, store your NFT in a cold-storage wallet that is protected from hackers.
- Only purchase NFTs from reputable sites—not via social media requests from persons you do not know.
- If you receive an email regarding a password change that you did not request, do not click the links.
- Always ensure you understand the smart contract or obtain assistance from a reputable/trusted person.
- Always log out of your wallet and any sites you may have your wallet connected to.
- If it seems "too good to be true"—it probably is a scam.

Additional Resources

Definitions

investopedia.com - Smart contracts

coinbase.com - What is a smart contract?

Fraud Resources

nftnow.com - How to identify and avoid NFT scams

fbi.gov - Scams and safety on the Internet

secretservice.gov - Combating illicit use of digital assets

Federally Prosecuted Cases

justice.gov - Former employee of NFT marketplace charged in first ever digital asset insider trading scheme

justice.gov - Two defendants charged in NFT fraud and money laundering scheme

2022 Public-Private Analytical Exchange Program
Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

2022 ANALYTIC EXCHANGE PROGRAM