



Republic of Namibia

Financial Intelligence Centre

P.O.BOX 2882, Windhoek
Tel: + 264 61 2835100, Fax +264 61 2835259

Web address: www.fic.na
E-mail address: helpdesk@fic.na

NON-FUNGIBLE TOKEN (NFT) SCAMS

ISSUED: May 2022

1. Background on Non-Fungible Tokens

Non-fungible tokens¹ (NFTs) are cryptographic assets on a blockchain with unique identification codes and metadata that distinguish them from each other. NFTs exist on a blockchain, which is a distributed public ledger that records transactions. Blockchain is the underlying platform that enables the exchange or movement of cryptocurrencies.

Unlike fiat currencies or cryptocurrencies that are fungible², each NFT/token is unique and irreplaceable, thereby making it impossible for one non-fungible token to be equal to another. Each token contains a unique, non-transferable identity to distinguish it from other tokens. They are also extensible, meaning, one can combine one NFT with another to “breed” a third unique NFT. Different types of NFTs include collectible items such as:

- a. Art (both physical and digital);
- b. In-game items such as skins or stickers;
- c. Items in a virtual world, such as a piece of land; ³
- d. Real-world assets such as cars or houses;
- e. Identity-related properties, such as certifications or medical history;
- f. Music and media, big sports moments, virtual fashion, memes and domain names, etc.

The above can be sold, purchased, or exchanged online, with cryptocurrencies.

Essentially, these tokens transform a digital work of art and other collectibles into a “one-of-a-kind”, verifiable digital asset that can be traded on the NFT market or NFT blockchain technology. Many NFTs come with their own unique information, including ownership and transaction details stored under its smart contract. NFTs can have only one owner, this ownership is managed using a unique identification (ID) and metadata that is unique to a particular NFT.

¹ The term token refers to a type of cryptocurrency that is created or exists on a blockchain.

² Fungible goods refer to securities, or other items, that are equivalent or consist of many identical parts such that, for practical purposes, they are interchangeable e.g. one is always equal in value to another bitcoin

³ Virtual land exists in the virtual world or the metaverse. The land can be used for anything, from an empty plot to a mansion, or even an art gallery. Virtual land is usually bought on an NFT marketplace

2. How do Non-Fungible Tokens Work?

Although NFTs have been around since 2014⁴, they have only started gaining popularity recently. They are becoming an increasingly popular way to buy and sell digital artwork. NFTs are considered a safe mechanism through which artists are paid. There is no middleman, the artists have complete control over how, when and at what price they wish to sell their artwork.

Those interested in collecting or investing in non-fungible tokens need a digital NFT wallet. A digital wallet is a cryptocurrency wallet that supports the blockchain protocol on which NFTs are built. Users often use cryptocurrencies which are the medium of exchange on the blockchain.

Three properties that make NFTs so desired are their **uniqueness, rarity and indivisibility**.

- a) **Uniqueness:** NFTs allow you to uniquely define an asset by providing metadata that describes the asset and sets it apart from other assets;
- b) **Rarity:** Rarity or scarcity ensures one can only define each NFT once on the blockchain. It is not possible to infinitely create new NFTs;
- c) **Indivisibility:** One cannot split an NFT, nor can one own a portion thereof. For example, you can own one full bitcoin, however, you can split a bitcoin into smaller denominations known as *Satoshi's*.

Much as there is growth in the usage of NFTs, there are also some challenges and risks associated with them. There has been an increasing trend of scams associated with NFTs. Hence, the FIC, in its duty to enhance public awareness around potentially fraudulent scams presents this communication. Below are some of the common scams associated with NFTs:

⁴ <https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/07/rise-of-a-new-disruptor-how-nfts-are-revolutionizing-the-art-and-entertainment-worlds/?sh=701ac1891a90>

- a) **Fraudulent NFT websites:** Scammers can replicate popular NFT websites and marketplaces to trick users into compromising their account information;
- b) **Fraudulent NFT offers:** Scammers often pose as legitimate trading platforms and send illegitimate/fake offers to NFT owners via email. These phishing emails have a link and if the victim clicks on the link, it takes him/her to a fraudulent NFT marketplace. Once the victim enters their login credentials, the scammers can then use keylogging or other types of spyware to record the victim's information and steal their NFTs;
- c) **NFT giveaways/airdrop scams:** Scammers often pose as legitimate NFT trading platforms on social media to promote NFT giveaway campaigns, also known as airdrop scams. The scammers will usually promise a free NFT if you spread their message and sign-up on their website. With this scam, if the victim links their cryptocurrency wallet credentials to receive their prize, the scammers record the victim's details/information and the scammers use such to steal their library of NFTs once they gain access to the victim's account;
- d) **Social media impersonation:** Social media impersonation is another NFT scam used to trick NFT owners. Using the same level of detail as they would for an illegitimate/fake NFT webpage, cybercriminals create online profiles to convince people of their credibility and sell them illegitimate/fake NFT artworks;
- e) **Counterfeit or plagiarized NFTs:** This happens when scammers steal an artist's work and opens an illegitimate account on the NFT marketplace, where they list counterfeit artwork for auction. Unsuspecting buyers will then make purchases on an NFT that has no value;
- f) **Bidding scams:** These scams typically occur when someone is trying to sell their NFT. An interested buyer submits their highest bid, then they later switch the cryptocurrency they were bidding in to one of lesser value without any communication. This leads to potential

losses for the seller. For example, instead of receiving 1 Bitcoin (equivalent to NAD 628,400.00), the seller then receives 1 Ethereum (which is equivalent to NAD 46,800.00);

- g) **Investor scams:** Scammers often use this to their benefit through the creation of seemingly attractive investment vehicles or projects. If victims invest in such, the scammers disappear with the funds they collected from interested people without a trace. These scams are common with NFTs primarily because of people's ability to remain anonymous when dealing with cryptocurrency.
- h) **Pump and dump schemes:** Scammers use “pump and dump” schemes to artificially “drive up” the price of an NFT. They do this by making several bids within a short time span to make it appear as though the NFT is popular. Once it gains attention and the selling price reaches a value they are comfortable with, they will cash out and sell to the highest bidder.

3. How to protect yourself from Non-Fungible Token scams?

- a) Always verify the URL of the NFT marketplace website before attempting to log in or make purchases;
- b) Verify the sender address of any email received from an NFT trading platform;
- c) Check the account's social media page for verification and/or ensure the link sent to you matches the NFT company's URL;
- d) Use the blue verification tick next to the seller's social media profile to verify their identity and to confirm the seller's credibility;
- e) Find verifiable contact information for the NFT creator you want to purchase from, before transferring money;
- f) Review the transaction history of the desired NFT. Several transactions conducted around one date could indicate a pump and dump scheme;

- g) Create unique and “strong” passwords for your cryptocurrency wallet and other NFT accounts;
- h) Activating two-factor authentication on all of your NFT accounts can also help ensure scammers do not get their digital hands on your valuables. The use of biometrics like fingerprint scanning and facial recognition helps make it nearly impossible for the imposter to replicate your identity;
- i) Before making an NFT purchase, cross-check the price on an official trading platform. If the price appears much lower than what is listed on the legitimate trading site, it is probably a scam; and
- j) Before investing in an NFT from any marketplace, always do your own research to make sure the NFT you are buying is from a verified account and it is the real artist you are dealing with. Most legitimate NFT sellers will have a blue checkmark beside their usernames.

REMEMBER

Dealing in NFTs is not illegal. There is however a growing tendency of such methods being abused to defraud innocent members of the public. Before deciding to trade in NFTs, one should always research the legitimacy and the history of people or entities prior to dealing with them. Remember, you could sustain a loss of some or all your investments. It is therefore advisable not to invest funds that you are not prepared to lose. In the same vein, members of the public are urged to be vigilant and conduct adequate due diligence before investing in NFTs and cryptocurrencies in general. If you become a victim of an NFT scam, immediately file a report with the FIC at the Bank of Namibia or contact the nearest police station to initiate a criminal investigation.