What Parents & Carers Need to Know about NFTs (NON-FUNGIBLE TOKENS)

A non-fungible token, or NFT, is a unique digital record of a particular file – such as an image, audio track or video (non-fungible meaning it can’t be replaced by an identical item). NFTs let digital content producers like artists and designers control how their work is distributed and monetised. The offline equivalent would be owning a limited-edition art print, signed by the artist, with a certificate of authentication. The value of the tokens is incredibly volatile, unregulated and very much based on hype, publicity and marketing. These digital assets – typically collectibles, avatars for social media profiles or character add-ons for online games – are traded in specialised marketplaces using cryptocurrency.

**WHAT ARE THE RISKS?**

**FAKE COLLECTIONS**
When searching for a particular collection of NFTs, it is common for fake versions to appear. Display alongside the originals, which can easily fool a less experienced buyer. Larger projects will be verified, but small ones will not, so check if the volume has been tracked and the authenticity verified – fake collections will have almost no trading history.

**LACK OF CLARITY**
Buying a limited-edition print of a painting isn’t the same thing as owning the original. Likewise, when someone buys an NFT, they’re not acquiring ownership of the original artwork. Some buyers don’t realise that – since many NFTs are publicly on view, purchasing one doesn’t stop other people from making their own copies of your NFT (by saving a screenshot or a file). So, NFTs financially validate what the purchaser is investing in, leaving buyers disenchanted when they actually receive, and as they are unregulated, there’s no procedure for returns and refunds.

**IP THEFT & "WASHTRADING"**
Many online thieves steal NFTs to sell, while another common scam is "washtrading." Here, an unscrupulous trader creates illusions to buy NFTs at multi times the original price (e.g., selling to 8 for 10, who sells to C for 100, who then sells to A for 1000). Once you have paid, you actually own all the same piece. The goal is lure in naive speculators with the illusion of a juicy opportunity.

**STORAGE ISSUES**
An NFT is a cryptocurrency that’s linked to an additional file that contains a digital asset. Due to the cost of storing data on a blockchain, it’s typical for a project founder to store only the NFT’s transaction record "on-chain" to prove ownership – with the accompanying asset stored "off-chain." Whether that storage is in the cloud or on a hard disk, there’s a risk of the asset being lost. So in a large number of cases, the NFT contains a link that points to the image data. If it is not the image data itself.

**TRANSACTION COSTS**
Issuing an NFT requires "minting" it and any future sales require updating a blockchain ledger to record the transaction – at the cost of this – depending on the blockchain and market conditions – can considerably impact supply and demand of "block space." In 2021, the fees paid for NFT transactions on one block regularly cost more than the value of the asset itself, often by hundreds of US dollars.

**PHISHING EMAILS & REPLICA SITES**
There have been instances of messages being sent advertising the availability of new NFTs with a link to a fake website with a very similar title. They link to a "crypto wallet" site, then link their cryptocurrency to the site, able to mint the fake NFTs and then "confirm," the cryptocurrency leaves your wallet and you are left without the NFT you were promised, and very much out of pocket.

**Advice for Parents & Carers**

**CHECK AUTHORSHIP**
Don’t buy NFTs from unknown sources, and be wary of trading outside of official marketplaces. Branded NFTs, like those sold by sports franchises, are typically available through verified marketplaces. NFTs sold by individual artists can be harder to verify. Research their online presence, check for social media profiles, and look for a recognised cryptocurrency wallet before you send a payment.

**WALLET SECURITY**
Wallet security can be the difference between keeping NFTs secure and having them stolen. There are two primary types: a hot wallet (such as metamask) is connected to the internet and vulnerable to hacking. A cold wallet (or "valet") is for storing high-value assets, as interactions can take place without physical record of ownership and a recognised cryptocurrency wallet before you send a payment.

**DON’T GAMBLE**
Beginners should avoid investing significant sums of money in NFTs, given the volatile nature of the market. NFTs can experience rapid price fluctuations, and making people believe that the next project will see a rise in value after over your decision and ensure you fully understand a project before getting involved.

**SPOT THE SCAMS**
Learn what type of message a hacker will leave. They’ll often try to create the illusion that you’re one of a select few who has this incredible, limited-time opportunity. These can appear on social media, via hacking or by being sent links outside official circuits, such as on messaging boards or private messages. The message will come from the service you join, and never click links that aren’t on a project’s official page.

**RESEARCH THE SPACE**
If you’re interested in NFTs and you’ve identified a blockchain of NFTs that you’re interested in, look into the authenticity of marketplaces. Research the background of the creator, the history of the marketplace and the trading records before – avoid artists and teams who insist on remaining anonymous.

Meet Our Expert

JP Verges is Associate Professor at the UCL School of Management and a researcher at the UCL Centre for Blockchain Technologies. His award-winning research on technology and organisation has been published in leading academic journals as well as in two books. JP is also a speaker and startup advisor at FourFour.