How is Phishing used to steal NFTs?

As is the case with most industries, when a product begins to gain significant value, it becomes a target for criminals to profit.

This is what has happened in the NFT industry, as some of these virtual works of art are currently selling for tens of millions of dollars.

Cybercriminals are developing more and more sophisticated ways to trick victims and steal their assets, with one particularly popular method being phishing. So how exactly is phishing used to steal NFTs?

How is Phishing used to steal NFTs?

You might think that the cryptography used in the purchase and storage of NFTs makes the entire system super secure. Yes, it will certainly be difficult for cybercriminals to access the NFT without some of your sensitive data. But this is why phishing is used in the theft process.

There are several ways that online attackers can get into your NFT through phishing, you should be on high alert to keep your assets safe.

1. Phishing via Discord

In recent years, the social networking site Discord has become a popular choice for crypto and NFT enthusiasts who want to connect with each other and their favorite artists or developers. But cybercriminals are also aware of this and thus use Discord to target unknown users.

Fake NFT giveaways are a particularly popular scam method on Discord, where scammers impersonate NFT artists and convince users to reveal certain information in order to be able to participate in the program. give a gift. These giveaway scams often ask you to enter your private key or seed phrase (a set of keywords used to access a cryptocurrency wallet).

However, no legitimate gifting program will ask you to provide these two pieces of sensitive data. So, if you are asked to provide your seed phrase or private key to participate in the giveaway, leave immediately. There's no reason why your private key should be needed to receive any kind of asset, so if you're asked for this, you're definitely running the risk of being scammed.

2. Phishing via Email

Cybercriminals often rely on emails to trick users into revealing sensitive information. Many people have provided their bank account details, login information and even social security numbers through these scams, and now, NFT holders are being targeted. pepper.

So, if you ever receive an email from a suspicious NFT artist, project developer or company, be aware that it could be a scam. Such emails may contain links to NFT discount sites, giveaway sites or something similar and may ask you to provide your seed phrase or private key.

Additionally, these emails can take the form of notifications from the marketplace, alerting NFT holders that someone is believed to have purchased or placing an offer on an NFT that they are selling. The user will be required to click on the link provided and log in to their account. If they do, the scammer will then be able to access their account and the NFTs they are selling on.

This happened in March 2022. Cybercriminals impersonated Opensea, a popular NFT marketplace, and emailed users to access their credentials. Several individuals have fallen victim to this scam and hundreds of NFTs have been lost as a result.

This is why it is important that you do not arbitrarily click on links in emails. If you are notified that your NFT has been sold or a deal has been made, go directly to the marketplace and log into it. You can then see if there is actually any activity related to the property you are selling.

3. Phishing via Instagram

Lots of NFT artists use Instagram to promote new work, discuss developments, and connect with their fans. But this also opened the door to impersonated accounts, and through which victims were duped without a doubt.

Scammers often perform this type of scam by messaging users who follow the artist, the project they are impersonating, or users interested in NFT in general. They will notify the user that they have won a gift and will then provide a link to a website where they can claim their prize.

Of course, there is no real prize and the link is provided only for users to provide scammers with the information they need to access the accounts or wallets they own. At that point, it may be too late for the victim.

But impersonating accounts aren't all Instagram-related NFT scams. More advanced criminals can hack official accounts and target individuals from there. This explicit layer of authentication gives scammers a better chance of tricking users.

4. Phishing via Twitter

Like Instagram, many of NFT's artists and projects gain large Twitter followings from fans and enthusiasts interested in their work. And this just provides another way for cybercriminals to exploit users.

NFT scams on Twitter work the same way they do on Instagram, where criminals target victims through impersonating accounts or hacking official accounts and start from there. Scammers may also publicly post phishing links from fake or compromised official accounts to create a wider attack wave and attract more victims.

Due to this risk, you need to exercise caution whenever encountering an NFT gift link. Again, if you've ever been asked to provide any kind of sensitive information in order to receive a gift, be wary. There's no reason why your seed phrase, login password, or private key should be needed in a giveaway.

You can also use link checking sites to check if a link is legit before clicking on it.

With NFTs reaching incredible prices, it's no surprise that cybercriminals do all they can to capitalize on this booming market. So, if you own any kind of NFT, remember that you should never give out any of your sensitive information, as this can be used to steal your valuables. you quickly.