Beware of NFT scams - this is how you recognize them

The NFT area is still relatively new and is becoming more and more popular, more and more people are investing and this unfortunately also attracts more and more scammers. And they are particularly interested in “newbies” in this area who are not yet very familiar with it.
You have to be extra careful as these scammers can steal all your NFT fortune from your wallet.

Here are examples of NFT scams:

1. **phishing websites**
   One of the biggest dangers with. Fraudsters copy websites here and want to get your account data in order to get your NFTs that are in the account.
   Even if you see an ad on twitter and are asked to click on a link that at first glance looks like the real website with only one ending different, you have already been caught by scammers.
   Example: www.veefriends.com is the main page, where you might also mint a new project. www.veefriends.ne will be shown to you via twitter and you will be enticed to log in there and link it to your wallet. As soon as you do this, the scammers have your data and empty your wallet!
   Important: Always check the URL address - including the endings - before you log in anywhere and connect your wallet.

2. **private messages**
   Scammers often send private messages in Discord or Telegram with offers to win NFT Mints or Raffle prizes. Never click on these links !
   Additional tip: Turn off the DMs in Discord and Telegram & Discord tighten your security settings!

3. **Pump & Dump at NFTs**
   Pump & Dump is often discussed in cryptocurrencies when prices of coins / tokens are artificially inflated. This is also the case with NFTs. This is where groups of people come together who want to artificially inflate the value of an NFT collection and then wait for others to blindly jump in and then sell at the highest price.
   Tip: You can recognize this when only a few buyer and seller addresses appear in the collection. Normally there should be a multitude.
4. **fake accounts**
   Fake accounts are often created on Twitter and Instagram - especially those of well-known NFT collections or well-known personalities in the NFT area. The aim here is to get the money or the wallet of the unsuspecting people
   Tip: Always look at the name of the account and whether it is listed with an addition or spaces or hyphens .NFT collections do not write to you via DM - this is often announced.

Scammers are likely to come up with even more in the future. Therefore, please always check three times before you connect your wallet or click on a link.