**Achtung NFT Scams - so erkennst Du sie**

Der NFT Bereich ist noch relativ neu und wird immer beliebter, immer mehr Leute investieren und das lockt leider auch zunehmend Betrüger an. Und die haben es insbesondere auf “Neulinge” in diesem Bereich abgesehen, die sich noch nicht so gut auskennen.
Du musst besonders vorsichtig sein, da diese Betrüger dir dein ganzes NFT Vermögen aus Deiner Wallet stehlen können.

Hier findest Du Beispiele für NFT Scams:

1. **Phishing Webseiten**
   Betrüger kopieren hier Webseiten und wollen an Deine Account Daten rankommen, um so Deine NFTs, die in dem Account liegen, zu sich ziehen.
   Selbst wenn Du auf Twitter eine Anzeige siehst und auf einen Link klicken sollst, der auf dem ersten Blick wie die echte Webseite aussieht und nur eine Endung anders ist, bist Du den Betrügern schon ins Netz gegangen.
   Beispiel: www.veefriends.com ist die Hauptseite, wo Du vielleicht auch ein neues Projekt mintest. www.veefriends.ne wird Dir über Twitter angezeigt, Du wirst angelockt dich dort einzuloggen und mit Deinem Wallet zu verknüpfen. Sobald Du dies tust, haben die Betrüger Deine Daten und räumen Deine Wallet leer.
   Wichtig: Immer die URL-Adresse prüfen - auch die Endungen - bevor Du Dich irgendwo einloggst und Deine Wallet verbindest.
2. **Private Nachrichten**
   Häufig werden im Discord oder Telegram private Nachrichten von Betrügern verschickt mit Angeboten zu NFT Mints oder Raffle Gewinnen. Klicke nicht auf diese Links!
   Zusätzlicher Tipp: Im Discord die DMs ausstellen und bei Telegram & Discord die Sicherheitseinstellungen verschärfen!
3. **Pump & Dump bei NFTs**
   Pump & Dump ist häufig bei Kryptowährungen im Gespräch, wenn Preise von Coins / Tokens künstlich in die Höhe getrieben werden. Dies gibt es auch bei NFTs. Hier schließen sich Gruppen von Menschen zusammen, die den Wert einer NFT Kollektion künstlich in die Höhe treiben wollen

und dann darauf warten, dass andere blind einsteigen und dann am höchsten Preis verkaufen.
Tipp: Du erkennst dies, wenn nur wenige Käufer und Verkäufer Adressen bei der Kollektion auftauchen. Normalerweise sollte es eine Vielzahl sein.

4. **Fake Accounts**
   Fake Accounts werden häufig auf Twitter und Instagram angelegt - insbesondere die von bekannten NFT-Kollektionen oder bekannten Persönlichkeiten im NFT Bereich. Ziel ist auch hier das Geld bzw. an die Wallet der nichts ahnenden Leute zu kommen.
   Tipp: Schaue immer auf den Namen des Accounts und ob dieser mit Zusatz oder Leerzeichen, Bindestrich etc. aufgeführt ist. Bekannte Persönlichkeiten / NFT Kollektionen schreiben Dir nicht per DM.

In Zukunft werden sich Betrüger wahrscheinlich noch mehr einfallen lassen. Deswegen bitte immer 3fach prüfen, bevor Du Dein Wallet connectest oder auf einen Link klickst.