Nicholas Lo
@nic_web3

9 Most Common Crypto Scams In 2023

Phishing Scam

Phishing scams have been around for some time but are still popular.

Scammers send emails with malicious links to a fake websites to gather personal details, such as cryptocurrency wallet key information.

Unlike passwords, users only get one unique private key to digital wallets. But if a private key is stolen, it is troublesome to change.

To avoid phishing scams, never enter secure information from an email link.
Always go directly to the official site.

Rug-Pull Scam

This involves investment scammers "pumping up" a new project, NFT or coin to get funding.

After the scammers get the money, they disappear with it. The setup for these investments prevents people from selling after purchase, so investors are left with a valueless investment.

A popular version of this scam was the Squid Coin Scam. The price of the Squid token went from 1 cent to about $90 per token.
The scammers made about USD 3 million.

Want to learn how to verify a project?
Refer to my previous post.

Investment Scam

Scammers contact investors claiming to be seasoned "investment managers."

The "investment managers" claim to have made millions investing in crypto and promise their victims to make money with investments. To get started, the scammers request an upfront fee. Then, instead of making money, the thieves simply steal the upfront fees.

The scammers may also request personal identification information, claiming it's for transferring or depositing funds.

This kind of scam can get really fancy, from fake celebrity endorsements to Elon Musk deep fake videos

Man-In-The-Middle Attack

When users log in to crypto accounts in a public location, scammers can steal their private, sensitive information.

A scammer can intercept any information sent over a public network, including passwords, cryptocurrency wallet keys and account information. This is done by intercepting Wi-Fi signals on trusted networks if they are in close proximity.

The best way to avoid these attacks is to block the man in the middle by using a VPN encryption.

Romance Scam

Dating apps are no stranger to crypto scams.

These scams involve relationships, typically long-distance and strictly online, where one party takes time to gain the other party's trust.

Over time, one party starts to convince the other to buy or give money in some form of cryptocurrency.

After getting the money, the dating scammer disappears. These scams are also referred to as "pig butchering scams."

Giveaway Scam

There are many fraudulent posts on social media outlets promising crypto/NFT giveaways.

Some of these scams also include fake celebrity accounts promoting the giveaway to lure people in.

However, when someone clicks on the giveaway, they are taken to a fraudulent site asking for verification to receive the bitcoin. The verification process includes making a payment to prove the account is legitimate.

The victim can lose this payment or, worse yet, lose their personal information and cryptocurrency stolen by a malicious link.

Ponzi Scam

Ponzi schemes pay older investors with the proceeds from new ones.

To get fresh investors, cryptocurrency scammers will lure new investors with bitcoin. It's a scheme that runs in circles, since there are no legitimate investments; it is all about targeting new investors for money.

The main lure of a Ponzi scheme is the promise of huge profits with little risk. There are always risks with these investments, however, and there are no guaranteed returns.

Fake Crypto Exchanges

Scammers may lure investors in with promises of a great cryptocurrency exchange, maybe even some additional bitcoin.

But in reality, there is no exchange and the investor does not know it's fake until after they lose their deposit.

Stick to known crypto exchange markets to avoid an unfamiliar exchange. #DYOR and check industry sites for details about the exchange's reputation and legitimacy before entering any personal information.

Fake Employment

Scammers will also impersonate recruiters or job seekers to get access to cryptocurrency accounts. With this ploy, they offer an interesting job but require cryptocurrency as payment for training.

There are also scams when hiring remote workers. E.g. North Korean IT freelancers are trying to capitalize on remote job opportunities by presenting impressive resumes and claiming to be US-based. They seek projects involving virtual currency and use access for currency exchanges. They then hack into the systems to raise money or steal information for the North Korea Government.