Here is a 5 Crypto Scams List in 2022

Original:
https://www.btcc.com/en-US/academy/research-analysis/here-is-a-5-crypto-scams-list-in-2022

Scams are inexorably linked to financial transactions. Cryptocurrency has the same problem.

Wormhole, a cryptocurrency exchange site, was hacked in February 2022 and lost $320 million. According to a report by the Federal Trade Commission, bitcoin scammers have taken over $1 billion since 2021.

Using a digital wallet, a person can convert digital currency into cash by depositing it into a bank account. Digital currency is distinct from cryptocurrencies like bitcoin. It is more difficult to recoup from theft because it doesn't run via financial institutions and uses the blockchain for verification.

However, despite the fact that bitcoin is a more recent trend, thieves are still committing fraud. Scams involving cryptocurrency are all too typical.

How Do Crypto Scams Work?

Scammers in the crypto world are after your cryptocurrency holdings just like they would be for your cash.

Scammers in the cryptocurrency market employ many of the same techniques used in the financial sector, such as pump-and-dump schemes, which use exaggerated claims about an asset's worth in order to convince unsuspecting investors to buy it.

For the latter, says Halbert Hargrove's director of technology and cybersecurity and financial advisor, Shane Cummings, the target may be a victim of a hack into their cryptocurrency wallet or an investor duped into sending digital assets as payment for a fake transaction.

Every single one of these attacks has the same goal in mind: to trick victims into handing over their private information or into sending over their hard-earned NFTs or other valuable digital assets.

According to Chengqi "John" Guo, a professor of computing information systems and business analytics at James Madison University, "as an instrument, crypto scams are particularly appealing to

nefarious agents who enjoy cryptocurrency's swift conversion to fiat money, ready-to-use third-party transaction applications, and rich obfuscation techniques."

Crypto Scams List in 2022

1. Bitcoin Investment Plans

Investors in bitcoin investment schemes are contacted by scammers who claim to be experienced "investment managers." According to the bogus investment managers, they've made millions by investing in bitcoin and convince their victims that they, too, can make money by investing.

Scammers typically demand money up front before they will begin their scam. Thieves merely take the upfront fees instead of making any money. For example, they may claim that they need personal identification to transfer or deposit money, and thus acquire access to cryptocurrency.

Fake celebrity endorsements are used in another kind of investment scam. Scammers use real images of celebrities and use them on fictitious websites, commercials, and other media to give the impression that the celebrity is endorsing a lucrative investment. Credible companies like ABC or CBS with a professional-looking website and logos appear to be the sources of these assertions. The endorsement, on the other hand, is bogus.

2. Phishing Scams

Despite their long history, phishing scams are still widely used today. For the purpose of obtaining sensitive information, such as the private keys to a user's cryptocurrency wallet, scammers send out

emails containing dangerous links.

Digital wallets, unlike passwords, only provide users with a single private key. If a private key is taken, however, it is time consuming and cumbersome to replace it. To update a wallet's key, the user will need to establish a new wallet.

Phishing scams can be avoided by avoiding clicking on links in emails that ask for personal information. No matter how credible a site or link appears, always go directly to the website.

3. Cryptocurrency Giveaways on Social Media

Social media posts claiming to offer bitcoin giveaways are common. Fake celebrity accounts advertising the giveaway are also used in some of these frauds to entice victims.

Clicking on the giveaway will take you to a bogus site where you will be asked for verification in order to obtain your bitcoin. The account verification process comprises making a payment in order to show that the account is real.

If the victim clicks on a fraudulent link, their personal information and cryptocurrencies can be taken. This payment can be lost.

4. Ponzi Schemes

Ponzi schemes are a type of pyramid scheme in which new investors pay off the older ones with their own money. Cryptocurrency scammers will use bitcoin as a bait to attract new investors. Due to the fact that there are no legal investments, this is a scam that goes around and around.

Most people are drawn to Ponzi schemes because they promise high returns and low risk. These investments, however, have dangers, and there are no assurances of a profit.

5.Romance Scams

Dating apps are no strangers to cryptocurrency frauds. This type of scam involves long-distance relationships where one side takes time to acquire the trust of the other party. One party gradually begins to persuade the other to buy or give money in a cryptocurrency.

The dating scammer vanishes after receiving the money. The term "pig butchering scams" is also used to describe certain types of fraud.

How to Keep Cryptocurrencies Safe?

Here are some of the most prominent red signs to look out for when it comes to bitcoin scams:

- Promises of big returns or investment increases by double
- Accepts just cryptocurrencies as a payment method
- Obligations imposed by law;
- In emails, social media posts, or any other form of communication; typos and grammatical problems
- Extortion and blackmail are two common forms of manipulation
- Promises of a bounty of cash
- The use of out-of-place celebrity endorsements or false influencers

Practicing good digital security habits such as strong passwords, utilizing only secure connections or VPNs, and storing digital wallets in a secure location will help protect them from scammers.

Both mechanical and digital wallets are available for use. Because they are housed online, digital wallets are more vulnerable to attack. The bitcoin wallet and keys are stored offline on a device with a hardware wallet.

The Federal Deposit Insurance Corporation does not cover cryptocurrency, thus protecting it is essential. Don’t let anyone else have a copy of your wallet’s keys or access codes.