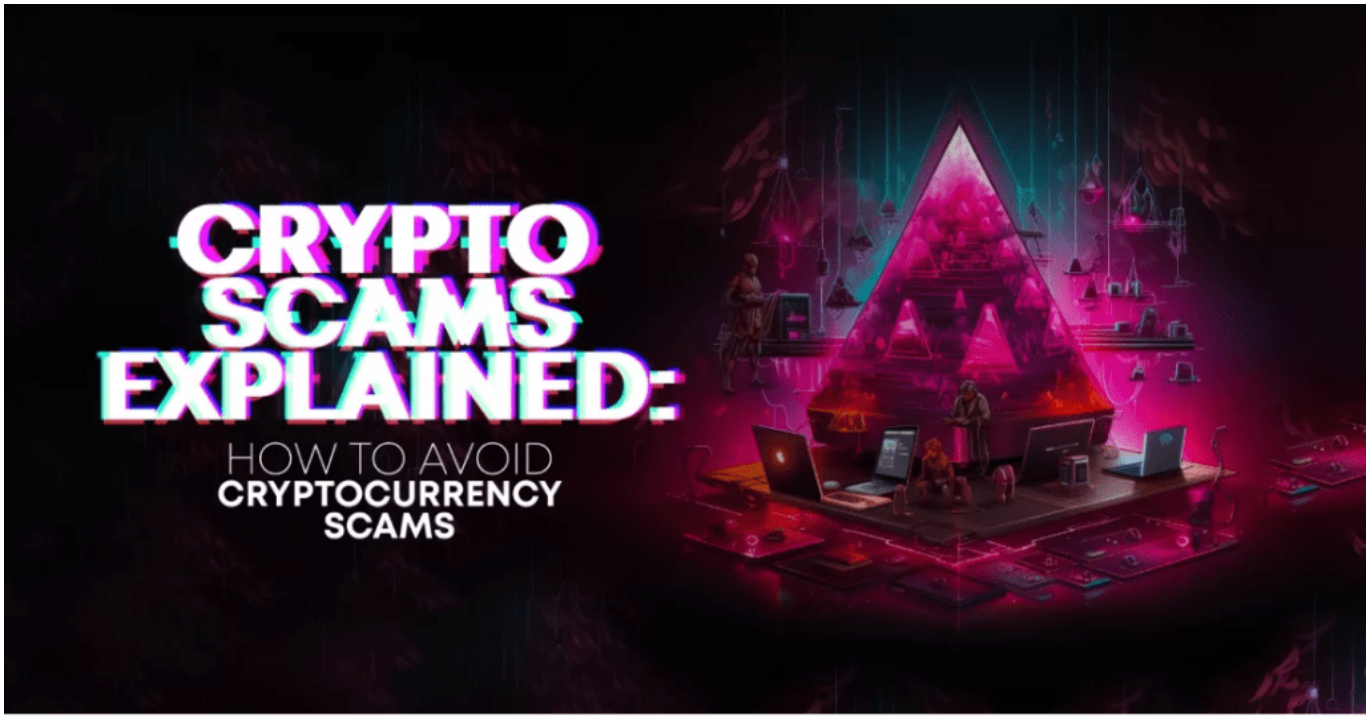
8 Types of Crypto Scams to Avoid in 2024

Original:
https://www.btcc.com/en-us/academy/crypto-basics/8-types-of-crypto-scams-to-avoid-in-2024

Have you fallen victim to a cryptocurrency scam? If so, you're not alone – crypto users lost close to $2 billion to scams, rug pulls, and hacks in 2023, and over $1.4 billion in the first half of 2024.

One crucial step towards safeguarding yourself is to gain a comprehensive understanding of the diverse types of cryptocurrency scams that exist. These range from phishing attempts to elaborate Ponzi schemes, with scammers continually devising new tactics to exploit unsuspecting individuals. By staying vigilant and well-informed, you can significantly mitigate the risks.
Our comprehensive guide outlines eight prevalent types of crypto investment scams. Let's delve into the details.



What is a Crypto Scam?

In essence, a cryptocurrency scam is an illicit attempt to unlawfully obtain money, personal data, or digital assets from an individual using cryptocurrencies. The decentralized and often pseudonymous nature of cryptocurrencies facilitates such fraudulent activities, making it challenging to trace and recover stolen funds. Unfortunately, once money is lost in a crypto scam, retrieving it is typically a daunting and unlikely task.

The variety and sophistication of scams can be confusing, making it difficult to discern genuine opportunities from scams. A common tactic employed by scammers is to promise investors unrealistic returns with minimal to no risk, enticing individuals with the prospect of substantial financial gains. These scams do not discriminate, targeting not only novices but also seasoned investors and even large corporations.

What Are the Eight Most Common Cryptocurrency Scams?

As we mentioned above, crypto users lost close to $2 billion to scams, rug pulls, and hacks in 2023 and over $1.4 billion in the first half of 2024. Let’s dive deeper into each of the scams, see how they work, and how you can prevent falling victim to them.

Phishing Scams

A phishing scam is a deceptive tactic employed by fraudsters, where they create fake websites, social media profiles, or send phony emails to trick you into divulging your personal information, including your identity, passwords, and cryptocurrency wallet keys. These scams cunningly imitate legitimate cryptocurrency platforms, such as exchanges, to instill trust in unsuspecting victims. The emails or messages you receive may seem credible, often containing enticing offers or urgent requests for your sensitive information, such as your private key or login credentials.

Once you have unwittingly disclosed this information to the scammers, they can then exploit it to steal your digital assets. This might involve accessing and emptying your cryptocurrency accounts on genuine platforms using the details you provided. Therefore, it's crucial to be wary of any unsolicited communication asking for your personal or financial information, especially if it promises too-good-to-be-true deals or creates a sense of urgency.

Romance Scams

Another perilous scam to be vigilant about involves emotional manipulation, particularly in the form of crypto romance scams. In these schemes, fraudsters create fictitious profiles on dating websites or popular social media platforms to gain your trust through a meticulously crafted, often lengthy, relationship. Over the course of weeks or even months, they establish a bond with you, leveraging emotional connections to their advantage.

Once the scammer has cultivated your trust, they'll introduce the idea of investing in a cryptocurrency scheme or request a direct cryptocurrency transfer. However, instead of using the funds for the promised investment, the money is promptly diverted into their own pockets. The financial losses incurred through these scams can be staggering, reaching astronomical amounts. According to AARP, in November 2023, the U.S. Justice Department and Secret Service retrieved $9 million worth of Tether from scammers who had targeted more than 70 victims. A large portion had been targeted through romance schemes.

Impersonation and Giveaway Scams

Scammers are increasingly adopting deceptive tactics by impersonating celebrities, influencers, and reputable companies to promote spurious investment opportunities and bogus giveaways. Here's a closer look at how these scams unfold:
Fake Celebrity Endorsements: Fraudsters create spurious social media profiles or infiltrate genuine, verified accounts. They leverage these platforms to advertise fraudulent cryptocurrency

schemes, promising lucrative giveaways or investment prospects with guaranteed high returns. Victims are enticed to send cryptocurrency to a specified address, under the false pretense of receiving a significant return in the future.

Social Media Scams: Scammers establish phony profiles, pages, or groups on platforms like Facebook and Instagram. They'll then use those pages to promote fraudulent investment schemes or phishing links – in 2024, fake social media scams, sometimes called deepfakes, surpassed $25b. Scammers managed to achieve this by posting fake testimonials, success stories, and screenshots of large profits to lure victims. The links on these posts will direct users to a site that captures login credentials or private keys.

Crypto Investment Scams

Scammers sometimes design enticing crypto investment schemes that promise high returns with little to no risk. They often involve elaborate ways to convince you that their investment is safe and profitable. The most common types include Ponzi schemes, pump-and-dump schemes, and fraudulent ICOs and NFTs.

Here's how they work:.

Ponzi Schemes
Ponzi schemes operate by leveraging new investors' funds to pay off early investors, fostering the misconception of a thriving investment opportunity. This strategy attracts an influx of additional investors, but as the pool of new investors dwindles, the scheme inevitably implodes, resulting in substantial losses for the majority of participants. Although these schemes persist today, they proliferated during the 2017/2018 cryptocurrency boom, manifesting primarily as high-yield investment programs (HYIPs).

Pump and Dump Schemes
Pump-and-dump schemes involve scammers artificially inflating the price of a cryptocurrency through deceitful claims. They accumulate a significant quantity of a low-priced, low-volume cryptocurrency and subsequently embark on an aggressive promotional campaign across social media and other marketing channels. This strategy lures unsuspecting investors, further escalating the cryptocurrency's value. At the peak of the surge, the scammer liquidates their holdings, triggering a dramatic price crash and leaving other investors with depreciated or worthless assets.

ICO and NFT Scams
Initial Coin Offerings (ICOs) and Non-Fungible Tokens (NFTs) serve as legitimate fundraising avenues for projects. However, scammers frequently exploit these mechanisms by soliciting funds for fictitious endeavors, such as promised revolutionary technologies or exclusive digital assets. They entice investors with spurious promotional materials but once they have amassed sufficient

funds, they abruptly vanish, leaving investors with empty promises and financial losses.

Blackmail and Extortion Schemes

The modus operandi of these schemes mirrors that of traditional monetary scams, albeit with cryptocurrency as the medium of exchange. Crypto scammers employ blackmail or extortion tactics, leveraging their possession of sensitive information like personal photos, videos, or financial records to coerce victims into making cryptocurrency payments. The victims acquiesce due to the fear of the consequences should this sensitive data be disclosed, often under the threat of a looming deadline. Thus, the scammers succeed in extracting payments in cryptocurrency from their intimidated victims.

Cloud Mining Schemes

Victims of these scams fall prey to deceitful tactics employed by fake companies posing as crypto mining contractors. These contracts entice with promises of profits derived from cryptocurrency mining without requiring ownership of costly equipment. However, the truth is that these companies are mere fronts set up by scammers who neither possess mining equipment nor the financial means to fulfill their promised returns to investors. In some instances, these mining scams initially function as Ponzi schemes, where initial investors are paid using funds sourced from newer investors, further perpetuating the fraudulent cycle.

Fake Cryptocurrency Exchanges and Wallets

To pilfer funds, scammers devise fake cryptocurrency exchanges and wallets that mimic legitimate platforms, rendering them nearly indistinguishable to the unsuspecting eye. These counterfeit sites entice victims with alluring offers, including reduced fees, enhanced security, and exclusive functionalities. However, once victims create accounts and deposit their funds, the scammers swiftly abscond with the stolen money, leaving the victims empty-handed.

In May of this year, two men in the UK stole almost £6 million worth of cryptocurrency from victims. They replicated the website of Blockchain.com so they could access victims’ online wallets.

Download App for Android

Download App for iOS

SIM-Swap Scams

These crypto fraud tactics are exceptionally sophisticated, leveraging victims' mobile numbers as a gateway to their online accounts, including crypto wallets. Scammers exploit this information to intercept verification codes and even reset passwords, thereby gaining direct access to digital assets. They can acquire mobile numbers through various means, such as social media profiles, data breaches, or phishing emails.

Scammers can often learn your mobile number through social media, data breaches, or a phishing email. With this information, a scammer can then contact your mobile provider and ask for a SIM swap which is how they can read your messages and bypass any two-factor authentication you have set up on your crypto exchange or wallet.

How to Avoid Crypto Scams Early?

Spotting a crypto scam early is a great way of protecting yourself against falling foul of a fraudulent scheme. You can do so by:

- Analyzing the investment's whitepaper
- Looking for red flags in communication
- Spotting unrealistic promises

The best ways to protect yourself against being scammed is to:

- Check third-party reviews
- Ignore unsolicited messages
- Verify any endorsements or partnerships
- Move slowly before investing
- Bookmark important links

Download App for Android

Download App for iOS

Where & How to Buy Crypto Safely?

If you want to buy cryptocurrencies safely, you can easily start by creating an account with BTCC, one of the longest-running exchange in the world. As a old exchange enjoy good reputation, **BTCC** is more reliable with no reported hacks or security breaches to date.

BTCC is among the best and safest platforms to buy cryptocurrencies. The reasons why we introduce **BTCC** for you summarize as below:

Industry-leading security with no reported hacks or security breaches to date

BTCC attaches great importance on security. Since founded in 2011, BTCC has never been hacked or been a victim of any other kind of successful malicious attack, which fully illustrates its security capabilities. Through measures like segregation of assets, 1:1 storage of users' assets, money laundering prevention and identity authentication and no collateralising tokens for loans, BTCC enjoys good reputation in asset security.

High liquidity & volume

BTCC is ranked top 10 by trading volume on both CoinMarketCap and CoinGecko, the world's two largest crypto information platforms. BTCC prides itself on providing crypto futures trading services to users worldwide with market-leading liquidity, offering perpetual futures on over 300 cryptocurrencies, including BTC, ETH, DOGE, LTC, SOL, XRP, SHIB, etc.

Extremely low fees

Charging high fees means less return for investors. Compared with other major exchanges, BTCC only charges 0.06% for both takers and makers, which are far below the industry average. According to the largest and most recent empirical study on crypto exchange trading fees, the average spot trading taker fee is 0.2294% and the maker fee is 0.1854%.

High and rich bonus

BTCC holds all kinds of campaigns where investors can participate to win exciting bonus. For example, new users can get rewards up to 10,055 USDT coupon through completing relevant missions, like registration, identity verification, first deposits, cumulative futures trading volume, etc. Besides, becoming VIP also can enjoy rewards like VIP-exclusive perks, including discounts on trading fees, access to exclusive campaigns, BTCC merch, priority customer support, fast withdrawal, and many more.

Excellent customer service

BTCC also gains great reputation in terms of customer support. If you are confused or have problem in the process of trading currencies, you can obtain customer support via email and live chat, BTCC offers 24/7 online customer service for you.

You May Like:

Best AI Coins On Solana To Buy In 2024

Best Crypto Airdrops In 2024

Best Energy Stocks To Buy In Canada For August 2024

What is eTukTuk (TUK) Coin: Next Token To Explode In 2024?

Best Crypto Trading Bots In Canada For August 2024

How to Choose Best Crypo Exchanges in Canada

A Beginner's Guide: How To Buy Meme Coins In Canada In 2024

A Beginner's Guide: How to Trading Crypto in Canada in 2024

What Is Mumu the Bull (MUMU) Meme Coin: Something You Need Know About It

Dogeverse ($DOGEVERSE) Meme Coin Review & Analysis: Meme Coin $DOGEVERSE Launches on DEXs

[What Is Beercoin (BEER) Meme Coin: Next 100x Solana-Based Meme Coin?]

[Binance Unveils New Megadrop Project $LISTA: What is Lista(LISTA) Coin?]

[Top Canadian Crypto Stocks to Buy in 2024]

[Canada Cryptocurrency Market Analysis and Outlook 2024]

[SEC Approves Spot Ethereum ETFs: When Will Ether ETFs Begin Trading?]

[Ethereum ETFs Review: Will Spot Ethereum ETF Get Approval This Year?]

[Best Cryptos to Buy Amid Higher Likelihood of Spot ETH ETF Approvals – Pepe, Arbitrum, Uniswap]

[How To Buy Ethereum (ETH) In Canada: A Updated Guidance For 2024]

[Is China’s Gold Buying Frenzy a Catalyst for Bitcoin’s Next Big Rally?]

[Oil Price Analysis & Forecast For 2024]