CBSW
TAX & BUSINESS ADVISORS

Providing you professional direction

Monthly Information Newsletter – Tax & Super

April 2023

Reducing the risk of crypto scams

ASIC has released fresh and timely information around crypto scams.

Scammers use cryptocurrencies, like bitcoin or ether, because they are not easily recovered. Crypto can be sent overseas quickly with limited oversight. If you lose your money to a crypto scam, your money is likely gone. If you buy crypto, only invest what you can afford to lose as it's a somewhat volatile investment.

How to spot a crypto scam

If you're investing in crypto, watch out for these potential red flags:

1. Unexpected contact

Someone you don't know contacts you with investment advice or offers:

- through phone, email, social media or text message
- claiming to be an investment manager or broker
- through an online forum discussing crypto.

2. Recommendations from someone familiar

You may hear about it through:

- an advertisement or fake celebrity endorsement on social media
- an online influencer promoting a token and claiming to have made huge, quick profits
- family and friends who have unknowingly been scammed themselves
- an online romantic partner who asks for money paid in crypto or suggests an investment opportunity.

3. Pressure to take action

You are being pushed to:

- transfer crypto off your current exchange and invest through their site
- use crypto to pay an individual or for a financial service
- download an investment app not listed on Google Play Store or Apple Store
- deposit money to invest into different bank accounts
- pay tax or invest more in order to access your funds.

4. Something just doesn't feel right

You're not sure about:

- the crypto investment offers 'guaranteed' high returns or 'free' money
- crypto service providers that withhold investment earnings for 'tax purposes'
- strange tokens appear in your digital wallet that you did not trade yourself
- there is little paper trail for crypto investments you make
- the document describing the crypto investment (sometimes called a 'whitepaper') is poorly written or non-existent
- online searches indicate that an entity may be a scam or has bad reviews
- a work from home job offer that requires you to purchase cryptocurrency.

How crypto scams work

There are three main types of crypto scams:

1. Investing in a fake crypto exchange, website or app

Scammers create fake crypto trading apps to steal your money. The giveaway is usually that they ask you to download the app from their website. They may appear on legitimate platforms like Google Play and Apple, but are usually promptly removed. If you find one on an app store, check for overly positive reviews and be cautious.

2. Fake crypto tokens, investments or jobs trading crypto

- Scam tokens in crypto wallets – A mystery token appears in your crypto wallet, seemingly worth thousands. If you

sell it, a 'smart contract' is activated. This transfers your legitimate crypto tokens and private keys to the scammer.

- Crypto Ponzi scheme – You are promised large 'returns' by investing in crypto. But the promoter uses money from other investors to pay your 'earnings'. For more on how these scams work.
- Jobs 'trading crypto' – You apply for a job ad for 'crypto traders', for a fake or impersonated financial services firm. You are told to set up multiple bank and crypto accounts, and are paid well for a few hours of work a week. You think you're trading crypto for the entity's 'investors' or 'clients', but you're actually money laundering for the scammers. You could be charged by state or federal police.

3. Using crypto to pay scammers

- Requests for payment in crypto – An online romantic partner, job recruiters, work from home job, or fake financial services firm asks for payment in crypto only.
- Giveaway scams – Fraudulent posts on social media offer to match or multiply crypto invested with them in a crypto giveaway scam. Often, this uses fake celebrity endorsement.
- Blackmail/extortion – You're told by a scammer they have your internet browsing history, compromising photos or videos. They demand payment in crypto.

Take-home message

If you're uncertain whether you're being scammed by an unsolicited contact, keep your powder dry and abstain from acting. Contact your advisors before acting.