Crypto investment scams and what you should know to stay safe

RBC Wealth Management

What you should know

Cryptocurrency investment scams, often known as "pig butchering," results in billions of dollars lost by consumers annually. Scammers form friendships with victims to lure them into making crypto investments via fake apps and websites. Initially, these investments seem to grow steadily with small amounts, but ultimately, the goal is to swindle victims out of tens of thousands to millions of dollars.

Types of cryptocurrency scams to watch

Fake cryptocurrency websites

Scammers create replica cryptocurrency websites, or slightly alter legitimate ones, to deceive victims into buying cryptocurrency. These fake sites often feature phony testimonials and trading records, leaving individuals unable to recover any funds once they make a payment.

Crypto phishing scams

Scammers use fake websites to engage in phishing, tricking individuals into revealing personal information, especially related to their cryptocurrency wallets. It's crucial to verify the authenticity of any site before entering sensitive data.

Fake celebrity endorsements

Scammers often use fake celebrity endorsements to promote fraudulent financial services, luring victims through social media with enticing offers that lead to downloading malicious apps, potentially granting access to personal funds.

Ponzi schemes

Ponzi schemes have adapted to the crypto landscape by enticing investors with seemingly legitimate cryptocurrency portfolios, using funds from new investors to pay earlier ones while pocketing the excess. Scammers often fake documents and account statements to maintain the illusion of success and attract more victims.

Cryptocurrency donations

Individuals and corporations can donate cryptocurrency to legitimate charities, but scammers often create fake websites that mimic these organizations to exploit people's charitable intentions and steal their money.

Rug pull scams

Pump-and-dump schemes involve fraudsters who artificially inflate the price of a cryptocurrency by promoting it, only to cash out and abandon the project, leaving investors with worthless coins.

Blackmail scams

Scammers may attempt to blackmail individuals by claiming to possess compromising images and asking for cryptocurrency payments to prevent them from sharing the material. In such cases, the FTC recommends ignoring the threats and reporting the incident to the FBI.

Business opportunity scams

Scammers frequently advertise fraudulent business opportunities, claiming they can yield substantial profits with little investment of money or time. They often create a sense of urgency to pressure victims into making payments.

Romance scams

Romance scams take advantage of individuals' emotions, particularly targeting the elderly. Scammers initiate fake romantic relationships online to gain trust and then manipulate victims into sending money for fabricated reasons.

The warning signs

- Unexpected contact online from someone you don't know
- A request not to consult with a financial institution or your financial advisor
- New companies or online friends promoting investment opportunities that you "can't miss"
- New companies or online friends pressuring you into making financial decisions and asking for money or fees

- Poor grammar on the website, low-quality images, broken links and multiple spelling errors
- Websites or social media accounts that closely resemble legitimate ones but differ by just a few words, aiming to trick people into investing in businesses they believe they have heard of or seen before.

How to protect yourself

- Purchase securities only from individuals who are registered and licensed to sell them.
- Communicate through legitimate company channels, never through social media or encrypted apps, as scammers can impersonate registered financial advisors to commit fraud.
- Don't send or transfer any funds until you've thoroughly verified the legitimacy of the seller.
- Be cautious of any online investment gurus who pressure you to "act quickly."
- Never send money to people you meet online and avoid making investments based solely on their advice.
- Do not download any software they may ask you to install on your computer.
- Be wary of anyone online offering investments with "guaranteed payouts."
- Even if these "online friends" arrange professional-looking video calls with multiple participants, they could all be in on it and it may still be a scheme.

How to report a cryptocurrency scam

If you discover that you have fallen victim to an online cryptocurrency scam, the first thing you should do is immediately stop sending money to the scammers. Next, contact your bank to inform them of the situation so they are aware. Make sure to collect all communications with the scammers. Finally, file a report with the **FBI Internet Crimes Complaint Center** at IC3.gov.

24-04-2872977_0442 (01/25)