ctpro.io

Crypto Investment Scams

Investment Scams

Investment fraud typically involves deceptive practices to induce investments based on false information, promising large returns with minimal risk. The widespread promotion of cryptocurrency as an investment, combined with the “fear of missing out,” has created opportunities for criminals to target consumers and retail investors, especially those unfamiliar with the technology and its risks.

Reported losses from cryptocurrency-related investment fraud to the IC3 increased by 53%, from $2.57 billion in 2022 to $3.96 billion in 2023. Many individuals have incurred significant debt to cover these losses. While those aged 30-39 and 40-49 filed the most complaints (around 5,200 each), individuals over 60 reported the highest losses, totaling over $1.24 billion.

Types of Investment Scams

US citizens and individuals abroad should be cautious of false job ads linked to labor trafficking. These scams, often targeting people in Asia, offer attractive salaries and benefits but change the job location. Upon arrival, passports may be confiscated, and threats or violence used. Workers start in debt due to travel expenses and must work to pay it off, while criminals use debt and fear of law enforcement to control them. Trafficked workers may be sold and transferred, increasing their debt.

Liquidity mining is a strategy to earn passive income with cryptocurrency by staking it in a pool and earning a share of trading fees. In a scam version, fraudsters target cryptocurrency owners, build a relationship, and promise daily returns of 1-3%. They convince targets to link their wallet to a fake liquidity mining app, then steal the funds without the owner's knowledge.

Criminals create fake play-to-earn gaming apps to steal cryptocurrency. They build online relationships with targets, who are directed to create a cryptocurrency wallet and buy cryptocurrency. As targets play the game, they see fake rewards. When they stop depositing funds, criminals drain the wallet using a malicious program. Even if additional fees are paid, targets cannot recover their money.

The FBI’S Virtual Assets Unit (VAU)

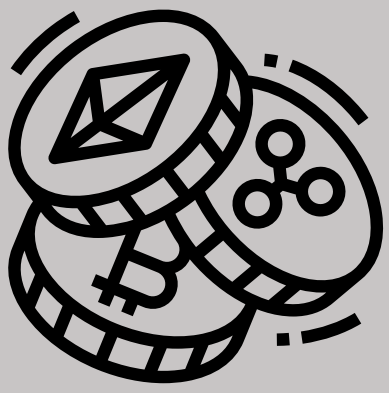
The FBI is a national security organization that focuses on both intelligence and law enforcement duties, addressing various threats. Utilizing its cyber and investigative expertise, the FBI plays a vital role in identifying, investigating, and prosecuting crimes involving virtual assets on a global scale. This is supported by its 63 Legal Attaché offices and 30 sub-offices in major cities worldwide, covering over 180 countries, territories, and islands.

To bolster these efforts, the FBI established the Virtual Assets Unit (VAU) in February 2022. This specialized team is dedicated to investigating cryptocurrency-related crimes, centralizing the FBI’s cryptocurrency expertise. The VAU provides advanced technological tools, blockchain analysis, virtual asset seizure training, and other specialized training for FBI personnel.

Cryptocurrency Recovery Schemes

Individuals who report losing money to cryptocurrency investment fraud are sometimes targeted again by fraudulent businesses claiming to recover lost funds. These businesses contact victims via social media, messaging platforms, or advertisements, promising to trace and recover cryptocurrency for an upfront fee. Often, they either stop communicating after receiving payment or provide inaccurate reports and request more money. They may falsely claim to be affiliated with law enforcement to appear legitimate.

It’s important to note that private recovery companies cannot issue legal orders to recover stolen cryptocurrency. Exchanges only freeze accounts based on internal processes or court orders. Victims may consider civil litigation to recover their funds.



Crypto Track Pro

Crypto Track PRO is a robust blockchain analytical engine designed to enhance investigative capabilities. As a private forensic firm, we collaborate with U.S. law enforcement as well as international investigators.

We also collaborate with international organizations such as the Cryptocurrency Defenders Alliance which provides us the ability to attempt to quickly blacklist cryptocurrency addresses linked to known criminal activity. This can provide law enforcement with the critical time needed to secure legal documentation and facilitate asset recovery for victims.

Sign up for a free 14-day trial at:
https://analytics.ctpro.io/login/