United States Secret Service
Cybercrime Investigations

Cryptocurrency Investment Scams

Digital Asset Technology Alliance (DATA) Guide

SAN FRANCISCO • CYBER FRAUD TASK FORCE •

The U.S. Secret Service continues to observe a significant increase in cryptocurrency and digital asset investment scams. These scams often target victims who use social media, online dating, or professional networking platforms.

PREVENT

- ✓ **Avoid unreasonably high returns on investment - is it too good to be true?**
- ✓ **Avoid cryptocurrency investment proposals with complex verbiage, such as pools, futures, mining, liquidity.**
- ✓ **Avoid sharing your personal information with unverified individuals. You can validate a broker by going to BrockerCheck by FINRA.**
- ✓ **Only download apps directly from legitimate App Stores (i.e., Apple App Store, Google Play Store).**
- ✓ **Beware of clicking on links, they can be malicious.**
- ✓ **Be wary of apps with excessive application permissions (i.e., administrator privileges).**
- ✓ **Beware of linking apps with external investment platforms, even legitimate apps may be linked to platforms that are not vetted.**
- ✓ **Never share your seed phrase - the string of words that can be used to access a cryptocurrency wallet on the blockchain.**
- ✓ **Avoid chat functions on external websites, instead contact support through a company's official website.**
- ✓ **Avoid external applications that end in .apk (Android) or .mobileconfig (iOS) as these are not screened and pose an immediate risk of compromising your device data through malicious software.**
- ✓ **Never mix someone you met online and investment advice.**

RESPOND

- ➢ **Don't pay more money (ransom) to release your funds.**
- ➢ **Keep records.**
  Take screen shots of conversations with the people involved in the scam.
  Save email addresses, phone numbers, applications, and other pertinent information.
- ➢ **Change login information to any financial accounts you provided to the people involved in the scam.**
- ➢ **Check for malicious software on your iOS device.**
  Go to Settings/General/VPN & Device Management and checking for any unauthorized device configuration.
- ➢ **Be cautious when seeking non-law enforcement assistance.**
  The information and assistance tracing lost assets may be incorrect and inadmissible in court, and may result in further loss.

REPORT

- ➢ **Report to your cryptocurrency exchange.**
  Provide transaction information (i.e., your wallet address, receiving wallet address, date and amount of transaction, type of cryptocurrency, domain (website) name or app name.
  Determine whether to close your account.
- ➢ **Contact credit reporting companies directly.**
  In some instances, if victims contact creditors (and in some cases collection agencies) immediately upon learning of a change in their ability to pay debts, the result may be a reduction, modification, or deferral of credit card or loan payments.
- ➢ **Report to law enforcement.**
  Contact your local police department and file a police report.
  File a complaint on the Internet Crime Complaint Center (IC3).
  Contact your local Secret Service field office.

IMPORTANT NUMBERS

Equifax Fraud Assistance Unit (800) 525-6285

Experian Consumer Fraud Assistance Unit (800) 682-7654

TransUnion Fraud Assistance Unit (800) 680-7289

National Foundation for Credit Counseling (800) 388-2227

National Suicide Prevention Lifeline Dial 988

U.S. Secret Service Victim and Witness Assistance Program