

CRYPTO INVESTMENT

SCAMS:

The Warning Signs



Unsolicited contact. Someone you don't know reaches out first about investing in crypto.

Legitimate investments are rarely initiated by strangers.



Confusion is a tactic. Crypto is complex—and scammers take advantage of that.

If an investment feels confusing or overwhelming, step back. Don't buy what you don't understand.



Encrypted apps. You are quickly asked to move the discussion of your investment onto an encrypted app like WhatsApp or Telegram.

Scammers push conversations to encrypted apps to avoid being traced. Real advisors usually communicate through official, verifiable channels, preferably in person.



Unfamiliar platforms. Scammers may push you to use obscure websites or apps with fake dashboards.

If you can't verify the platform independently, avoid it.



Guaranteed profits. You are promised quick, high returns with little risk.

All real investments carry some risk and grow gradually over time.



Romance + Crypto = Red Flag. Someone you've only met online asks you to invest in crypto, especially early in the relationship.

Trustworthy romantic partners will not ask you for money, especially before you have met in person and developed a trusting relationship.



No access to funds. You invest a small amount, but you are unable to withdraw the money or asked to pay more to “unlock” the funds.

Investment scammers may falsify documents to convince you to invest more and chase even higher returns. Do not invest additional money.



Too good to be true. Your investment feels unreal—guaranteed returns, VIP investor access, etc.

Trust your instincts. If your investment seems too good to be true, it probably is.

What to do if you suspect you have been scammed:

Stop all communication immediately. Do not respond to the scammer. Block them to prevent further manipulation.

Don't send money—even to “unlock” funds. Scammers often claim you need to pay additional fees or taxes to access your investment.

Document everything. Save messages, screenshots, email addresses, crypto wallet addresses, and any transaction records.

Protect your accounts. Change passwords, enable two-factor authentication, and monitor financial accounts for unusual activity.

Tell your bank or crypto exchange. If you shared financial information or transferred funds, contact your bank immediately. They may be able to freeze transactions or flag suspicious activity.

Report the scam. File a complaint with IC3.gov (FBI Internet Crime Complaint Center), the Federal Trade Commission (ReportFraud.ftc.gov), or the Securities and Exchange Commission (SEC).