

What to Do After a Crypto Scam

1. Cut Off Communication (Immediately)

- Do **not** respond to the scammer.
- Do **not** send more money (even if they threaten or beg)
- Screenshot messages with scammers in case they delete conversations.

2. Secure Your Devices & Accounts

- Disconnect from scam websites or apps immediately
- Run antivirus/malware scans on all devices used
- Change passwords:
 - Email (especially if it was used to sign up on exchanges)
 - Crypto exchanges and wallets
 - Banking apps and services
 - Any reused passwords

3. Document & Save All Evidence

- Take screenshots of:
 - All chats and communications
 - Wallet addresses used
 - Transaction history (TXIDs)

Go-Crypto

www.go-crypto.org

Educating. Analyzing. Protecting Digital Assets.

Developed by Go-Crypto, a nonprofit initiative focused on cryptocurrency fraud awareness and blockchain analysis.

- Scam websites, platforms, and login screens
- Create a timeline of events with dates, platforms, and dollar amounts
- Download PDFs or CSVs of account activity if possible

4. Notify Financial Institutions (Bank, Card, Payment Apps)

- Call your bank or credit card company to dispute unauthorized charges or transfers
- Request a chargeback or fraud review
- Freeze or close compromised accounts if needed

5. Report to Crypto Exchanges and Wallets

- Report the scam to platforms used to buy/send crypto (Coinbase, Binance, etc.)
- Provide TXIDs and any wallet address the funds were sent to
- Request review of associated accounts for potential monitoring or restriction, where applicable
- <https://support.google.com/mail/contact/abuse>
- <https://www.scamadviser.com/report-a-scam>

6. File a Police Report

- Visit or contact your local police or cybercrime unit
- Bring a copy of all evidence and the scammer's information
- Request a case number and get an officer's contact if possible

Go-Crypto

www.go-crypto.org

Educating. Analyzing. Protecting Digital Assets.

Developed by Go-Crypto, a nonprofit initiative focused on cryptocurrency fraud awareness and blockchain analysis.

7. Report to Federal Agencies

- FBI Internet Crime Complaint Center (IC3): <https://www.ic3.gov>
- Federal Trade Commission: <https://reportfraud.ftc.gov>
- U.S. Secret Service Cyber Fraud Task Force (via local field office):
<https://www.secretservice.gov/contact/field-offices>
 - Secret Service Phone Script
https://www.go-crypto.org/files/ugd/9f9825_6b06debc0e3c481493c1523935470111.pdf
- National Elder Fraud Hotline (age 60+ yrs.): 833-372-8311 10 am-6 pm ET
<https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope>

8. Protect Yourself Going Forward

- Enable 2FA (two-factor authentication) on all accounts
- Stay off investment forums or dating apps used in the scam
- Educate others in your network if they may have been targeted too

Need Help Understanding Your Situation?

Go-Crypto is a nonprofit initiative focused on:

- Educating individuals affected by cryptocurrency scams
- Analyzing blockchain transactions for clarity and awareness
- Supporting victims, attorneys, and law enforcement through structured, educational reporting

If you would like guidance or help understanding your situation, you can submit your information here:
<https://forms.gle/wk6zTKoMJ4VSUfrb7>

Go-Crypto

www.go-crypto.org

Educating. Analyzing. Protecting Digital Assets.

Developed by Go-Crypto, a nonprofit initiative focused on cryptocurrency fraud awareness and blockchain analysis.