BEGINNER DOWNLOAD 02

Crypto Scam Red-Flag Checklist

Use this page when an investment, payment, wallet request or recovery offer feels urgent, secret or unusually profitable.

PAUSE BEFORE ACTING

Stop the conversation. Do not send money, connect a wallet, sign a request or install software while another person is waiting or directing you.

Contact and pressure

[ ] The contact was unsolicited or began through an advertisement, wrong-number text, dating app or social platform.

[ ] The person claims to be a government agency, bank, exchange, employer, celebrity or trusted adviser.

[ ] I am being told to act immediately, keep the matter secret or avoid speaking with family or my bank.

[ ] Caller ID, official-looking documents, testimonials or video are being used as the main proof of legitimacy.

Investment and withdrawal

[ ] Returns are guaranteed, unusually consistent or described as low risk.

[ ] A stranger is coaching me to buy crypto and send it to a wallet or platform they selected.

[ ] A dashboard displays profits, but I cannot independently verify the assets or operator.

[ ] I must pay a tax, security deposit, insurance fee or account upgrade before withdrawing.

[ ] A small early withdrawal is being presented as proof that a larger deposit is safe.

Wallet and account access

[ ] Someone requests my recovery phrase, private key, password or authentication code.

[ ] I am asked to install remote-access software or share my screen.

[ ] A link asks me to connect a wallet to verify, cancel, claim, mint or unlock something.

[ ] The signature or approval is unclear, unlimited or unrelated to what I expected.

[ ] An unsolicited token, NFT or airdrop contains a link or instruction to visit a website.

ONE RED FLAG IS ENOUGH TO PAUSE

Several checked boxes indicate a strong likelihood of fraud. Verification must be independent of the person or website making the request.

VERIFY AND RESPOND

Stop. Separate. Search. Confirm. Consult.

The safest verification happens outside the conversation and outside links supplied by the person requesting money or access.

Five-minute verification routine

- [ ] STOP - I ended the call or conversation and did not transact under pressure.
- [ ] SEPARATE - I closed supplied links and opened the organization through a verified app, bookmark or independently found website.
- [ ] SEARCH - I checked registration records, regulator warnings and credible reports.
- [ ] CONFIRM - I contacted the real organization using independently verified details.
- [ ] CONSULT - I described the request to a trusted person who is not involved in the opportunity.

If fraud may have occurred

- [ ] Stop all payments and contact with the suspected fraudster.
- [ ] Preserve wallet addresses, transaction hashes, messages, emails, URLs, phone numbers and screenshots.
- [ ] From a clean device, protect affected email, exchange, banking and social accounts.
- [ ] If a recovery phrase or key was exposed, move remaining assets to a newly created secure wallet.
- [ ] If malicious token approvals were granted, revoke them using a trusted method.
- [ ] Notify the bank, exchange, custodian, payment provider or crypto ATM operator involved.
- [ ] Report promptly to local police and the appropriate national fraud-reporting service.
- [ ] Ignore anyone who guarantees recovery or requests another fee, key or wallet connection.

Official Canadian starting points

Report fraud and cybercrime	Canadian Anti-Fraud Centre reporting
Check investment registration	CSA: Are They Registered?
Review investor warnings	CSA Investor Alerts
Immediate danger	Contact emergency services and local police.

NEVER DISCLOSE No legitimate support representative, regulator, investigator or recovery professional needs your recovery phrase or private key.

INCIDENT RECORD

Preserve the Evidence

Complete this worksheet as soon as possible. Accurate transaction and contact information can assist platforms, financial institutions and investigators.

Incident details

Date and time	
How contact began	
Names / organizations used	
Website / phone / username	
Wallet addresses	
Transaction hashes	
Amount and asset	
Bank / exchange involved	
Reports filed	
Case / reference numbers	

Evidence to preserve

- [ ] Original emails, text messages, chat histories and voice messages.
- [ ] Screenshots of profiles, advertisements, websites and investment dashboards.
- [ ] Wallet addresses, transaction hashes, QR codes and blockchain-explorer records.
- [ ] Bank, exchange, crypto ATM, bridge and payment receipts.
- [ ] Names, usernames, telephone numbers, email addresses and domain names used.
- [ ] A written timeline of instructions, payments and attempted withdrawals.

Actions taken

- [ ] Affected accounts secured and passwords changed from a clean device.
- [ ] Bank, exchange, wallet provider or payment service notified.
- [ ] Local police and national fraud-reporting service contacted.
- [ ] Trusted contacts warned if an email or social account was compromised.

DO NOT ALTER THE EVIDENCE Keep original files and messages whenever possible. Do not continue communicating merely to collect more evidence or attempt your own recovery.