# Stolen cryptocurrency checklist

What to do if your cryptocurrency is stolen. Work down the list in order and tick each step as you finish it. The full guide, with the reasons behind every step, is at confirmedstolen.com/stolen-crypto/.

## In the first hour

- [ ] **Stop interacting with the suspected scammer, site or app**
  Do not send more funds, sign more transactions or reply to messages. Disconnect the wallet from any site you do not trust.
- [ ] **Switch to a device you trust**
  If your computer or phone may be infected or your recovery phrase was exposed, do the next steps from a different, up-to-date device.
- [ ] **Move remaining assets to a new wallet with a new recovery phrase**
  Create a fresh wallet on the clean device and transfer what is left. Do not reuse the old recovery phrase (the 12 or 24 backup words that control a wallet).
- [ ] **Revoke token approvals on the affected wallet**
  Use a token approval tool for the wallet's network to cancel permissions you granted to apps. Revoking costs a network fee; see this OpenSea help article (support.opensea.io/en/articles/8867133-how-can-i-revoke-token-approvals-and-permissions-on-ethereum).
- [ ] **Secure your exchange accounts through the official app or site**
  Change passwords, remove withdrawal addresses you did not add, and turn on authenticator-app or security-key MFA. Type the address yourself rather than using links.
- [ ] **Contact the exchange's official support if funds moved through it**
  Use only the support channel inside the exchange's app or website. Ask whether it can freeze or flag the receiving account and record your ticket number.

## Within 24 hours

- [ ] **Secure the email account linked to your crypto accounts**
  Change the password, review recovery options and forwarding rules, and sign out other sessions. Our hacked accounts guide (confirmedstolen.com/hacked-accounts/) covers each step.
- [ ] **Check for a SIM swap if your phone lost service**
  If your number stopped working before the theft, call your carrier from another phone. See our SIM swap guide (confirmedstolen.com/sim-swap/).
- [ ] **Record every transaction hash, address, date and amount**
  IC3 lists transaction hashes, cryptocurrency addresses, coin types, amounts, and dates and times as key details for a complaint. See IC3's cryptocurrency page (www.ic3.gov/CrimeInfo/Cryptocurrency).

- [ ] **Save screenshots, messages and website addresses**
  Capture chats, emails, profile names, phone numbers, URLs and any kiosk receipts before they are deleted. Store copies off the affected device.

- [ ] **Tell your bank if you bought the crypto with a card or transfer**
  Call the number on your card or statement. Crypto payments are typically not reversible, but the payment that funded them may be worth disputing.

## This week

- [ ] **File a complaint with the FBI IC3**
  Report the theft at ic3.gov (www.ic3.gov/) with your transaction details, even if the amount seems small, and keep the confirmation.

- [ ] **Report the fraud to the FTC**
  File at ReportFraud.ftc.gov (reportfraud.ftc.gov/). If the site is temporarily unavailable, check consumer.ftc.gov and try again later.

- [ ] **Report the receiving addresses to Chainabuse**
  Submit the scam addresses and URLs to Chainabuse (www.chainabuse.com/) so others can see the warning. It is a reporting tool, not a recovery service.

- [ ] **File a local police report**
  Ask for the report number. Exchanges, banks and tax preparers may ask for it, and some cases are referred between agencies.

- [ ] **Report identity theft if your personal data was taken**
  If you sent ID documents or your Social Security number, create a recovery plan at IdentityTheft.gov (www.identitytheft.gov/).

## Recovery

- [ ] **Ignore anyone who promises to recover your crypto for a fee**
  The FBI warns that recovery offers are a common follow-on scam. Law enforcement does not charge victims to investigate. See the FBI warning (www.ic3.gov/PSA/2023/PSA230811).

- [ ] **Ask a tax professional about the loss**
  Tax treatment of stolen or scammed digital assets depends on the facts. Keep your records and review the IRS digital assets page (www.irs.gov/filing/digital-assets).

## Prevent it happening again

- [ ] **Keep your recovery phrase offline and never share it**
  No legitimate exchange, wallet provider or agency needs your recovery phrase or private key. Anyone who asks for it is attempting theft.

- [ ] **Use authenticator-app or security-key MFA, not text messages**
  Protect exchange, email and password manager accounts with phishing-resistant MFA, and add a carrier account PIN.

- [ ] **Limit and review token approvals regularly**
  Set spending limits instead of unlimited approvals where your wallet allows it, and revoke approvals you no longer need.

## Your case record

Wallet addresses involved

Transaction hashes (TXIDs)

Exchange support ticket

IC3 complaint number

FTC report number

Notes

Version November 6, 2026. General information, not legal advice. Agencies change their procedures, so confirm each step with the organization named. Confirmed Stolen is an independent reference; it is not law enforcement and does not recover property. Free to print and share with attribution.