

Crypto Wallet Security Guide

For investors and large holders — 2026 edition

Crypto Safety Notes · crypto-safety-notes.pages.dev

Notice: Educational only. Not financial or investment advice. No profit promises. We will never ask for your seed phrase or for money.

1. Seed phrase storage

- Your 12/24 words *are* your money. Whoever has them owns the wallet.
- Write by hand on paper; better, stamp on fire/water-resistant metal.
- Never store it in photos, screenshots, cloud notes, email or WhatsApp.
- Keep two copies in separate secure locations (e.g. home safe + bank safe-deposit box).
- Consider an optional passphrase (25th word), stored separately.

2. Hardware wallets

- Buy only from the manufacturer or an authorised reseller, never second-hand.
- A device arriving with a pre-printed recovery phrase is a scam.
- Verify address and amount on the device screen before signing.
- Split funds: small hot wallet for daily use, cold storage for savings.

3. Multisig

- Requires several keys (e.g. 2-of-3) to move funds; one lost or stolen key is not enough.
- Spread keys across devices and places; a trusted person or custodian can hold one.
- Test with small amounts and back up the wallet configuration.

4. Inheritance planning

- If your family can't access your crypto, it may be lost forever.
- Write a letter of instruction (where assets are, how to recover) without the seed itself.
- Use multisig with an heir/lawyer, or split information so no single party has full access.
- Consult a local legal professional about your will; review yearly.

5. Address poisoning

Scammers send tiny or zero transfers from an address matching the first/last characters of one you use, hoping you'll copy it from history.

- Never copy addresses from transaction history; use a verified address book.
- Check the full address and send a small test first.

6. Fake advisors / WhatsApp & Telegram scams

- Unknown numbers, "expert" signal groups, new acquaintances pushing a "guaranteed" platform.
- Fake profits on a dashboard, then "fees" or "tax" before withdrawal — always a scam.
- No return is guaranteed. Never install remote-access apps or share your screen.
- Bank, government and exchange-support impersonation is common; contact official channels you find yourself.

7. OTC scams

- Large buy/sell offers above market price, or cash meetups, are classic traps.

Found this useful? ☺ Support: crypto-safety-notes.pages.dev/tip

- Never release assets before payment is truly settled; beware fake bank receipts.
- Use only licensed, reputable OTC desks; get a contract and verify identity.

8. Phishing

- Look-alike domains, sponsored ads, "account will be closed", "claim airdrop in 10 minutes".
- Read what you sign; unlimited approvals can drain tokens. Revoke old approvals.
- Real support never asks for your seed phrase.

Quick checklist

- ☐ Seed on paper/metal, two copies, nothing digital
- ☐ Hardware wallet from official source
- ☐ Multisig for large amounts
- ☐ Letter of instruction for heirs
- ☐ Address book + test transfer
- ☐ No WhatsApp "advisors", no guaranteed profits

If this guide helped, you can optionally support the project at crypto-safety-notes.pages.dev/tip.html — thank you. Our content stays free.