

How not to lose your crypto

A checklist: what never to do, how to protect yourself, and what to do if it has already happened.

Never do this

- 1 **Never tell anyone your recovery phrase (12–24 words) or private key.** No exchange, support team or police officer will ask for it. Whoever asks wants to steal.
- 2 **Never invest through someone you met online:** on a dating app, Telegram, WhatsApp or Facebook. That is how most scams start, even after months of chatting.
- 3 **Never believe guaranteed profit.** “2% a day”, “no risk”, “today only” always mean a scam.
- 4 **Never pay to withdraw your own money.** If a “fee”, “tax” or “insurance” is demanded before a payout, the money is already gone.
- 5 **Never install remote access apps** (AnyDesk, TeamViewer and the like) because someone asks you to.
- 6 **Never answer “support” that wrote to you first.** Real admins and exchange staff do not message first.
- 7 **A call from your “bank”, “exchange” or “the police”?** Hang up and call the official number yourself.
- 8 **Never approve anything in your wallet you do not understand.** One “Approve” or “Sign” on a fake site can empty the whole wallet.
- 9 **Check the whole recipient address, not only the start and end.** Do not copy addresses from your transaction history: scammers plant look-alike addresses there.
- 10 **Never trust “recovery” services** that guarantee your money back or want crypto up front. That is the second scam after the first.

How to protect yourself

- Type the exchange address yourself or open it from a bookmark. Fake sites appear in Google results and ads.
- Use an exchange licensed to operate in your country or region. Turn on two-step verification with an authenticator app, not SMS.
- Turn on the withdrawal address allowlist on your exchange, so money can only go to addresses you approved.
- Keep larger amounts on a hardware wallet bought only from the manufacturer.
- Now and then, check which sites your wallet has given permissions to and revoke the ones you do not need (for example with revoke.cash).

If it has already happened

- 1 **Do not pay anything more** and stop talking to the scammers.
- 2 **Save the evidence:** transaction IDs (TxID), addresses, amounts, times, and screenshots of the chats and the website.
- 3 **Report it at once** to your exchange and to the police. The first hours matter most: while the money is still on an exchange, it can be frozen.
- 4 **If you need to trace where the money went** and prepare evidence for the police and the exchange: trailforensics.com.

Trail Forensics never asks for recovery phrases, passwords or wallet access, and does not guarantee that money will be returned.