

Wallet Setup and the Seed You Can Restore

Crypto Guidance, a trade name of Crypto Boutique LLC | Free guide | Education only. Nothing here is investment, tax, or legal advice.

Why this guide exists

Most people who lose crypto they actually own do not lose it to a genius hacker. They lose it because the backup they wrote down years ago does not work, because they typed it into the wrong place, or because nobody else knew it existed. This guide is a slow, boring checklist for your first wallet. Boring is the goal.

You will finish with three things: a wallet you set up yourself, a paper backup you have personally proven works, and a short list of things you will never type into a website. Take your time. Nothing here needs to happen today.

Part 1: Pick the kind of wallet

A wallet does not hold coins. It holds the keys that let you move coins recorded on a blockchain. The seed phrase (usually 12 or 24 words) is the master copy of those keys. Whoever has the words has the money.

- Software wallet: an app on a phone or computer. Free, fast, good for small amounts and learning.
- Hardware wallet: a small device that keeps keys offline and asks you to confirm on its own screen. Better for amounts you would be upset to lose.
- Exchange account: not a wallet you control. The exchange holds the keys. That can be fine for some people, but it is a different kind of risk, and this guide is about wallets you hold yourself.

A reasonable path for many people is to learn on a software wallet with a small amount, then move to a hardware wallet before the amount matters.

Part 2: Buying and unboxing a hardware wallet

- Buy directly from the manufacturer's own website, typed by hand, or from the manufacturer's official store on a major retailer. Avoid secondhand and third-party marketplace sellers.
- When it arrives, the device should ask YOU to create a new seed. If a seed phrase card is already printed and filled in inside the box, stop. Do not use it. Contact the manufacturer.
- Install the companion app only from the manufacturer's site or your phone's official app store. Check the publisher name.
- Update the firmware through the official app before you put money on it.

Part 3: Writing the paper backup

When the wallet shows you your words, this is the most important ten minutes of the whole process.

- ☐ Use the backup card that came with the device, or plain paper and a pen. Not a pencil that smudges.
- ☐ Write each word clearly, numbered 1 through 12 or 1 through 24. Order matters.
- ☐ Check the spelling of each word against what the screen shows. Seed words come from a fixed list, so a misspelling can usually be spotted, but do not rely on that.
- ☐ Do not photograph the words. Do not type them into notes, email, a password manager, a cloud document, or a text to yourself.
- ☐ Do not say them out loud near a smart speaker or on a call.
- ☐ Store the paper somewhere dry and private. A fire safe or a sealed envelope in a place only you and one trusted person know about is common.
- ☐ If your wallet offers an optional passphrase (sometimes called the 25th word), understand that forgetting it means losing access. Beginners often skip it until they are comfortable.

Part 4: The restore test (do this before serious money)

A backup you have never restored from is a hope, not a backup. The restore test proves your paper works.

The safest version uses a spare device:

- ☐ Send a small test amount to your new wallet. An amount you would shrug off losing.
- ☐ Take a second device. This can be a second hardware wallet of the same or compatible brand, or a factory reset spare phone with the official wallet app.
- ☐ Choose "restore" or "recover existing wallet" on the spare device, never "create new."
- ☐ Enter your words from paper, on the device itself. Not on a website. Not in a browser.
- ☐ Check that the spare device shows the same receiving address and the same small balance.
- ☐ If it matches, your paper works. Wipe the spare device if you do not plan to keep it as a backup.
- ☐ If it does not match, stop. Do not add more money. Recheck the word order and spelling, or start over with a fresh wallet.

Some people instead wipe and restore the original device. That works too, but it is more stressful, because if the paper is wrong you just erased the only working copy. The spare device method avoids that.

Repeat the restore test once a year, or any time you move or rewrite your backup.

Part 5: What never to type into a website

Write this list on a sticky note if it helps.

- Your seed phrase. Ever. No legitimate company, support agent, airdrop, wallet "validation" page, or "sync" tool needs it. Crypto Guidance will never ask for it either.
- Your hardware wallet PIN. It is entered on the device only.
- Your optional passphrase.
- A private key exported from any wallet.
- Recovery codes for your exchange account, unless you are on the exchange's real site and you started the recovery yourself.

If a page asks for your seed words, the page is the problem. Close the tab. You have not done anything wrong by looking. You only lose funds if you type the words in.

Part 6: Who would find it

If something happened to you, could anyone you trust find out that this wallet exists? They do not need the words today. They need to know there is something to look for and where the instructions are. The free Holdings Book guide at cryptoguidance.org covers this in more detail. For now, a sealed note that says "I have a hardware wallet, the backup is in X, call Y for help" is better than nothing.

One page checklist

- ☐ Bought from the manufacturer directly
- ☐ Device generated a new seed for me
- ☐ Firmware updated through the official app
- ☐ Words written on paper, numbered, spelling checked
- ☐ No photos, no typing, no cloud
- ☐ Small test amount sent
- ☐ Restore test passed on a spare device
- ☐ Paper stored somewhere dry and private
- ☐ Someone I trust knows a wallet exists
- ☐ Calendar reminder set for next year's restore test

Questions about this guide: john@cryptoguidance.org. We will never ask for your seed phrase.