Self-custody checklist — Single-signature + passphrase

Printed from **bitcoinkeys.guide/checklist**. **Work down it in order.** The sequence is the point: your backup exists, and has restored a wallet in a real test, before any real money moves. Each step says what to do and why, and carries the address of the lesson behind it — this sheet is a map, and the site is the detail.

> **This sheet is for single-signature + passphrase**, and every other setup on the ladder has its own — print the one that matches yours. It lists **every step this setup can need** (22 of them); the version on the site trims it further once it knows which hardware you own and whether anyone else may one day have to recover your coins.

STEP 1 Get set up

The moves that get your Bitcoin out of someone else's hands and into your own.

- [ ] **Get a hardware wallet**
  A device from our cold-storage tier — Bitcoin-only firmware available, its own screen, offline signing. Buy direct from the maker and check the tamper seal.
  `Rule 05 · Buy it new and direct · bitcoinkeys.guide/wallets`

- [ ] **Install the maker's wallet app**
  Your hardware wallet pairs with an app on your computer or phone — that's where you'll see balances and prepare the payments the device signs. Get it from the maker's official site only, typed by hand, never from a search result or an ad: fake copies of these apps exist, and they are built to steal.
  `bitcoinkeys.guide/learn/phishing-and-scams`

- [ ] **Generate a fresh seed — and add your own randomness**
  Power the device on and follow the maker's official start page — the address printed in the box or on their site, not a link someone sent you. Set a PIN when it asks, then let the device create the seed in front of you: it shows the words on its own screen, and you copy them down by hand. Never use pre-set words, and never type the words into a computer or phone. Where your device allows it, add your own dice throws to the randomness it generates — it takes a few minutes, it cannot make the result worse, and it removes the one part of your setup you otherwise have to take on trust.
  `Rule 05 · Buy it new and direct · bitcoinkeys.guide/learn/generate-your-seed`

- [ ] **Roll your passphrase — don't invent one**
  The secret "25th word" that opens your real wallet; the seed alone opens a decoy. It can't be reset, nothing rate-limits a guess, and there is no "wrong passphrase" error — mistype it and a different, empty, perfectly valid wallet opens instead. So don't think one up: roll it off the same word table you used for the seed. Six words is the floor, eight if this is protecting savings. Plain ASCII, no space at either end, and capitals count.
  `bitcoinkeys.guide/learn/ladder#rung-2`

- [ ] **Set a PIN on the device**
  The PIN stops someone who physically grabs the device from using it. It does NOT protect the seed — anyone holding your recovery words needs no PIN at all, which is why the backup is the thing that must never be seen. Set one anyway; it is free and it closes the easiest theft there is.
  `bitcoinkeys.guide/learn/ladder`

- [ ] **Verify every address on the device's own screen**
  The device's screen is the one display malware can't rewrite — your computer will show a swapped address without blinking. Read the address on the device, confirm it, then approve — every single time.
  `Rule 08 · Verify on the hardware wallet · bitcoinkeys.guide/learn/send-bitcoin-safely`

- [ ] **Send a small test amount to your new wallet**
  Move a little off the exchange — enough to prove the route works, small enough that a mistake costs nothing. Verify the receive address on the device's own screen first, then confirm it arrives. The rest of your Bitcoin stays put until your backup is proven.
  `Rule 02 · Not your keys, not your coins · bitcoinkeys.guide/learn/send-bitcoin-safely`

STEP 2 Secure the backup

The backup IS the wallet. This is the part people get wrong, and it's the part that loses coins.

- [ ] **Write the seed on paper, check it, then move it to metal**

  Copy the words by hand and check them against the device. Paper is fine for today; get it onto metal before the wallet holds anything you would miss, and keep each copy in a genuinely separate place. No photos, no cloud, ever.

  `Rule 06 · Never digital · bitcoinkeys.guide/metal-backups`

- [ ] **Back up the passphrase — separately from the seed**

  The single most documented way people lose passphrase-protected Bitcoin: they memorise it, never write it down, then forget it or die. The seed is backed up so the wallet LOOKS recoverable — it isn't. Back up the passphrase as carefully as the seed, in a different place.

  `bitcoinkeys.guide/learn/ladder#rung-2`

STEP 3 Prove it works

A backup you haven't tested is a hope. Do this before you move real money.

- [ ] **Prove recovery works before funding**

  Wipe the device and restore from your backup with a tiny amount. A backup you haven't tested is a hope.

  `Rule 07 · Test before you fund · bitcoinkeys.guide/learn/test-your-backup`

- [ ] **Restore with the passphrase, not just the seed**

  Restoring the seed alone lands you in the decoy wallet — and everything will look fine. Confirm the passphrase restores the wallet that actually holds your coins.

  `bitcoinkeys.guide/demos/passphrase`

- [ ] **Move the rest — now that the backup is proven**

  Your backup exists, lives in more than one place, and has restored the wallet in a real test. Now the rest of your Bitcoin can follow the test amount. Verify the receive address on the device's screen each time, and move it in a couple of pieces rather than one blind step.

  `Rule 02 · Not your keys, not your coins · bitcoinkeys.guide/learn/send-bitcoin-safely`

STEP 4 Live with it

Once your coins are cold, close the everyday gaps — and leave a plan someone else could follow.

- [ ] **Learn the daily-safety habits**

  Treat every unexpected message, call, or "support" contact as a trap until proven otherwise. Nobody legitimate ever needs your seed words — the demand itself is the proof.

  `Rule 09 · Requiring your words = theft · bitcoinkeys.guide/learn/phishing-and-scams`

- [ ] **Keep a low physical profile**

  Don't advertise that you hold Bitcoin. Keep amounts vague, skip the branded gear, and reduce where your name is tied to it.

  `Rule 10 · Talk about Bitcoin, not yours · bitcoinkeys.guide/learn/privacy`

- [ ] **Address your privacy**

  Use a fresh address every time, be careful about combining coins, and reduce KYC exposure (the ID checks exchanges make you pass, which tie your name to your coins).

  `Rule 11 · A fresh address every time · bitcoinkeys.guide/learn/privacy`

- [ ] **Write a recovery kit and inheritance plan**

  A plain-language document your future self and your heirs can follow — without ever writing the seed words in it.

  `Rule 12 · Leave a plan they can follow · bitcoinkeys.guide/learn/recovery-kit`

- [ ] **Make sure the right person knows the kit exists**

  A perfect recovery kit nobody knows about is no plan at all. They don't need the seed or the passphrase — only to know the kit exists and where to find it.

  `bitcoinkeys.guide/learn/recovery-kit`

EVERY YEAR Keep it alive

A setup is a practice, not a one-time event. Once a year, in one sitting:

- [ ] **Re-test a backup**
  Do a quick signed-message check (a built-in test that proves your keys still work, without moving any money), or a full wipe-and-restore if something has changed.
  `Rule 07 · Test before you fund · bitcoinkeys.guide/learn/test-your-backup`

- [ ] **Update device firmware**
  Apply the maker's security updates from their official app only.

- [ ] **Review your recovery kit and heirs**
  Are the instructions still accurate? Do the right people still know where to look?
  `bitcoinkeys.guide/learn/recovery-kit`

- [ ] **Confirm your backup locations**
  Has anything moved, flooded, or changed hands? Fix it while you remember.
  `bitcoinkeys.guide/learn/back-up-your-seed`

- [ ] **Reconsider your rung**
  If your holdings have grown a lot, re-check whether it's time to move up the ladder.
  `bitcoinkeys.guide/learn/ladder`

---

bitcoinkeys.guide/checklist — the full course behind every step, and a version of this list that adapts to your own plan. Independent: we sell nothing and take no affiliate money. No analytics, no trackers, no cookies. **Never write your seed words on this sheet**, or anywhere that is not your permanent backup.