

Home setup checklist

Work through this at home. Check boxes as you finish each step. Leave secrets off this page — no words, no xpubs, no txids. The biggest threat is a single point of failure.

Prepare at home

- ☐ A room you can close. Phones and cameras out of the room while words or plates are visible.
- ☐ A computer that can boot from USB. This becomes the online watch-only machine later — never type a seed on it.
- ☐ Two dedicated USB sticks: one for Tails only, one clean data stick for verified files and PSBTs.
- ☐ 5 casino d6 + cup. Pen. Printed 02_Print_Packet.pdf and 10_Recovery.xlsx.
- ☐ Verified copies of: Tails ISO, Sparrow Linux .tar.gz, Electrum, local Ian Coleman BIP39 HTML.
- ☐ Three titanium plates, letter stamps, steel block, eye protection. A second pair of eyes if you have one.
- ☐ Optional later: hardware signers from more than one vendor. Do not buy three of the same device.

Do the setup

- ☐ Tails ISO, Sparrow, Electrum, and Ian Coleman verified (hash + signature) before any USB is used offline.
- ☐ Tails flashed. Welcome screen: Networking Disabled every boot.
- ☐ Seed 1 from dice, converted offline, 24 words match in two tools, first addresses match.
- ☐ Seed 2 generated independently. Same checks. Seed 3 generated independently. Same checks.
- ☐ 2-of-3 P2WSH wallet built. Path m/48'/0'/0'/2'. Descriptor exported.
- ☐ Watch-only online Sparrow shows the same receive addresses. Dust received. Confirmed in two explorers.
- ☐ Dust spent at home: unsigned PSBT → Tails Seed 1 → full shutdown → Tails Seed 2 → broadcast.
- ☐ Three plates stamped and read back. At least one seed restored from the plate, not from paper.
- ☐ Paper bits and paper seeds destroyed only after plate checks pass.
- ☐ Optional: export a finished seed onto a trusted hardware wallet for signing. If you export more than one key, use different vendors.
- ☐ Plates leave for three different locations. Descriptor packet with at most one seed. 10_Recovery.xlsx updated (locations only).

House rules

- A key generated with sufficient entropy in an airgapped environment is the foundation of self-custody.
- No photos of seeds, plates, or screens that show words.
- No seed on a networked machine. No two seeds in one Tails session.
- If verification fails, stop. Do not continue “just this once.”
- If Tails networking was on with a seed loaded, that session is burned.
- Savings move only after dust receive and dust spend both succeed.
- Never let one vendor, one device, one tool, or one address hold a quorum.