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.

Airgapping at home with Tails

A computer that has never seen your seed while a network interface was live. You can build that on a kitchen table. That airgapped birth of the key is the foundation of self-custody.

Airgap does mean

- Networking disabled on the Tails welcome screen, before the desktop appears.
- The seed exists in RAM only. Shutdown wipes it.
- Data crosses the gap as files on a clean USB (PSBT, descriptor, verified binaries).
- The household computer stays watch-only: xpubs and the descriptor, never seeds.

Airgap does not mean

- “I turned Wi-Fi off after Sparrow opened.”
- The family laptop’s installed disk, even if you unplug Ethernet.
- Photographing a seed “just to be safe.”
- A password manager, printer, or cloud note as backup.

Prepare Tails on a trusted online computer

01 Download the Tails ISO only from the official Tails site. Fetch the signing key from more than one published source.

02 Verify the ISO signature and checksum before you flash. If verification fails, stop.

03 Flash Tails to its own USB with the official installer. Label it TAILS. Never mix it with the data USB.

04 On a separate clean USB, copy only already-verified files: Sparrow .tar.gz, optional Electrum, local Ian Coleman HTML.

Every offline session at home

01 Insert Tails. Boot. Set Networking to Disabled. Start Tails.

02 Plug in the data USB. Copy only what you need onto the live session.

03 Convert entropy, restore one seed, sign one PSBT, or export the descriptor.

04 Copy results back to the data USB. Shut Tails down fully. Wait for the screen to go dark before unplugging.

05 Never load two seeds in one session. Never turn networking on while a seed is in memory.

Two-machine rule at home. Online computer: watch-only Sparrow, builds the spend, broadcasts. Offline Tails: loads exactly one seed, signs, exports the PSBT, shuts down. The only secret that crosses a USB is a signature file — not a seed. A networked machine with a seed loaded is a single point of failure. Treat that session as burned.

Verify with more than one tool

Download official releases at home, check them, then take only verified files across the airgap. One program can lie. Two independent implementations should not agree by accident.

Get files from the official project — not a search-ad look-alike

Tails (official Tails site) · Sparrow Wallet (official Sparrow site) · Electrum (official Electrum site) · Ian Coleman BIP39 (official GitHub repo, saved as local HTML). Bookmark those yourself. Do not follow a random video's shortened link.

A. Verify every download

- [ ] **Tails ISO** — signing key from more than one source; ISO signature and checksum both pass.
- [ ] **Sparrow** .tar.gz — published SHA-256 matches; GPG or minisign signature verifies.
- [ ] **Electrum** — official release, published hash, signature. Second wallet, not the only wallet.
- [ ] **Ian Coleman BIP39** — official repo, hash-checked, opened only as a local HTML file while offline.
- [ ] **Any converter script** — read it. Confirm the dice-to-bits mapping and the published BIP39 wordlist.

B–D. Cross-check keys, wallet, and every spend

- [ ] Dice bits → same 24 words in the converter and in offline Ian Coleman.
- [ ] Same seed + path in Sparrow and Electrum → same first receive addresses.
- [ ] Output descriptor reconstructs the same addresses when imported in the second tool. Path m/48'/0'/0'/2', P2WSH, 2-of-3.
- [ ] Watch-only online Sparrow matches the offline receive addresses. Dust in, two explorers agree.
- [ ] Unsigned PSBT: both tools show the same destination, amount, change, and fee before you sign.
- [ ] After signature 1, session 2 sees it as valid. After signature 2, online Sparrow reports fully signed and unchanged.

The rule of two at home. Two downloads (hash + signature). Two wallets (Sparrow + Electrum). Two humans if someone you trust can read a plate against a screen. Two rehearsals — dust in, dust out — before savings move.

Generate Bitcoin entropy with dice

Unbiased 5 × d6 · 256-bit BIP39 seed · Done offline at home · No hardware wallet required

A d6 has six faces. Treating all six as bits biases the result. Keep only faces 1–4 (exactly two fair bits). Discard 5 and 6 and shake those dice again.

Face	1	2	3	4	5	6
Bits	00	01	10	11	—	—
Action	KEEP	KEEP	KEEP	KEEP	REROLL	REROLL

How to roll, convert, and verify offline

01 Shake five dice. Read left to right every time. Keep 1–4 as two bits. Skip 5 and 6.

02 Append only 0s and 1s. Example: 4, 6, 1, 3, 2 → 11 00 10 01 → **11001001**.

03 Aim for 320–400 bits (~50–60 shakes), minimum 256. Extra bits are hashed down to 256.

04 Boot Tails with networking disabled. Convert with a verified script or local Ian Coleman HTML.

05 Write all 24 words. Word 24 is the checksum — do not invent it.

06 Restore in Electrum and Sparrow while still offline. First addresses must match.

07 Repeat independently for Seed 2 and Seed 3. Shut Tails down. Destroy the raw bit notes.

Safety. Generate and convert only offline. Never type a real seed on a computer that is online. Casino dice and a consistent reading order reduce bias and recording mistakes.

Dice recording sheet

Read left to right. Write only 00 / 01 / 10 / 11. Leave a cell blank if that die was 5 or 6. Print extra copies — each seed needs ~50–60 shakes.

Seed # 1 2 3 **Date** _____ **Reader** _____ **Checker** _____

#	Die 1	Die 2	Die 3	Die 4	Die 5	Bits this shake
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						

Running bit count (filled pairs × 2): _____ Target ≥ 256, better 320–400. Do not photograph this sheet. Destroy it after the 24 words are stamped and verified.

Sparrow Wallet on Tails at home

Offline signing on your Tails USB. Networking stays disabled the entire session.

Before you begin: a verified Sparrow Linux standalone archive (sparrowwallet-*.tar.gz) must already sit on the clean data USB. Verify SHA-256 and the GPG / minisign signature on the online computer first. Do not download Sparrow from inside Tails.

Launch Sparrow offline

01 **Boot Tails offline.** Networking to Disabled. Start Tails.

02 **Copy the archive** from the data USB to the Desktop.

03 **Extract.** Terminal: cd ~/Desktop then tar -xvf sparrowwallet-*.tar.gz then ls

04 **Launch.** cd Sparrow then ./bin/Sparrow — wait 15–30 seconds.

Sign in the airgap session

01 Import the 2-of-3 wallet from the output descriptor, or restore **one** software keystore from one seed.

02 File → Open Transaction → From File → select the .psbt.

03 Read destination, amount, change, and fee against your written notes. Then Sign.

04 Export with a new filename such as tx-partial-s1.psbt. Close Sparrow. Shut Tails down fully.

Safety at home

- Keep networking disabled. If it is on, shut down and treat the session as burned.
- Load only one seed at a time. Seed 3 stays boxed unless Seed 1 or 2 is gone.
- Full shutdown before you carry the data USB back to the online computer.
- Test the whole path with a small amount before savings touch this wallet.

Sign and broadcast at home

Default path: two offline Tails sessions. Optional path after the key exists: sign on hardware wallets you imported the airgapped seed into. Either way, one seed per session, and two independent makers if hardware is in the quorum.

Step 1 — Build the spend (online watch-only)

01 Open watch-only Sparrow. Recheck the receive history so you know this is the right wallet.

02 Send tab: destination, amount, fee. Read every field against a written note.

03 Finalize for signing. Export tx-unsigned.psbt to the data USB.

Step 2 — First signature (Tails session 1, or hardware A)

01 Boot Tails, networking disabled. Launch verified Sparrow. Or unlock hardware wallet A that already holds Seed 1.

02 Restore Seed 1 only (Tails) — or confirm Seed 1 is the only key on that device. Open tx-unsigned.psbt. Confirm fields. Sign.

03 Export tx-partial-s1.psbt. Full shutdown of Tails, or unplug the hardware signer.

Step 3 — Second signature (Tails session 2, or hardware B)

01 Fresh Tails boot, networking disabled. Restore Seed 2 only. Or unlock hardware wallet B from a different vendor.

02 Open tx-partial-s1.psbt. Confirm the first signature and unchanged spend. Sign.

03 Export tx-signed.psbt. Full shutdown.

Step 4 — Broadcast (online computer)

01 Watch-only Sparrow: File → Open Transaction → fully signed file.

02 Confirm fully signed and fields unchanged. Broadcast. Record the txid in 10_Recovery.xlsx.

If you export a key onto hardware

- Generate the seed on airgapped Tails first. Import the finished 24 words. Do not let the device roll its own entropy for this stack.
- Multi-vendor examples (not a ranking): Foundation Passport, Blockstream Jade, BitBox02, SeedSigner / Krux. Official shops only.
- Two keys on two brands. Never three of the same box. A bricked vendor is one lost key — plates and geography still hold the wallet.
- If Sparrow and Electrum disagree about the PSBT, stop. Do not sign. Test with a small amount first.

Titanium plates and geographic split

Paper fails in the ways houses fail. Stamp each seed once at home, verify the stamp, then separate the plates so no single address holds a quorum. Geography is how you retire the last single point of failure.

Why metal

Paper / notebook	Ink runs. Fire wins. Do not stop here.
Steel plates	Survive most house fires and flooding. Watch cheap stamps.
Titanium stamp plates	Higher melt point, no rust, compact. Recommended default.
Digital copies	Photos, clouds, printers, password managers — treat as a leak.

How to stamp at home

01 Private room. No phones. Plate on a steel block. Stamp each letter deep.

02 Number words 1–24. Quiet label such as S1 — not your name, not “Bitcoin.”

03 Read the plate back against the paper seed. A mis-stamped word is a bricked backup.

04 Restore from the plate on offline Tails and confirm first addresses.

05 Destroy paper only after the plate-restore check passes.

What goes on each plate

Plate A

Seed 1 only

Home safe / fire box

Never Seed 2 or 3 here

Plate B

Seed 2 only

Off-site #1

Same address as A or C

Plate C

Seed 3 only

Off-site #2

Same address as A or B

Print the output descriptor and keep 10_Recovery.xlsx. Store that packet with Plate A and a copy at one off-site — never beside all three seeds. Hardware wallets do not replace these plates. Once a year at home: restore from plates, receive dust, spend dust, update locations. Write a letter that points to this packet and which two locations are needed — not the words.