It is critical that each key is made on a computer that is offline. Tails OS is installed on one of the two USB drives. It can be booted on any computer, and it is designed to forget the session when the machine shuts down. When Tails is booted, networking is set to Disabled. This is the offline computer. The other USB drive carries only files that have already been checked. The household computer is used first, on the network, and it never holds a seed. It is shut down fully before Tails is booted.

Airgap does mean

- Networking is set to Disabled on the Tails welcome screen, before the desktop appears.
- The seed exists in memory only. Shutdown wipes it.
- Files cross on a clean USB. Those files are the payment file, the wallet map, and the checked programs.
- The household computer stays watch-only. It holds the map, and it never holds a seed.
- A stronger setup removes the Wi-Fi card. Ethernet is never plugged. Tails is still used.

Airgap does not mean

- Networking turned off after Sparrow has already opened.
- Unplugging the cable on a disk that was online yesterday.
- Photographing a seed.
- A password manager, a printer, or a cloud note used as the backup.

Prepare Tails on a trusted online computer

01. The Tails file is downloaded only from the official Tails site. The signing key is fetched from more than one published source.

02. The signature and the checksum are checked before the drive is written. If the check fails, the work stops.

03. Tails is written to its own USB with the official installer. The drive is labeled TAILS. It is not mixed with the data USB.

04. Persistent Storage is not created. The passphrase is skipped. The drive stays amnesic.

05. The data USB receives only files that have already passed. The Sparrow file has to be named sparrowwallet-2.5.5-x86_64.tar.gz. That is the Linux file. The Windows installer and the Mac installer do not go on this drive. The drive is labeled DATA.

Every offline session at home

01. The Tails drive is inserted and the computer is booted. Networking is set to Disabled. Persistent Storage is not unlocked. Tails is started.

02. The data USB is plugged in. Only the file needed for that session is copied onto the live session.

03. The session converts the dice, restores one seed, signs one payment file, or exports the wallet map.

04. The result is copied back to the data USB. Tails is shut down fully. The screen goes dark before the drive is unplugged.

05. Two seeds are never loaded in one session. Networking is never turned on while a seed is in memory.

Do not use Persistent Storage

- Tails will offer an encrypted area on the same USB. It is not created, and an existing one is not unlocked.
- It is not hidden. Anyone holding the USB can see that it exists, and the passphrase can be forced or tricked out.
- The Electrum feature writes the wallet onto the stick. That file contains the seed, protected only by the wallet password. That is a spending convenience, not this setup.
- Extra software and saved settings can undo choices Tails already tested.
- It stays off. The seed stays in memory. Shutdown wipes the session. That is why this USB exists.

Stronger chassis, optional

- An old laptop can be the dedicated Tails machine. The Wi-Fi card is pulled. Bluetooth usually leaves with it. Leaving the

card in the slot and marking it disabled is not the same thing.

- Ethernet is often still on the board. It is never plugged. It is disabled in the BIOS when that option exists.
- The previous owner’s disk is ignored or removed. Tails does not use it. That operating system is not booted.
- The Tails file is still checked. Networking is still set to Disabled. A clean data USB is still used.

One computer is used twice. The first boot watches the wallet and broadcasts a finished payment. It never holds a seed, and it is shut down fully. The second boot is the Tails USB on that same computer, with networking off. It loads exactly one seed, signs, copies the payment file out, and shuts down. The only secret that crosses is a signature file, not a seed. A networked machine with a seed loaded is a single point of failure. That session is treated as burned.

Next. The three keys are made next. A word is not written until Tails is running with networking turned off.