

Wallet Security & Self-Custody Checklist

A one-page reference for new hardware-wallet users

- | | |
|-----------------------------------|---|
| Seed Phrase Storage: | Generate the recovery phrase on-device never on a phone app or pre-printed card. Record it to a durable physical medium: paper or a metal seed-phrase plate. Store in at least two physically separate, secure locations. Never digitize: no photos, no cloud notes, no password managers. |
| Two-Factor Authentication: | Enable 2FA on every exchange / custodial account that holds part of your stack. Prefer an authenticator app or hardware key over SMS where possible. Store backup codes in the same offline medium as your seed phrase. |
| Hardware Wallet Use: | Buy the hardware wallet directly from the manufacturer never a 3rd-party marketplace. Verify the device firmware with the manufacturer before transferring funds. Send a small test transaction before moving meaningful amounts. Keep firmware up to date; never install unofficial firmware. |
| Recovery Plan: | Practice a full recovery from the seed phrase on a second device where supported. Document the location of each backup and who in your household knows the plan. Re-test the recovery flow annually, or after any major firmware update. Review beneficiary / estate instructions so a trusted contact can recover if needed. |

Print this page. Tape it inside the safe-deposit box. Treat every unchecked line below as work to do before you move meaningful funds to self-custody. For the broader context on why self-custody matters and how the November 2026 ISO 20022 migration reshapes payment rails, read the Sentinel explainer.