

Don't Keep the Backup in the Hardware Wallet Box

October 17, 2026 · Document #354 · bip39-pharse.com

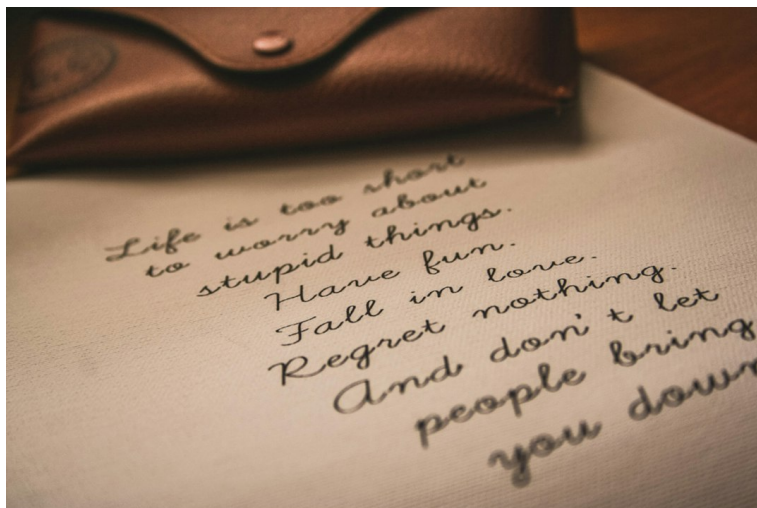


Photo by Alexander Naglestad on Unsplash

Storing your recovery seed inside the original hardware wallet box creates a single point of failure that compromises theft and disaster resilience.

Contents

The Failure of Combined Storage	2
Threat Modeling: Physical Theft and Environmental Hazards	2
Storage Location Comparison	2
Strategies for Physical and Geographic Separation	3
FAQ	3
Sources	3
Example BIP39 word sequences	4
Reading a BIP39 phrase	4
See also	5

Hardware wallet manufacturers package devices with USB cables, user guides, and blank cardboard recovery sheets for recording 12-, 18-, or 24-word BIP-39 mnemonics. Placing the completed recovery card back into the original box alongside the device, accessories, or recorded PIN numbers creates a single point of failure. Doing so invalidates the core security model of hardware wallets.

The Failure of Combined Storage

A hardware wallet acts as a physical secure boundary. Its internal secure element or microchip architecture protects your private keys against malicious software, unauthorized extraction, and physical tampering. In contrast, the paper or cardboard recovery card has zero defensive controls. It contains the raw BIP-39 mnemonic in human-readable plain text.

When you store the recovery card inside the original device packaging along with the physical wallet, an adversary does not need to bypass the device's secure microchip or guess its access PIN. They bypass the hardware security entirely by reading the mnemonic card. Storing these components together collapses two distinct security tiers into the security tier of the weakest element: an unsecured piece of paper.

Furthermore, users frequently store other sensitive records inside the box, such as device setup passwords, passphrase hints, or the device unlock PIN written on quick-start leaflets. Anyone who gains access to the container gains immediate and unencumbered control of the cryptographic assets.

Threat Modeling: Physical Theft and Environmental Hazards

Retaining the complete setup in one retail box increases vulnerability across multiple attack vectors:

- **Targeted and Opportunistic Burglary:** Retail packaging carries distinct brand logos, iconography, and labels that advertise crypto asset custody. Burglars look for identifiable consumer electronics boxes in desks, safes, and wardrobes. Grabbing the box yields both the signing device and its master secret.
- **Residential Fires:** Cellulose paper degrades and combusts at approximately 233°C (451°F), while typical residential fires reach 600°C to 800°C. Standard hardware wallet packaging offers no thermal protection. Storing the device and paper together ensures that a localized house fire destroys both the primary signing tool and its sole recovery mechanism simultaneously.
- **Water Damage and Mold:** Standard retail packaging is not hermetically sealed. Flooding, burst pipes, or high ambient humidity rot paper cards and corrode internal circuitry simultaneously.
- **Accidental Disposal:** Family members or house cleaners unfamiliar with cryptographic key backups may mistake the manufacturer packaging for an empty electronics box and discard it.

Storage Location Comparison

Storage Method	Physical Theft Risk	Fire/Water Destruction Risk	Setup Complexity
Original Box (Device + Sheet)	Critical	Critical	Minimal
Separated Paper Backup	Moderate	High	Low
Stainless Steel Backup (Offsite)	Low	Low	Moderate
Shamir Secret Sharing (SLIP-0039)	Very Low	Low	High

Strategies for Physical and Geographic Separation

To preserve the fault tolerance of BIP-39 hierarchical deterministic wallets, you must separate the physical device from its backups across independent locations.

- 1 **Separate Device and Backup Locally:** Keep the operational hardware wallet in a functional, easily accessible location protected by a robust PIN (minimum 6 digits, avoiding patterns). Store the initial paper or metal backup card in an entirely separate, concealed, fire-rated container or safe.
- 2 **Upgrade to Stainless Steel Backups:** Replace paper recovery cards with 304 or 316 grade stainless steel plates. Steel maintains legible character indentations well past 1200°C, resisting house fires and structural collapse, while eliminating water degradation.
- 3 **Establish an Offsite Redundancy:** Secure a secondary backup at an independent geographic location, such as a secure safety deposit box or an encrypted offsite vault. Ensure the offsite storage does not contain hardware or notes indicating the wallet address or owner identity.
- 4 **Discard or Repurpose the Retail Box:** Once initialization and verification are complete, recycle or repurpose the manufacturer box. Storing a hardware wallet in plain sight inside unmarked domestic containers (like a generic toolkit or utility pouch) provides better passive defense through obscurity than high-profile retail packaging.
- 5 **Apply BIP-39 Passphrases (13th or 25th Word):** Introduce an optional BIP-39 passphrase stored separately from both the hardware wallet and the seed phrase. Even if an attacker uncovers the seed phrase, they cannot compute master private keys without the passphrase.

FAQ

Can I keep the empty packaging for warranty or resale?

You can keep the original packaging, provided it contains only standard cables, stickers, and blank documentation. Never store recovery cards, handwritten notes, or PINs inside it.

What happens if I lose the hardware wallet but keep the backup?

Your crypto assets remain safe on the blockchain. You can purchase a replacement device from any vendor adhering to BIP-39/BIP-44 standards and import your mnemonic phrase to restore full access.

Is writing my device PIN on the recovery card acceptable?

No. Writing down your device PIN on the recovery card gives an attacker everything required to access your funds if they discover the hardware wallet and backup card together.

Sources

- [BIP-0039: Mnemonic code for generating deterministic keys \(github.com\)](#)
- [BIP-0032: Hierarchical Deterministic Wallets \(github.com\)](#)

Continue reading on bip39-phrase.com: [Cold Sharding Method: Ultimate Private Key Security](#)
More on this topic: [Seed Phrases](#)

Example BIP39 word sequences

Randomly generated sequences of words from the BIP39 English wordlist. None of them passes the BIP39 checksum, so no wallet will accept them: they show the format only. Never store funds with a phrase you found in a document.

Example 1

1	toe	2	pretty	3	naive	4	extend	5	dizzy	6	slab
7	risk	8	patient	9	engine	10	cover	11	arena	12	exile

Example 2

1	mixture	2	pulp	3	canoe	4	legal	5	popular	6	dream
7	goat	8	feel	9	grape	10	region	11	exercise	12	item

Example 3

1	icon	2	brown	3	forget	4	volcano	5	warfare	6	hammer
7	tomato	8	puppy	9	purpose	10	reason	11	marine	12	keep

Example 4

1	anger	2	bone	3	swamp	4	input	5	tooth	6	erase
7	tank	8	rotate	9	old	10	noodle	11	wing	12	clever

Example 5

1	barrel	2	solar	3	unique	4	girl	5	news	6	people
7	cost	8	brown	9	crew	10	tray	11	pony	12	express

Example 6

1	require	2	luxury	3	result	4	zero	5	magnet	6	shy
7	company	8	park	9	coin	10	patient	11	slot	12	pipe

Example 7

1	twist	2	lady	3	next	4	glue	5	fringe	6	deny
7	crunch	8	iron	9	jealous	10	shadow	11	gather	12	glance

Reading a BIP39 phrase

Every word stands for an 11-bit number: its position in the 2048-word list, counted from 0. Here is Example 1 decoded word by word. Each word links to its page on bip39-phrase.com, where the list is numbered from 1.

#	Word	Index (0-2047)	Word no.	11 bits
1	toe	1820	1821	11100011100
2	pretty	1361	1362	10101010001
3	naive	1173	1174	10010010101
4	extend	647	648	01010000111
5	dizzy	513	514	01000000001
6	slab	1623	1624	11001010111
7	risk	1491	1492	10111010011
8	patient	1288	1289	10100001000
9	engine	595	596	01001010011
10	cover	396	397	00110001100
11	arena	91	92	00001011011
12	exile	637	638	01001111101

The 12 words carry 132 bits: 128 bits of entropy followed by a 4-bit checksum. The checksum must equal the first 4 bits of the SHA-256 hash of the entropy.

Entropy (hex): e395464aa8740395ee9d084a66302da7

This sequence ends in the checksum bits 1101, but SHA-256 of its entropy starts with 1011, so wallets reject it as an invalid phrase. That is the point of the checksum: about 15 of every 16 random or mistyped sequences fail it.

See also

- [Cold Storage Solutions for Long-Term Holding](#) · June 2, 2026
- [BIP-39 SEED PHRASE The Principles of Cryptographic Backup and Wallet Recovery](#) · seed-phrase_june-10
- [BIP-39 Seed Phrases: The Most Dangerous Backup You'll Ever Own](#) · backup-own_2025-june
- [How to Safely Store Your Seed Phrase](#) · June 15, 2026

Educational document. The example sequences are random and fail the BIP39 checksum: they are not wallets and must never hold funds. Security notes: bip39-phrases.com/security/