# Home Safe or Hiding Spot for a Seed Backup?

November 10, 2026 · Document #424 · bip39-phrase.com



Photo by Kelly Sikkema on Unsplash

Compare home safes and concealed seed backups by theft, fire, disposal, and inheritance risks, and learn when combining them helps.

**Contents**


What a home safe protects—and what it does not 2

What concealment protects—and what it risks 2

When combining both makes sense 3

FAQ 3

Sources 3

Example BIP39 word sequences 4

Reading a BIP39 phrase 4

See also 5


A portable home safe can let a burglar carry away your seed backup; a clever hiding spot can let your family throw it away. The better choice depends on which risks you can control: theft, fire, water, accidental disposal, and recovery after your death or incapacity.

A BIP39 mnemonic commonly contains 12 or 24 words. Without an additional passphrase, someone who copies those words can generally restore the wallet represented by them and spend its funds. Physical storage therefore has two jobs: prevent unauthorized copying and keep the backup recoverable.

## What a home safe protects—and what it does not

A home safe provides a defined place for the backup and a barrier against casual access. It also advertises that something valuable may be inside. Burglars may target the safe rather than search the rest of the room, especially if it is portable.

- **Fire protection:** Look for an independently tested rating, not merely “fireproof” advertising. UL 72 Class 350 concerns protection of paper records, with an interior temperature limit of 350°F, approximately 177°C. The duration matters: a one-hour rating is not unlimited protection. Other UL 72 classes address contents that require lower interior temperatures.
- **Burglary resistance:** A fire rating does not establish resistance to prying, drilling, or removal. Check the exact model’s burglary certification separately. A basic lockbox and a burglary-rated safe are not equivalent.
- **Anchoring:** Bolt the safe to a suitable structural substrate using the manufacturer’s approved mounting points and installation instructions. A heavy safe that two people can move is still removable. Poor anchoring can fail, while unauthorized drilling may compromise fire protection.
- **Water exposure:** A fire rating does not establish flood resistance. Consider plumbing leaks, firefighting water, and whether the chosen location could become submerged.

Paper inside a rated safe may be a reasonable arrangement, but inspect it periodically for moisture and deterioration. A corrosion-resistant metal backup can improve durability, although its performance depends on the alloy, construction, and how the words are recorded. Metal does not prevent theft or copying.

Keep the safe combination or key accessible through a separate, controlled recovery process. A backup locked inside a safe that nobody can open has an availability problem, even if the words remain intact.

## What concealment protects—and what it risks

A concealed spot avoids an obvious target. Its weakness is that secrecy can disappear instantly: a contractor opens a panel, a visitor notices a container, or someone reorganizes a cupboard.

- **Discovery:** Avoid assuming an ordinary household hiding place is unknown to burglars. Concealment delays discovery; it does not provide a tested access barrier.
- **Accidental disposal:** Do not put the only backup inside packaging, old electronics, furniture, or another object likely to be sold, recycled, or discarded.
- **Environmental damage:** Roof spaces, basements, and wall cavities can expose backups to heat, condensation, pests, or leaks. An obscure location may also make inspection difficult.
- **Inheritance failure:** If only you know the location, your heirs may never recover it. Leave a controlled locator instruction that identifies the backup and explains whom to contact, without unnecessarily reproducing the words.

Test the retrieval process without photographing or typing the seed into an internet-connected device. Can an authorized person identify the correct object, reach it safely, and understand its purpose? If not, the hiding scheme is incomplete.

## When combining both makes sense

A discreetly installed, anchored safe combines concealment with an access barrier. This makes sense when the safe can be kept out of casual view without blocking its door, undermining installation requirements, or exposing it to moisture. Concealment should supplement the safe, not substitute for its security rating.

Two backups can also reduce loss risk, but two copies in the same house remain exposed to the same building fire or burglary. Each additional complete copy creates another opportunity for theft.

1. Identify the most credible hazards: opportunistic theft, targeted burglary, fire, flooding, household disposal, or your own incapacity.
2. Choose a durable backup medium and a location that address those hazards. For a safe, verify the exact model's ratings and anchoring requirements.
3. Consider a second complete backup in a separately controlled location if losing the home would otherwise destroy every copy. Document who can access each location.
4. Leave recovery instructions that explain where the backup is and which wallet setup it restores. Never place the actual seed words in a publicly accessible document.
5. Review access and condition after moving, renovating, changing household arrangements, or changing executors.

Do not improvise by dividing the word list between hiding places. Missing words can prevent recovery, and partial disclosure can reduce security. A BIP39 passphrase can separate possession of the mnemonic from spending access, but it introduces another secret that must survive independently; every passphrase produces a valid seed, including a mistyped one.

## FAQ

### Is a cheap fire safe enough?

It may help with a limited fire exposure if independently rated, but that does not establish burglary resistance. Check anchoring, certification, and the backup medium separately.

### Should I hide the safe key beside the backup?

No. Keep access credentials under separate control, with a documented route for authorized recovery.

### Can heirs recover a wallet from the words alone?

Often, but not always. They may also need a BIP39 passphrase and wallet-specific information such as derivation paths or multisignature configuration.

## Sources


- BIP 39: Mnemonic code for generating deterministic keys (github.com)
- BIP 32: Hierarchical Deterministic Wallets (github.com)

> Continue reading on bip39-phrase.com: How to Store Crypto Safely: A Hot, Cold and Backup Plan
> 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 | praise | 2 | mule | 3 | poet | 4 | insect | 5 | maximum | 6 | flush |
| 7 | resist | 8 | city | 9 | benefit | 10 | eternal | 11 | artwork | 12 | please |

**Example 2**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | merit | 2 | quality | 3 | royal | 4 | ahead | 5 | clap | 6 | enemy |
| 7 | employ | 8 | lab | 9 | jewel | 10 | file | 11 | winter | 12 | account |

**Example 3**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | latin | 2 | run | 3 | sketch | 4 | lonely | 5 | arch | 6 | detail |
| 7 | file | 8 | hunt | 9 | cycle | 10 | spatial | 11 | power | 12 | blade |

**Example 4**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | wage | 2 | laptop | 3 | puppy | 4 | hard | 5 | harvest | 6 | message |
| 7 | wreck | 8 | coffee | 9 | pave | 10 | cable | 11 | measure | 12 | beyond |

**Example 5**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | current | 2 | crawl | 3 | protect | 4 | laptop | 5 | talk | 6 | glove |
| 7 | boy | 8 | indicate | 9 | view | 10 | empower | 11 | tag | 12 | boat |

**Example 6**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | equip | 2 | range | 3 | reflect | 4 | resist | 5 | comic | 6 | dry |
| 7 | image | 8 | train | 9 | apple | 10 | merry | 11 | jaguar | 12 | priority |

## 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 | praise | 1356 | 1357 | 10101001100 |
| 2 | mule | 1162 | 1163 | 10010001010 |
| 3 | poet | 1337 | 1338 | 10100111001 |

| # | Word | Index (0-2047) | Word no. | 11 bits |
|---|---|---|---|---|
| 4 | insect | 936 | 937 | 01110101000 |
| 5 | maximum | 1099 | 1100 | 10001001011 |
| 6 | flush | 718 | 719 | 01011001110 |
| 7 | resist | 1467 | 1468 | 10110111011 |
| 8 | city | 331 | 332 | 00101001011 |
| 9 | benefit | 169 | 170 | 00010101001 |
| 10 | eternal | 620 | 621 | 01001101100 |
| 11 | artwork | 105 | 106 | 00001101001 |
| 12 | please | 1331 | 1332 | 10100110011 |

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): a9922a9cba8896b3add94b1529b034d3`

This sequence ends in the checksum bits 0011, but SHA-256 of its entropy starts with 1010, 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

- Off-Site Seed Backup Options Beyond Your Home · June 15, 2026
- Fire Safes Can Trap Humidity Around a Seed Backup · October 26, 2026
- Picking a Seed Phrase Executor: Trust Before Skill · October 27, 2026
- Don't Keep the Backup in the Hardware Wallet Box · October 17, 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-phrase.com/security/