Do You Actually Need a BIP39 Passphrase?

November 9, 2026 · Document #423 · bip39-phrase.com

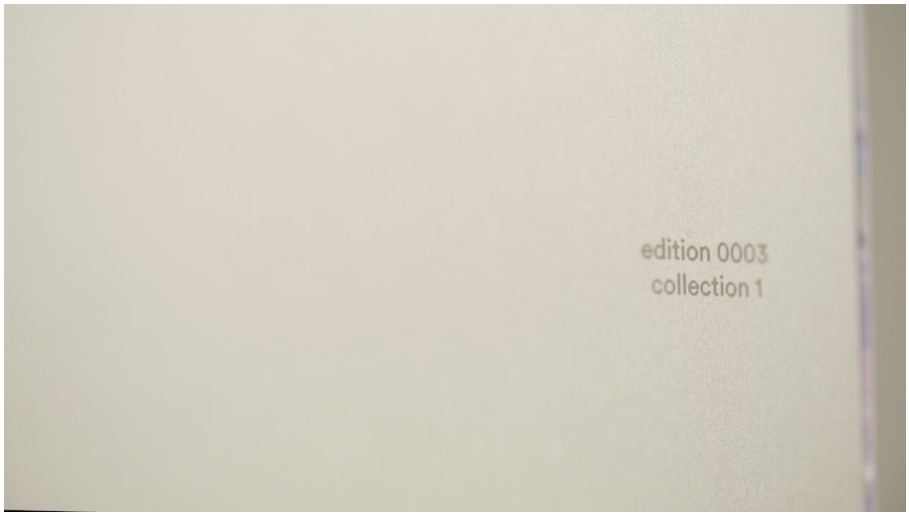


Photo by gomi on Unsplash

Weigh BIP39 passphrase protection against backup theft, coercion limits and the risk of losing access through recovery mistakes.

Contents

What a BIP39 passphrase actually changes	2
Protection against theft and coercion	2
Who benefits, and how to decide	3
FAQ	3
Sources	4
Example sequences from the BIP39 wordlist	4
Reading a BIP39 phrase	5
See also	6

A strong BIP39 passphrase can stop someone who finds only your seed phrase backup from accessing your wallet. It also adds another secret you must reproduce: losing it can permanently lock you out, even when every seed word is correct. Whether you need one depends on which failure your setup is more likely to suffer. ([trezor.io](https://trezor.io/guides/backups-recovery/advanced-wallets/what-is-a-passphrase))

For individual holders, forgetting, mis-recording or failing to pass on an extra secret can be a more immediate concern than a targeted theft. There is no universal loss rate that settles this decision. Start with your storage arrangements, recovery habits and inheritance needs.

What a BIP39 passphrase actually changes

BIP39 turns a mnemonic and an optional passphrase into a 512-bit seed using PBKDF2-HMAC-SHA512 with `2048` iterations. The mnemonic is the password input; the salt is `mnemonic` followed by the passphrase. Both are NFKD-normalized and UTF-8-encoded. If no passphrase is used, it is an empty string. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

The passphrase is separate from your wallet application's password or hardware wallet PIN. Those usually restrict access to a particular device or file. A BIP39 passphrase changes the seed from which the wallet derives its keys, so it matters during recovery on another compatible wallet. ([coldcard.com](https://coldcard.com/docs/passphrase/))

Every passphrase produces a valid seed. BIP39 has no passphrase checksum or built-in wrong-passphrase test. A typo generally opens a different wallet, although applications can add confirmation checks. Capitalization, spaces and punctuation matter; different Unicode strings that normalize to the same NFKD text produce the same seed. Character support varies between wallets. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

The nickname “25th word” is misleading. A passphrase need not be one word, need not use the BIP39 word list and can accompany a 12-word mnemonic. Avoid using a single predictable word simply because of that nickname. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Protection against theft and coercion

If someone obtains only your mnemonic backup, a sufficiently strong, separately protected passphrase makes recovering the protected wallet through guessing impractical. This is useful when backups sit somewhere that other people could access, such as a shared home, safe-deposit box or relative's property. ([coldcard.com](https://coldcard.com/docs/passphrase/))

An attacker holding the mnemonic can guess passphrases offline. BIP39's fixed `2048` iterations provide limited resistance to guessing attacks. A familiar quotation, reused password or predictable variation may offer much less protection than expected. Use an independently generated secret with substantial randomness, such as several randomly selected words, and confirm your wallet's supported input limits. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Keeping the passphrase beside the mnemonic removes most of its benefit against discovery of that location. Keeping it only in your head creates a different weakness: illness, injury, time or death can make recovery impossible. ([coldcard.com](https://coldcard.com/docs/passphrase/))

Coercion is harder to address. Different passphrases can create separate wallets, allowing someone to disclose one wallet while another remains undisclosed. However, **plausible deniability is not a guarantee of safety**. An attacker may suspect additional wallets, see transaction evidence or continue demanding access. No wallet balance proves that another wallet does not exist. Do not treat a passphrase as a dependable solution to physical threats. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Who benefits, and how to decide

The strongest candidates are people with a credible backup-discovery risk and the discipline to maintain separate, tested recovery records. Examples include holders with backups across several locations, people in shared accommodation and experienced users separating substantial long-term savings from everyday spending. ([coldcard.com](https://coldcard.com/docs/passphrase/))

The weakest candidates are people who already struggle to locate backups, frequently confuse passwords or depend on relatives who would find recovery difficult. Adding complexity before fixing those problems can reduce overall safety. A secure mnemonic backup, a device PIN and a tested recovery process may deserve attention first. ([trezor.io](https://trezor.io/guides/backups-recovery/advanced-wallets/what-is-a-passphrase))

Before enabling a passphrase, work through these steps:

1. Identify the specific exposure. Write down who could obtain your mnemonic and how. If you cannot name a realistic scenario, the extra recovery burden may outweigh the benefit.
2. Choose an exact, reproducible secret. Avoid personal facts, reused credentials and improvised spelling tricks. Check passphrase support, allowed characters and entry limits on both your normal wallet and your intended recovery device. ([trezor.io](https://trezor.io/guides/trezor-suite/using-a-passphrase-wallet-in-trezor-suite))
3. Create a durable record stored separately from the mnemonic. Protect both locations against unauthorized access and accidental loss. Include instructions that identify the need for a BIP39 passphrase without putting both secrets together. ([coldcard.com](https://coldcard.com/docs/passphrase/))
4. Test recovery before depositing substantial funds. Use trusted hardware or an appropriate offline process. Compare the full receiving address for the same network, account, address type and address index. Never enter a live mnemonic into a website to perform this test. ([trezor.io](https://trezor.io/guides/trezor-suite/using-a-passphrase-wallet-in-trezor-suite))
5. Plan for incapacity and inheritance. An authorized successor needs access to both secrets and enough instructions to identify the wallet. Record relevant wallet software, networks and derivation details separately where necessary. ([coldcard.com](https://coldcard.com/docs/passphrase/))

Adding a passphrase creates a separate wallet; it does not automatically protect funds already held in the wallet using an empty passphrase. Moving on-chain funds to the new wallet requires one or more transactions on the relevant networks. Verify the destination on your trusted device and test with a small amount first. ([trezor.io](https://trezor.io/guides/trezor-suite/using-a-passphrase-wallet-in-trezor-suite))

FAQ

Can I recover funds if I forget the passphrase?

The mnemonic alone cannot recreate that wallet. Recovery from the mnemonic requires the same normalized passphrase or successful guessing, which a strong passphrase makes impractical. An accessible wallet that retains the necessary signing keys, or a separate backup of those keys, may still let you move the funds. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Should I memorize it instead of writing it down?

Memorization can supplement a backup. Relying on memory alone exposes recovery to forgetting, injury and inheritance failures.
([trezor.io](https://trezor.io/guides/backups-recovery/advanced-wallets/what-is-a-passphrase))

Does everyone need a BIP39 passphrase?

No. It is most useful when protection against a discovered mnemonic justifies managing another essential secret and testing its recovery.
([trezor.io](https://trezor.io/guides/backups-recovery/advanced-wallets/what-is-a-passphrase))

Sources

- BIP39: Mnemonic code for generating deterministic keys (github.com)
- Trezor: What is a passphrase? (trezor.io)
- Trezor: Using a passphrase wallet in Trezor Suite (trezor.io)

> Continue reading on bip39-phrase.com: Is a Seed Phrase Case Sensitive? BIP39 Words vs Passphrase
> More on this topic: Seed Phrases

Example sequences from the BIP39 wordlist

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 tuition	2 treat	3 equip
4 tonight	5 member	6 tube
7 sausage	8 bread	9 girl
10 fever	11 large	12 clock

Example 2

1 relief	2 arrange	3 orient
4 stable	5 habit	6 menu
7 bind	8 athlete	9 patrol
10 siren	11 reflect	12 lawsuit

Example 3

1 topic	2 miracle	3 tackle
4 expose	5 owner	6 boil
7 valve	8 club	9 orchard
10 door	11 rice	12 pretty

Example 4		
1 student	2 sister	3 baby
4 magnet	5 trial	6 physical
7 feature	8 noise	9 romance
10 input	11 cloud	12 sheriff

Example 5		
1 horse	2 term	3 diet
4 chat	5 kiss	6 main
7 remove	8 tattoo	9 develop
10 better	11 peanut	12 cargo

Example 6		
1 person	2 steak	3 famous
4 welcome	5 share	6 manage
7 that	8 neglect	9 width
10 tiger	11 cream	12 aim

Example 7		
1 people	2 fantasy	3 author
4 twenty	5 video	6 sure
7 quality	8 runway	9 ocean
10 loyal	11 fiber	12 artist

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	tuition	1873	1874	11101010001
2	treat	1854	1855	11100111110
3	equip	609	610	01001100001
4	tonight	1828	1829	11100100100
5	member	1110	1111	10001010110
6	tube	1872	1873	11101010000
7	sausage	1533	1534	10111111101
8	bread	219	220	00011011011
9	girl	786	787	01100010010

#	Word	Index (0-2047)	Word no.	11 bits
10	fever	683	684	01010101011
11	large	1001	1002	01111101001
12	clock	347	348	00101011011

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): ea3cf930f248add42fe8db624aadf495
```

This sequence ends in the checksum bits 1011, but SHA-256 of its entropy starts with 1101, 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

- Don't Keep the Backup in the Hardware Wallet Box · October 17, 2026
- Coins Sent to Mistyped or Wrongly Restored Wallets · October 15, 2026
- Diceware Lists and BIP39 Words: Different Jobs · October 30, 2026
- Understanding Seed Phrases · June 9, 2025

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/