Seed Word Not on the BIP39 List: Find the Right Word

November 25, 2026 · Document #439 · bip39-phrase.com



Photo by Paul Arky on Unsplash

Find an unlisted seed word offline using prefixes and spelling variants, then verify the correction with a checksum and known address.

Contents

Why the exact word matters 2

Find plausible corrections offline 2

Confirm with checksum and wallet evidence 3

FAQ 3

Sources 4

BIP39 format examples 4

Reading a BIP39 phrase 5

See also 6

A BIP39 restore screen that enforces word-list membership rejects an unlisted word because each word must identify one of exactly 2,048 entries in the selected language’s list. A spelling such as `armour` cannot substitute for the listed English word `armor`. Some software can derive a seed from nonstandard text, so acceptance alone does not establish validity. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039/english.txt))

The practical repair is to compare your written word with the official list offline, identify plausible corrections, and test them against both the mnemonic checksum and a receive address you already know belongs to the wallet.

Why the exact word matters

BIP39 assigns each word an index from `0` through `2047`. Each index represents 11 bits. Together, the words encode the original entropy and a checksum derived from its SHA-256 hash. Standard mnemonic lengths are `12`, `15`, `18`, `21` and `24` words. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

An unlisted word has no index in the selected list, so a validating restore interface cannot decode it using that list. Adding it to a local dictionary does not repair the original backup. The list's ordering matters too. Seed derivation uses the normalized mnemonic text, so changing a word can change the resulting wallet even if software accepts it. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

First confirm that the backup actually uses BIP39 and that you selected the correct language. Other recovery systems can use different dictionaries or encoding rules. A valid word in another system does not become a valid BIP39 entry simply because it looks familiar. ([trezor.io](https://trezor.io/support/troubleshooting/trezor-suite-issues/troubleshoot-wallet-backup-and-recovery-problems?utm_source=openai))

BIP39 also specifies Unicode NFKD normalization, but normalization does not translate English regional spellings, remove plural endings or change verb tenses. Those differences require identifying the original word. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

Find plausible corrections offline

For an English backup, use the official English word list from the Bitcoin BIPs repository. Obtain it on a separate device, then make it available on the offline device without transferring your seed phrase to the online device. A local text viewer is enough to inspect the list; a recovery website is unnecessary. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039/english.txt))

1. Preserve the original transcription. Work from a copy, and mark the uncertain word's position. Keep all other words in their original order.
2. Check the first four letters. The English list was designed so that the first four letters uniquely identify each word. For entries shorter than four letters, use the complete word. If your recorded prefix is accurate, it can identify the intended entry even when the ending is wrong. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))
3. Compare lengths. Count letters and look for an added suffix, an omitted letter or a doubled character. Length helps rank candidates; it is not a strict filter because a copying mistake can change it.
4. Check nearby spelling variants. Consider a plural instead of a singular, a different verb tense, or a regional spelling. For example, recorded `armour` has the same first four letters as `armor`, but contains an extra `u`. Only `armor` is in the official English list. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039/english.txt))
5. If the prefix finds nothing, inspect the handwriting again. One of the first four letters may also be wrong. Compare similar letter shapes, adjacent-letter swaps and single-letter omissions against actual list entries.

Build a small candidate set containing only official words. Do not assume that removing an ending always produces the answer: the resulting word must appear in the list. Never upload the phrase, a photograph of the

backup or a partially completed restore form to obtain suggestions.

Confirm with checksum and wallet evidence

Use a trusted hardware wallet's recovery interface or a verified BIP39 implementation on an offline device to test the candidate replacements. Follow the device's prompts for entering words by position. Do not wipe a working wallet to test candidates; use its backup-check feature or a spare device. Dictionary membership alone does not establish that the checksum passes. ([trezor.io](https://trezor.io/support/troubleshooting/trezor-suite-issues/troubleshoot-wallet-backup-and-recovery-problems?utm_source=openai))

A passing checksum is necessary for a standard BIP39 mnemonic but insufficient to identify your wallet. A 12-word mnemonic has four checksum bits; a 24-word mnemonic has eight. Exactly `1/16` and `1/256`, respectively, of uniformly random sequences of listed words pass. These proportions do not predict the precise pass rate of a particular spelling-based candidate set. The checksum catches most errors, not all. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

After a candidate passes, restore with the original BIP39 passphrase, if you used one; otherwise use an empty passphrase. NFKD normalization applies to the passphrase too, so different spellings that normalize identically produce the same seed. A passphrase mistake does not change the mnemonic checksum and can open a different wallet without a checksum error. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

Next, reproduce a **known receive address** from your wallet records. Match the complete address, checking it on the hardware wallet's trusted display where supported. Use the same network, account, derivation path, address type and receive/change branch and index. For Bitcoin, different script types can produce different addresses from the same seed. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0044.mediawiki))

If the first displayed address differs, check those settings before discarding the candidate. Your recorded address may belong to a later receive index or another account. Record any known path and index alongside the comparison result. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0044.mediawiki))

Once a candidate passes the checksum and reproduces the known address under the expected settings, correct the physical backup clearly and perform the wallet's backup verification procedure, if available. Preserve the original transcription until verification is complete. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0044.mediawiki))

FAQ

Can I enter only the first four letters?

Some wallets support unique-prefix entry. Others require the complete word. The four-letter rule applies to the English list; follow the interface's instructions and confirm the expanded word. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

Can two corrections both pass the checksum?

Yes. The checksum does not uniquely identify the original mnemonic. Use the original passphrase and a known receive address to distinguish plausible candidates. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

What if no candidate works?

Recheck the language, word count, word order and other transcriptions. The invalid-looking word may not be the only mistake. If the original wallet accepted a nonstandard phrase, consult its recovery documentation: BIP39 seed derivation can process text that fails standard mnemonic validation. ([raw.githubusercontent.com](https://raw.githubusercontent.com/bitcoin/bips/master/bip-0039.mediawiki))

Sources

- BIP39: Mnemonic code for generating deterministic keys (github.com)
- BIP39 official English word list (github.com)
- BIP44: Multi-Account Hierarchy for Deterministic Wallets (github.com)

> Continue reading on bip39-phrase.com: Invalid Seed Phrase? How to Find and Fix a Wrong Word (BIP39)
> More on this topic: Recovery

BIP39 format examples

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 alcohol	2 reward	3 humble	4 over
5 ivory	6 juice	7 monitor	8 cake
9 cricket	10 jaguar	11 hollow	12 enter

Example 2			
1 strike	2 hazard	3 park	4 witness
5 immense	6 country	7 occur	8 jungle
9 bronze	10 early	11 shove	12 acoustic

Example 3			
1 blind	2 sister	3 bomb	4 vocal
5 silent	6 rubber	7 escape	8 donkey
9 hockey	10 front	11 slice	12 remove

Example 4			
1 gate	2 dove	3 route	4 length
5 assault	6 tonight	7 wish	8 fuel
9 hamster	10 position	11 depth	12 vapor

Example 5			
1 olive	2 siege	3 review	4 great
5 card	6 theory	7 whale	8 health
9 execute	10 neutral	11 assume	12 confirm

Example 6			
1 pluck	2 host	3 used	4 energy
5 peasant	6 spring	7 club	8 bonus
9 acoustic	10 indoor	11 letter	12 juice

Example 7			
1 hood	2 wheel	3 define	4 cause
5 like	6 grid	7 pencil	8 middle
9 better	10 wink	11 pepper	12 force

Example 8			
1 theme	2 oil	3 frequent	4 uphold
5 quick	6 dress	7 upper	8 orange
9 ill	10 sort	11 edit	12 flip

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	alcohol	48	49	00000110000
2	reward	1477	1478	10111000101
3	humble	887	888	01101110111
4	over	1263	1264	10011101111
5	ivory	951	952	01110110111
6	juice	966	967	01111000110
7	monitor	1144	1145	10001111000
8	cake	258	259	00100000010
9	cricket	411	412	00110011011

#	Word	Index (0-2047)	Word no.	11 bits
10	jaguar	953	954	01110111001
11	hollow	871	872	01101100111
12	enter	603	604	01001011011

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): 061715bbcef76ef1a3c102336ee5b3a5
```

This sequence ends in the checksum bits 1011, but SHA-256 of its entropy starts with 0011, 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

- 12, 18 or 24 Words: Picking the Right Count at Restore · November 20, 2026
- French Seed Phrases: Accents and Shared English Words · November 18, 2026
- Leaving Off the Last BIP39 Word: A False Trick · January 8, 2025
- Decoding a BIP39 Phrase Back Into Entropy Bits · July 18, 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/