Lost Your Seed Backup but the Wallet Still Works?

November 19, 2026 · Document #433 · bip39-phrase.com



Photo by Aaron Burden on Unsplash

Treat a signing wallet with a lost backup as temporary access: check official recovery options, verify a new backup, and migrate assets before access fails.

Contents

Act before the wallet stops working 1

Why memory is not a reliable backup 2

Apps and hardware wallets handle phrases differently 3

Move funds to a new seed 3

FAQ 4

Sources 5

Example sequences from the BIP39 wordlist 5

Reading a BIP39 phrase 6

See also 6

Act before the wallet stops working

If your wallet can still sign transactions but its seed backup is lost, treat that access as temporary. A device failure, app deletion, forgotten PIN, damaged storage, or an unexpected reset can remove it. Opening an app and seeing a balance does not prove that you can spend: a watch-only wallet or disconnected hardware wallet may still display accounts. For a seed-based wallet, the recovery phrase and any required passphrase let compatible software recreate its derived keys. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki))

Do not wait for a convenient time to solve the problem. First identify the wallet's backup format, whether it uses an additional passphrase, and which networks and accounts contain funds. Not every wallet uses BIP39; some use SLIP39 shares or other recovery methods. One seed can derive many accounts, but separately imported private keys may need their own backups. Record relevant derivation paths and account types too. ([trezor.io](https://trezor.io/learn/security-privacy/personal-security-standards/understanding-trezor-wallet-backups-12-20-or-24-words?utm_source=openai))

Why memory is not a reliable backup

Recreating an old phrase from memory alone is unsafe because every word and its position matters. BIP39 phrases use a specified word list and include a checksum. That checksum catches most accidental errors, not all: an incorrect phrase can still pass validation and derive a different wallet. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Common memory errors include:

- Swapping two adjacent words.
- Remembering a similar word from the BIP39 list.
- Omitting a repeated word.
- Confusing a 12-word phrase with a 15-, 18-, 21-, or 24-word phrase.
- Mistyping words or separators instead of following the wallet's expected input format.
- Remembering the recovery phrase but forgetting a separate BIP39 passphrase, whose capitalization and spaces matter. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

A restored wallet showing no funds does not establish whether the phrase is correct. Check known receiving addresses, derivation paths, accounts, networks, and any passphrase. A different BIP39 passphrase derives a different wallet without an inherent "wrong passphrase" error. Repeatedly entering recovery material into unfamiliar tools also creates opportunities for theft. ([support.metamask.com](https://support.metamask.com/configure/wallet/how-to-restore-your-metamask-wallet-from-secret-recovery-phrase?utm_source=openai))

Never submit a real recovery phrase to a website, chat, support form, or unfamiliar checker. Enter it only when necessary through a verified wallet's documented recovery process, preferably on the hardware device when supported. A checksum check verifies word-list membership, length, and checksum consistency; it cannot prove ownership or rule out every transcription error. ([support.metamask.com](https://support.metamask.com/configure/wallet/how-to-reveal-your-secret-recovery-phrase/))

Apps and hardware wallets handle phrases differently

A software wallet app normally stores secret material on a phone or computer, often protected by an app password or operating-system security. If it remains accessible, its settings may offer “reveal,” “show,” or “export” for the recovery phrase. The behavior depends on the wallet and account type. MetaMask, for example, supports revealing a locally stored phrase after authentication. Follow the official procedure and copy it directly to a durable offline backup without screenshots or cloud notes. ([support.metamask.com](https://support.metamask.com/configure/wallet/how-to-reveal-your-secret-recovery-phrase/))

A hardware wallet normally keeps signing secrets isolated from its companion application. That application can request signatures, addresses, and public keys, but generally cannot display the recovery phrase. Phrase display, later backup options, and supported recovery services vary by device and firmware; initial setup and backup verification are different operations. Follow the manufacturer’s documented procedure, and do not trust unofficial software promising to reveal the seed. ([trezor.io](https://trezor.io/support/troubleshooting/trezor-suite-issues/troubleshoot-wallet-backup-and-recovery-problems?utm_source=openai))

If a hardware wallet is still usable and you have a candidate backup, check whether it offers an official backup check. This can compare the entered backup with the device’s stored wallet without exporting its secrets. It does not necessarily verify a separate passphrase or every account configuration. Do not reset your only working device to test a suspected backup. ([trezor.io](https://trezor.io/guides/backups-recovery/general-standards/check-backup-on-trezor-safe-3))

Move funds to a new seed

When the old backup is permanently missing and cannot be safely recreated through the wallet’s official procedure, the safer fix is usually to create a new wallet and transfer the funds. Set up the destination separately: resetting your only working device first can destroy your remaining access. ([trezor.io](https://trezor.io/guides/backups-recovery/general-standards/move-crypto-to-a-wallet-with-a-new-wallet-backup))

1. Create the new wallet using a trusted hardware wallet or a reputable wallet app obtained through official channels. Generate the new seed through its normal setup flow; never choose the recovery words yourself. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))
2. Write the new recovery phrase on paper or another suitable offline backup medium. Consider two accurate copies stored securely in separate locations. If using a share-based backup, follow its threshold and storage requirements instead. Complete the wallet’s backup verification process. ([trezor.io](https://trezor.io/guides/backups-recovery/general-standards/check-backup-on-trezor-safe-3))
3. Record whether you use an additional passphrase, preserving its exact capitalization and spaces. Treat it as essential recovery information and decide whether to store it separately based on your threat model. ([trezor.io](https://trezor.io/guides/trezor-suite/using-a-passphrase-wallet-in-trezor-suite?utm_source=openai))

4 Obtain receiving addresses from the new wallet, confirm the destination supports the asset and network, and verify addresses on the hardware device when available. Send a small test amount first where fees and network rules make that practical. ([trezor.io](https://trezor.io/guides/trezor-devices/trezor-fundamentals/moving-to-trezor-from-another-wallet?utm_source=openai))

5 Transfer assets from every relevant old account and network. Token balances, NFTs, staking positions, layer-two funds, and contract roles may require separate transfers, withdrawals, or ownership updates; some positions have restrictions or waiting periods. ([ethereum.org](https://ethereum.org/developers/docs/transactions/))

6 Confirm transactions have sufficient network confirmation and that the new wallet can sign. Keep the old wallet available until migration is complete. For later monitoring, use public addresses or supported watch-only data; never import the old seed merely to create a watch-only view. ([trezor.io](https://trezor.io/guides/backups-recovery/general-standards/move-crypto-to-a-wallet-with-a-new-wallet-backup))

A balance transfer does not automatically migrate contract ownership, token approvals, domain registrations, or staking arrangements. Review each separately; disconnecting a dapp does not revoke token approvals. On networks such as Ethereum, keep enough native currency in the old account to pay remaining transaction fees unless a supported fee-sponsorship mechanism covers them. On Bitcoin and similar UTXO networks, check for unspent outputs and change left behind. ([support.metamask.com](https://support.metamask.com/more-web3/dapps/manage-dapp-permissions/?utm_source=openai))

If you later find the old paper backup, treat it as potentially compromised if anyone could have accessed it. Finding it does not undo that exposure. Keep the replacement backup offline and verify recovery before relying on it for substantial funds, using an official backup check or a separate trusted device. Do not erase the only working wallet as a recovery test. ([trezor.io](https://trezor.io/blog/security/what-to-do-if-your-trezor-or-wallet-backup-goes-missing))

FAQ

Can I guess the missing words until the wallet appears?

Do not rely on guessing. Limited missing information can sometimes be recovered, but checksum validity alone cannot identify your wallet. Confirm any candidate against known addresses and the correct wallet configuration using trusted offline methods. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Why can my app show the phrase but my hardware wallet cannot?

A software wallet may retain the phrase locally and offer an authenticated export function. Hardware wallets usually restrict secret export, and their companion apps generally cannot reveal the phrase. Exact backup options depend on the device and firmware. ([support.metamask.com](https://support.metamask.com/configure/wallet/how-to-reveal-your-secret-recovery-phrase/))

Should I transfer funds if the old wallet still works?

Usually yes when the backup is permanently lost and cannot be safely recreated through an official procedure. Create and verify a separate new wallet first, then migrate every relevant account and asset while the old wallet can still sign. ([trezor.io](https://trezor.io/guides/backups-recovery/general-standards/move-crypto-to-a-wallet-with-a-new-wallet-backup))

Sources

- BIP-39: Mnemonic code for generating deterministic keys (github.com)
- BIP-32: Hierarchical Deterministic Wallets (github.com)
- MetaMask: How to reveal your Secret Recovery Phrase safely (support.metamask.com)

> Continue reading on bip39-phrase.com: Recover Lost Bitcoin: Find Wallet Backups and Seed Phrases
> 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	brain	2	rocket	3	produce	4	salt	5	inside	6	doll
7	coil	8	strategy	9	abandon	10	width	11	owner	12	insane

Example 2

1	skin	2	salad	3	nasty	4	save	5	unlock	6	throw
7	danger	8	stuff	9	spoil	10	poet	11	machine	12	disagree

Example 3

1	pyramid	2	meadow	3	armed	4	remove	5	cloud	6	slender
7	today	8	enrich	9	punch	10	frozen	11	voice	12	require

Example 4

1	say	2	cinnamon	3	clown	4	good	5	pet	6	wisdom
7	van	8	clinic	9	neglect	10	able	11	fever	12	motion

Example 5

1	ignore	2	hospital	3	cheap	4	drift	5	confirm	6	dutch
7	planet	8	combine	9	motion	10	then	11	wild	12	endorse

Example 6												
1	spatial	2	right	3	drastic	4	canal	5	safe	6	giggle
7	donate	8	deliver	9	powder	10	index	11	input	12	cradle

Example 7												
1	budget	2	lift	3	reveal	4	gorilla	5	refuse	6	purpose
7	mistake	8	dirt	9	include	10	flat	11	shock	12	hobby

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	brain	215	216	00011010111
2	rocket	1499	1500	10111011011
3	produce	1373	1374	10101011101
4	salt	1525	1526	10111110101
5	inside	937	938	01110101001
6	doll	517	518	01000000101
7	coil	362	363	00101101010
8	strategy	1718	1719	11010110110
9	abandon	0	1	00000000000
10	width	2006	2007	11111010110
11	owner	1265	1266	10011110001
12	insane	935	936	01110100111

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): 1af76eaedf5752814b56b6001f5a78ba`

This sequence ends in the checksum bits 0111, 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

- Don't Keep the Backup in the Hardware Wallet Box · October 17, 2026
- Do You Actually Need a BIP39 Passphrase? · November 9, 2026
- Mnemonic Keys to the Kingdom: Why BIP-39 Still Matters in 2025 · June 15, 2025

- Restored Wallet Still Syncing: Wait or Worry? · October 31, 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/