Picking a Seed Phrase Executor: Trust Before Skill

October 27, 2026 · Document #410 · bip39-phrase.com



Photo by Ashley West Edwards on Unsplash

Choose a trustworthy person to carry out wallet inheritance instructions, then fill technical gaps with a helper and a tested recovery guide.

Contents

Choose someone who will follow your instructions	2
Separate authority, secrets, and technical help	2
Write a recovery guide that closes the knowledge gap	2
FAQ	3
Sources	4
BIP39 format examples	4
Reading a BIP39 phrase	5
See also	6

Anyone who obtains a usable seed phrase and any required passphrase may be able to move the wallet’s funds. Multisignature wallets and other spending conditions may require additional keys or authorization. That makes choosing the person who will carry out your crypto inheritance instructions a question of trust before technical ability. A skilled wallet user can still misuse access; an honest, reliable person can learn a carefully documented recovery process with help.

Choose someone who will follow your instructions

An executor is a legal role whose powers depend on the applicable law and estate documents. The person helping recover your wallets might be that executor, a trustee, or someone working under their authority. Make clear who has legal responsibility, who receives the assets, and who provides technical assistance. Possessing wallet credentials does not establish legal ownership or permission to spend.

Start with evidence of character. Look for someone who has handled confidential information, kept commitments, and accounted for money accurately. Familiarity with exchanges, hardware wallets, or Bitcoin transactions is useful, but it does not establish honesty.

Consider whether the person can manage an uncomfortable task during grief, resist pressure from relatives, and ask for help without handing secrets to strangers. Someone who routinely loses documents or ignores administrative duties may struggle even with excellent instructions.

Discuss the responsibility before naming them. Explain the likely workload, the need for confidentiality, and the importance of keeping records. Let them decline. Name a replacement and review the choice after major changes in relationships, health, or availability.

Separate authority, secrets, and technical help

The person responsible for carrying out your wishes does not need to become a wallet expert. Their job is to control the process, verify authority, protect access, and ensure that distributions match the estate instructions.

A separate technical helper can identify compatible wallet software, explain recovery options, and help check transaction details. Choose someone who can explain each step clearly and work under supervision. A professional title alone does not establish competence or trustworthiness.

Define the helper’s access in advance:

- Give them wallet documentation and public information first; explain which records also reveal financial privacy.
- Arrange for the responsible person to enter recovery secrets directly into a suitable hardware wallet where the supported recovery procedure allows it.
- Require approval of the destination, amount, and fees before signing a transaction.
- Agree on fees, confidentiality, recordkeeping, and when specialist help is necessary.

Supervision cannot undo exposure. If a helper sees the complete seed phrase and any required passphrase, assume they could retain the ability to derive its keys. Where practical, recover into an environment you control and transfer the assets to a fresh wallet whose secrets are controlled by the authorized recipient or estate representative. A compromised computer can also substitute a destination, so check transaction details on the signing device’s trusted display where supported. Avoid approving transactions whose effects you cannot verify.

Write a recovery guide that closes the knowledge gap

A useful guide explains what exists, where authorized access begins, and how to recognize success. Keep general instructions separate from recovery secrets. Avoid putting the seed phrase in a will that could enter a public court record; arrange appropriate confidential storage and access procedures with local legal advice.

1. List the wallets and networks involved. Record the wallet application, hardware model if relevant, asset types, and whether additional accounts or addresses were used. Assets on different networks can require separate recovery steps.
2. Describe the backup precisely. BIP39 supports phrases of `12`, `15`, `18`, `21`, or `24` words, although individual wallets may support only some lengths. Some wallets use other backup formats, so record the actual standard rather than assuming every word backup is BIP39. BIP39's checksum detects many transcription errors, but it does not catch every error.
3. Document whether a BIP39 passphrase is required and how the authorized person can obtain it. BIP39 derives a seed from the mnemonic and passphrase without checking whether the passphrase is the intended one. A typing mistake can therefore open a different, apparently empty wallet without an error message. Capitalization and spaces matter; BIP39 requires Unicode NFKD normalization, so some differently encoded character sequences are equivalent.
4. Preserve wallet discovery details. Record derivation paths, account numbers, and address types where applicable. BIP32 defines hierarchical key derivation, but wallet software still needs compatible conventions to locate the intended accounts. For multisignature wallets, preserve the required wallet configuration as well as the necessary key backups.
5. Provide a verification reference. Keep a known receiving address or suitable public wallet record so the responsible person can check that recovery reached the intended wallet. Treat extended public keys as sensitive financial information because they can reveal linked activity within the branches they cover.
6. Explain the first transfer. Identify who approves it, how to verify the recipient's address independently, and how to fund network fees. A small test transfer can confirm receipt before a larger distribution, although it does not prove the recovery environment is secure or protect later transfers from address substitution.

Rehearse with a separate practice wallet containing no meaningful funds. Have the chosen person locate the instructions, explain the access process, and recover that practice wallet with the proposed helper or guide. Never use a published example seed for real assets. Update the documentation whenever the wallet structure or storage arrangements change.

FAQ

Does my executor need to understand cryptography?

No. They need sound judgment, reliable records, and enough understanding to supervise recovery and recognize when qualified help is necessary.

Should I give them my seed phrase now?

Not automatically. Immediate access may create immediate spending capability, depending on passphrases, multisignature requirements, and other spending conditions. Choose storage and release arrangements that support both confidentiality and timely authorized access.

Can I split the words between two people?

An improvised word split can weaken security and complicate recovery. If shared control is necessary, evaluate a documented threshold backup or multisignature arrangement and rehearse its recovery process. A threshold backup divides recovery material into shares; multisignature requires multiple signing keys. They have different compatibility and backup requirements.

Sources

- BIP39: Mnemonic code for generating deterministic keys (github.com)
- BIP32: Hierarchical Deterministic Wallets (github.com)
- Bitcoin.org: Securing your wallet (bitcoin.org)

> Continue reading on bip39-phrase.com: How to View Your Seed Phrase in MetaMask, Trust and More
> More on this topic: Seed Phrases

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 since	2 seminar	3 blind
4 cotton	5 bachelor	6 silent
7 erosion	8 badge	9 slogan
10 claw	11 chair	12 deal

Example 2		
1 gate	2 ranch	3 silent
4 napkin	5 quick	6 general
7 visit	8 express	9 height
10 device	11 laptop	12 evoke

Example 3		
1 maid	2 attend	3 response
4 shy	5 rebel	6 half
7 slim	8 relax	9 hunt
10 twist	11 reflect	12 artwork

Example 4		
1 agree	2 auto	3 awake
4 before	5 april	6 eyebrow
7 merit	8 nuclear	9 market
10 tired	11 hockey	12 strategy

Example 5		
1 unhappy	2 dove	3 rotate
4 few	5 mercy	6 thing
7 runway	8 judge	9 physical
10 galaxy	11 under	12 pink

Example 6		
1 twice	2 hurry	3 inch
4 tube	5 chuckle	6 depth
7 broccoli	8 lunch	9 member
10 pattern	11 method	12 only

Example 7		
1 much	2 title	3 armed
4 record	5 tip	6 turkey
7 twenty	8 unit	9 problem
10 system	11 exist	12 orange

Example 8		
1 purse	2 across	3 dilemma
4 true	5 drip	6 general
7 creek	8 aerobic	9 foot
10 recycle	11 neck	12 arrange

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	since	1609	1610	11001001001
2	seminar	1564	1565	11000011100
3	blind	190	191	00010111110
4	cotton	390	391	00110000110
5	bachelor	137	138	00010001001

#	Word	Index (0-2047)	Word no.	11 bits
6	silent	1603	1604	11001000011
7	erosion	613	614	01001100101
8	badge	139	140	00010001011
9	slogan	1631	1632	11001011111
10	claw	336	337	00101010000
11	chair	302	303	00100101110
12	deal	449	450	00111000001

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): c938705f18611390d3288bcbe540971c`

This sequence ends in the checksum bits 0001, but SHA-256 of its entropy starts with 0101, 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

- Letter of Instruction for BIP39 Seed Phrases · June 14, 2026
- Liana Wallet: Timelocked Recovery Paths Explained · January 16, 2025
- Understanding Seed Phrases · June 9, 2025
- BIP-39 SEED PHRASE The Principles of Cryptographic Backup and Wallet Recovery · June 10, 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/