Broken Phone Screen: Getting Into Your Wallet

November 23, 2026 · Document #437 · bip39-phrase.com



Photo by Elena Mozhvilo on Unsplash

Recover a wallet after a broken phone screen using a compatible backup, and understand when mirroring or data-preserving repair can help.

Contents

Restore the wallet without the damaged phone	2
When screen mirroring can help	3
Repair, verification and securing the old phone	3
FAQ	4
Sources	4
Sample sequences of BIP39 words	5
Reading a BIP39 phrase	6
See also	7

A broken phone screen does not necessarily mean a lost wallet. For a self-custody software wallet with a usable backup, restoring on another trusted device is often the most practical recovery route. Screen mirroring is a fallback, and it helps only when the phone still runs and the necessary connections and permissions work. ([support.metamask.com](https://support.metamask.com/configure/wallet/using-the-same-metamask-wallet-on-multiple-devices/?utm_source=openai))

Restore the wallet without the damaged phone

A software wallet manages signing keys; a hardware-wallet companion app may hold no private keys itself. Your assets remain recorded on their networks. A compatible backup can restore access without using the damaged phone, but separately imported keys may need separate backups. ([support.metamask.com](https://support.metamask.com/configure/accounts/how-to-add-missing-accounts-after-restoring-with-secret-recovery-phrase?utm_source=openai))

First, identify your wallet's recovery method. Many wallets use a **BIP39 recovery phrase**, commonly 12 or 24 words, but not every wallet does. Some use another mnemonic format, encrypted backups, a connected hardware wallet or account-based recovery. An exchange account generally requires the provider's account-recovery process instead. Follow the original provider's recovery instructions. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

1. Find your original offline backup and identify the wallet app. Do not type the words into a website, support chat, search box or screen-sharing session.
2. Use a trusted replacement device. Install the authentic wallet through the developer's official distribution channel, checking the publisher rather than following an advertisement.
3. Select the wallet's restore or import option. Enter the words in their original order, privately and without photographing them. For a hardware wallet, follow its device-specific recovery instructions.
4. If you used a BIP39 passphrase, enter that too. It is separate from the phone PIN and the app's local unlock password.
5. Enable the correct networks and accounts. Compare addresses with your own previous records, and check whether separately imported accounts need restoring. ([support.metamask.com](https://support.metamask.com/configure/wallet/using-the-same-metamask-wallet-on-multiple-devices/?utm_source=openai))

A standard BIP39 phrase contains 12, 15, 18, 21 or 24 words. It derives a 512-bit seed using PBKDF2-HMAC-SHA512 with 2,048 iterations. Its checksum detects many transcription errors, not all. Every passphrase produces a seed, so a mistyped passphrase can open an unrelated, empty wallet without a BIP39 password-error warning. A valid checksum does not prove that you entered the original phrase or passphrase. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Wallet compatibility also matters. BIP44 defines paths structured as `m / purpose' / coin_type' / account' / change / address_index`, with purpose set to `44'`; apostrophes mark hardened derivation. Other schemes use different purposes or structures. If accounts are missing, check the original wallet's recovery documentation, including address discovery limits. Multisignature recovery may also require configuration data and enough other signers. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki))

When screen mirroring can help

Mirroring can help if the phone is running but its display is unusable. Ordinary mirroring tools do not bypass device encryption or an unknown unlock code, and cannot display a phone that is not running. Some wallet screens may also block capture. ([developer.android.com](https://developer.android.com/tools/adb))

- If the image is visible but touch is broken, a compatible USB mouse through an adapter may let you enter the unlock code and operate the wallet. Support depends on the phone, adapter and accessory security settings. ([samsung.com](https://www.samsung.com/us/support/answer/ANS10002919/?msockid=3e33945c4f2f66ab233782014e2d6723&utm_source=openai))
- If the display is black, wired video output may work on models that support it. A USB-C connector alone does not guarantee video output; check the phone's specifications and the adapter's power requirements. ([samsung.com](https://www.samsung.com/us/support/answer/ANS10002919/?msockid=3e33945c4f2f66ab233782014e2d6723&utm_source=openai))
- Wireless mirroring can require setup, pairing or on-screen approval. Check the requirements for your phone and receiver before relying on it after the display fails. ([github.com](https://github.com/Genymobile/scrcpy))
- Android computer-control tools commonly depend on Android Debug Bridge, or ADB. USB debugging must be enabled for ADB over USB, and the computer must be authorized. A previously unauthorized computer normally triggers an approval prompt on the phone. Some tools offer input-only modes without debugging, but these do not mirror the display. ([developer.android.com](https://developer.android.com/tools/adb))
- iPhone computer access can likewise depend on unlocking the device and confirming trust. Connecting a cable does not automatically grant access to wallet keys or a usable wallet backup. ([support.apple.com](https://support.apple.com/en-ie/109054?utm_source=openai))

Use only a computer you control. Mirroring software, remote-support sessions and screen recording can expose an unlocked wallet or displayed recovery words. Avoid enabling debugging merely because an unsolicited "recovery technician" requests it. ([github.com](https://github.com/Genymobile/scrcpy))

If you regain control, follow the wallet's documented backup procedure privately. Do not assume that copying app files or completing a general phone transfer produces a usable wallet backup; confirm what the wallet actually supports. ([support.metamask.com](https://support.metamask.com/configure/wallet/using-the-same-metamask-wallet-on-multiple-devices/?utm_source=openai))

Repair, verification and securing the old phone

If there is no usable backup and no workable external display, preserving the original phone becomes important. Stop using and charging it if you suspect battery damage, swelling or overheating. Do not charge a wet device. For liquid damage or boot failure, seek qualified repair before further power-on attempts. ([support.apple.com](https://support.apple.com/en-ie/guide/iphone/iph301fc905/27/ios/27?utm_source=openai))

Tell the repairer that preserving data is essential. A screen replacement may retain wallet access; a factory reset erases local data, and replacing the mainboard generally leaves the original data on the old board. Modern encryption can prevent accessing that data by moving storage alone. Do not give a repair shop your recovery phrase. Arrange to enter the unlock code yourself where possible. ([support.apple.com](https://support.apple.com/guide/security-pdf/data-protection-sece8608431d/1/web/1?utm_source=openai))

Restoring a phrase **does not revoke the old phone's keys**. For a conventional seed-based wallet, if the old keys may be exposed, create a new wallet with a newly generated backup on a trusted device and transfer assets after verifying the destination. Account for fees, tokens, multiple networks and accounts, and positions that need separate handling. Changing the restored app's PIN does not rotate blockchain keys. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Do not erase the damaged phone until you have verified recovery and secured any other necessary data. Once recovery is confirmed, erase the old device using its manufacturer's procedure where possible. If it cannot be erased, secure it until data-preserving repair or appropriate disposal is arranged. ([support.apple.com](https://support.apple.com/en-mide/guide/deployment/dep0a819891e/1/web/1.0?utm_source=openai))

FAQ

Can I recover without the phrase?

Possibly, if the original wallet remains accessible or another documented recovery method exists. With neither accessible signing keys nor a usable recovery method, recovery may be impossible. ([support.metamask.com](https://support.metamask.com/configure/wallet/using-the-same-metamask-wallet-on-multiple-devices/?utm_source=openai))

Why is the restored wallet empty?

Check the phrase, BIP39 passphrase, network, account index and address type. Different derivation paths show different addresses, and separately imported keys may need restoring individually. A valid checksum does not rule out a phrase error. ([github.com](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki))

Should I share my screen with wallet support?

Never while entering recovery words or exposing private keys. Do not send those secrets to support staff; legitimate troubleshooting does not require you to disclose them. ([support.metamask.com](https://support.metamask.com/configure/accounts/how-to-add-missing-accounts-after-restoring-with-secret-recovery-phrase?utm_source=openai))

Sources

- BIP39: Mnemonic code for generating deterministic keys (github.com)
- BIP44: Multi-Account Hierarchy for Deterministic Wallets (github.com)
- Android Debug Bridge (adb) (developer.android.com)

> Continue reading on bip39-phrase.com: What Is a Seed Phrase? How a Recovery Phrase Works
> More on this topic: Recovery

Sample sequences of BIP39 words

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 blossom	2 achieve	3 ahead
4 voyage	5 fortune	6 castle
7 trade	8 first	9 sweet
10 bar	11 mention	12 record

Example 2

1 loud	2 pyramid	3 iron
4 evoke	5 achieve	6 tribe
7 setup	8 above	9 lady
10 canyon	11 task	12 require

Example 3

1 net	2 afford	3 humble
4 castle	5 account	6 base
7 work	8 change	9 just
10 success	11 sing	12 crash

Example 4

1 enter	2 detail	3 project
4 fruit	5 world	6 pitch
7 include	8 ocean	9 universe
10 jewel	11 inspire	12 motor

Example 5

1 lab	2 just	3 style
4 lazy	5 spare	6 rack
7 boring	8 sausage	9 craft
10 census	11 salmon	12 truck

Example 6

1 hill	2 crowd	3 magnet
4 absorb	5 concert	6 february
7 jungle	8 depth	9 suspect
10 insect	11 torch	12 then

Example 7

1 renew	2 stamp	3 flag
4 awkward	5 affair	6 advice
7 right	8 patient	9 strike
10 swap	11 educate	12 first

Example 8

1 dignity	2 mule	3 situate
4 notable	5 review	6 other
7 control	8 style	9 eternal
10 latin	11 twenty	12 prepare

Example 9

1 mesh	2 wife	3 column
4 guess	5 improve	6 season
7 series	8 include	9 camp
10 field	11 shy	12 want

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	blossom	192	193	00011000000
2	achieve	14	15	00000001110
3	ahead	41	42	00000101001
4	voyage	1968	1969	11110110000
5	fortune	732	733	01011011100
6	castle	284	285	00100011100
7	trade	1845	1846	11100110101
8	first	699	700	01010111011
9	sweet	1757	1758	11011011101

#	Word	Index (0-2047)	Word no.	11 bits
10	bar	147	148	00010010011
11	mention	1112	1113	10001011000
12	record	1438	1439	10110011110

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): 18003814fb05b84739aabbdba24e2c59`

This sequence ends in the checksum bits 1110, 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

- How to Stamp Seed Words into a Steel Plate · November 3, 2026
- Your Wallet Vault Inside Phone Cloud Backups · December 22, 2025
- Twelve Words, Infinite Responsibility: A Conversation About BIP-39 · June 26, 2025
- The Twelve Words Between You and the Void · June 27, 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/