Common Mistakes When Recovering A Seed Phrase

Jeff Hong ⋮ 8-10 minutes

You go to recover your seed phrase and enter your seed phrase into a wallet...uh oh, you get an error.

Or, it recovers something unexpected (e.g. no coins).

What happened?

Well, that's what we're here to try and find out. Let's get into some common overlooked mistakes when recovering your seed phrase.

Seed Standard

Your seed phrase most likely comes from a standard known as **BIP39**.

BIP stands for **B**itcoin **I**mprovement **P**roposals. BIPs are documentation for features, ideas, information, changes, improvements, etc. for how Bitcoin works.

Each of these BIPs are designated by a number.

BIP39 or Bitcoin Improvement Proposal: 39 is one of the many design ideas that was approved by an economic majority of the Bitcoin community and became a standard for many popular wallets.

BIP39 is the use of a mnemonic phrase -- a group of easy to remember words -- to serve as a back up to recover your wallet and coins in the event your wallet becomes compromised, lost, or destroyed.

The BIP39 documentation describes the specific steps a wallet must take (i.e. algorithm) to create this mnemonic phrase. This includes specific requirements, structure, practices, words, etc.

There are other standards such as:

- Lighting Network Daemon (AEZeed): If you're using the Lightning Network Daemon wallet, it uses a different seed scheme known as AEZeed.
- Electrum: If you're using the Electrum Wallet, it also uses a unique seed scheme.
- Satoshi Labs Improvement Proposal (SLIP 39): If you're using Trezor's parent company, Satoshi Labs, unique seed standard of Shamir Secret Shares, SLIP 39.

For these unique standards, they can only be recovered on wallets that support that standard. If your wallet does not "understand" how your seed phrase created, it will not understand how to recover it either.

For BIP39, it is the most widely used and most wallets support this standard.

Your best bet is to recover your seed phrase on the wallet you originally used to generate it.

Wrong Words

The words in your seed phrase aren't just any random words. They are pulled from a specific list of 2048 words known as the BIP39 wordlist. The words in the list are in alphabetical order.

Check your seed phrase to ensure each word is in this wordlist.

Also, there are **no two words** in this list with the same first four (4) letters. In other words, if you know the first four letters, you know the rest of the word by looking for those first four letters in the BIP39 wordlist.

If there is a word not in the list, you might be able to check which word it should be from the first four letters.

Misspelled Words

As we mentioned above that the words in your seed phrase BIP39 wordlist. Check the spelling of each word to ensure it matches the exactly the spelling in the wordlist.

Some words are uncommon which you may be unfamiliar with. For example, the word "satoshi" in the wordlist.

There are some words that might be spelled differently than what you're used to. For example, the word "artefact". *Artifact* is the preferred spelling in American dictionaries, but *artefact* is the British/Australian spelling.

There are many words that sound similar with only a single letter difference. For example, "aware" and "awake" or "vote" and "note". "See Similar Words in the BIP39 Wordlist".

And again, if there is a misspelled word, you may be able to get a clue of what word it should be from the first four letters.

Too Many/Little Words

Count the number of words in your seed phrase.

For BIP39, there is a designated number of words allowed in a seed phrase.

You may have only 12, 15, 18, 21, or 24 words.

The most common length seed phrases are 12 and 24 words.

Ensure you're not missing a word or have too many.

Invalid Last Word (Checksum)

The last word of BIP39 seed phrase is called a **checksum** (well "part" of it to be accurate).

In general, the purpose of a checksum is to detect errors in a set of data.

In the case of a seed phrase, the purpose of the last word is ensuring your seed phrase is following the "rules" and structure described in the BIP39 standard. It is calculated from the

initial data used to generate your seed.

If you're wondering why the seed phrase you made up worked in a wallet you've used before, per the BIP39 documentation, "*Although using a mnemonic not generated by the algorithm described in "Generating the mnemonic" section is possible, this is not advised and software must compute a checksum for the mnemonic sentence using a wordlist and issue a warning if it is invalid.*"

This means that a wallet will not outright reject an invalid seed phrase, rather it will accept it and should only give you a warning (which is up to the developer's discretion).

You **cannot** chose any 12-24 words and have a valid seed phrase due to the last word acting as the checksum.

If you "made your own" seed phrase without properly calculating the last word, this could be the reason you've recovered an empty wallet.

Or, if you're getting an invalid error, most likely the last word is incorrect.

Passphrase

A passphrase is *different* from your 12-24 word seed phrase. It is an optional, advanced security feature that allows you to create a new wallet by adding an additional word to a 12-24 seed phrase. It is supported by many wallets utilizing the BIP39 standard.

Think of it as an additional word to your seed phrase that can be (almost) anything. (A-Z, a-z, 0-9, special characters i.e. ASCII characters.)

Your seed phrase by itself is technically a wallet with an empty ("") passphrase. And as such, is a valid wallet. Adding a passphrase creates a **different** brand new wallet on top of your seed.

Thus if you utilized a passphrase when generating your seed phrase, it will not recover the same wallet if you recover with only the seed phrase.

Most wallets by default will have the passphrase option turned off. You may have to manually enact the feature and enter your passphrase to recover your coins

Derivation Path

There are also BIP standards that your wallet uses when receiving coins.

These standards are called derivation paths and are a "map" telling your wallet where to find your coins. The most common ones are described in BIP44, BIP49, and BIP84.

Your wallet must support the same derivation path that you've been using (i.e. "have the map") to "store" your coins.

Whether a wallet supports a certain derivation path should be well documented or referenced on their website.

If another wallet does not support a derivation path that your original wallet supported, that doesn't mean your coins are lost. It simply means you're unable to access them (because it doesn't know how to find them!).

Again, the most probable way to recover your coins is to use the same wallet you recovered on. Some wallets will require you to "re-add accounts" with the different derivation paths.

See, "What is a Derivation Path?" for more details.

Coin Support

You might have noticed that not all wallets support all coins.

Your wallet must not only know how to find your coins but also support the coin you're trying to find.

Coin types are the cryptocurrencies (e.g. bitcoin, ethereum, etc.)

Coin support should be well documented or referenced on the wallet developer's website. Again, if a wallet does support a specific coin, it doesn't mean they are lost. You'll need to find another wallet that does in order to access them again.

Some wallets will require you to re-install the app associated with the type of coin you've stored.

Malicious Wallet

This is the worst case scenario.

Basically, the wallet you used sole purpose is to steal your seed phrase.

Ensure you're using a reputable wallet.

Many scammers will try to impersonate reputable well-known developers.

When downloading wallets from developers websites, ensure the URL that you're using is the correct one. There might be a slight typo in spelling or a reputable sounding URL that's not the developers website.

Entering your seed phrase into any website is already a security risk and a common way to "send" your seed phrase elsewhere.