The Best Seed Phrase Storage

Jeff Hong ⋮ 11-13 minutes

What is Seed Phrase Storage?

Seed phrase storage refers to securely copying/writing your **seed phrase** on a medium (such as paper) in effort to store and preserve that data in the long run. Your seed phrase (also known as recovery phrase, seed phrase, recovery seed, mnemonic seed, wallet backup, etc.) is an ordered set of 12-24 words that is randomly generated by your wallet. It stores the information that can be used to recover your wallet when your wallet fails unexpectedly (such as damage, unable to access, misplaced, theft, etc). Ensure it is hidden in a secure location and stored/written on something that will last your lifetime.

Storing Your Seed Phrase

I'll make it clear right now.

There is **no** best seed phrase storage or best way to store your seed phrase. (I know, *how dare you*)

Why? Because seed phrase storage is unique to you.

Like many things in life: something that works for you, might not work for someone else. Everyone is different.

Seed phrase storage is specific to what works for you and your situation.

We'll go over some of the most popular ways to store your seed phrase and help you figure out what works for you.

For information on where to store your seed phrase on (i.e. physically location), see Where to Store Your Seed Phrase.

Online (Anything with an Internet Connection)

Typing your seed down into anything connected to the internet exposes your seed to a plethora of unknown threats and possibilities (such as malware, viruses, unauthorized access, etc.)

Anything connected to the internet includes your computer, phone, any cloud storage, etc.

You may not know who has access to your information and by the time you notice, it might be too late.

The purpose of a hardware wallet is to store your private keys offline. A seed stored online defeats that purpose.

It's highly recommended not to do this. There is no best way, but this is definitely the worst way. You might as well have left your coins on an exchange if you decide to do this.

Best for: No one. Leave your coins on an exchange at this point. You'd probably be better off.

Paper & Pencil

Writing down your seed phrase on a piece of paper will probably be the first thing you do before considering other methods.

Obviously paper is not very durable. It gets wet, it burns, it gets torn up.

But, more likely is paper to be lost or thrown away.

When was the last time you forgot where that one note was. Did you accidentally throw it away?

To prevent a single point of failure, having another copy in different location will prevent loss if the other copy is destroyed or misplaced.

The downside of this is obviously a higher chance of someone else finding it. It's a balance between security and accessibility. It's up to you how many copies you'd feel comfortable with.

Consider making new copies every few years and destroying the old ones. Not only does this gives you a refresher of where you put those copies but it replenishes the structural integrity of the paper and legibility of the writing.

For more information on preservation of writing on paper, see here.

Best for: If you're looking for easy, simple but with some maintenance over time

Metal

Putting your seed phrase on metal is a popular choice when combating the elements of time and mother nature.

It's strong, durable, and resistant to moisture and heat.

Psychologically, it's not as often to be thrown away (I mean, looks at your parents. They probably have physically "junk" hoarded for *years*!).

But due to being physical, storing your seed phrase on metal can again, be a single-point of failure. Having another copy will help but also again increases the chances of being found.

Although, there is no need to make new copies and can be relatively worry-free in terms of physical deterioration.

Be careful when choosing a metal. You want a metal than can withstand a house fire (over 1200°F) and have relatively good corrosion resistance.

Corrosion is the deterioration of the material due to a chemical reaction between the metal and its environment. One of the most common forms is iron oxide. The iron present in the metal interacts with the oxygen in water or air to create iron oxide or that brownish-red stuff better known as rust.

Stainless steel (300 series) is a good option and is a great balance between cost and durability. Stainless steels are composed of at least 10.5% chromium. Chromium reacts with the oxygen in the air to create a regenerative protective layer (chromium oxide) thats prevents the underlying metal from corroding (even after getting damaged). Stainless steel has a melting points well above 1200 °F (2750 °F).

Titanium is also a good but more expensive option. Titanium provides better corrosion resistance to more harsh environments and a bit higher melting point (3038 °F) than stainless steel.

For a do-it-yourself option, metal stamping or hand engraving are popular options. Metal stamps, engravers, and metal plates can be found at hardware stores or online marketplaces.

For commercial options, Jameson Lopp reviews many seed storage devices and tests them for crush, heat, and corrosion resistance. He also has a very thorough article in terms of what he believes are the characteristics of the best seed phrase storage design based on his extensive experience testing them.

Keep in mind, the “cooler” your seed storage looks, the more likely it’ll be seen as interesting enough to ask about or valuable enough to take. There’s a difference between clean (legible) and fancy.

Best for: If you're looking for little more effort/cost but peace of mind durability and longevity wise.

Splitting It Up

You might have heard of some people "spitting" their seed words by separating some portion of the words and putting them on different pieces of paper. Thus, you would need put the splits together to get your seed phrase.

This requires you to keep track of multiple splits and locations.

It's not recommended you split your seed phrase in half. There is no significant benefit vs having your seed all together.

If you lose one of the splits or its stolen, that's it. Your coins are gone. It's also more likely for you to lose one of the two pieces than a single piece.

Some people have done a splitting scheme where you need a certain number of pieces in order to complete the seed (2 pieces out of 3, 3 pieces out of 5, etc.)

For example for a 24 word seed where you need 2 out of 3 pieces:

- 1st Piece: Words 1-16
- 2nd Piece: Words 8-24
- 3rd Piece: Words 1-8 and 16-24

Thus, you could lose one piece and still be able to complete your seed phrase.

This method does reduce the security of the seed if one of the pieces is found (as only 8 words need to be cracked, which can arguably take quite a bit of time). And, if you're not aware one of

the pieces is gone, they have all the time in the world. So, this is not recommended for a 12 word seed.

There are also (more advanced) hardware wallet specific options such as Trezor's Shamir Backup where their software will split your wallet for you into various pieces (or "shares" as they call them). These shares will be comprised of 20 or 33 words. You can decide how many total shares are created and how many shares you need to recover your wallet (e.g. 2 out of 3, 3 out of 5, etc).

The benefit is if you lose one of the shares you can still recover your wallet, but someone cannot brute force with a single share to get into your wallet.

The negative is this is Trezor specific and can only be done and recovered on a Trezor.

Best for: Those who want to avoid a single point of failure but at the expense of increased logistics.

Memorizing It

There's not much to say on this. Memorizing your seed phrase is probably the best way to ensure your seed cannot be found and only you know your seed.

Your seed will always be on you, yet it's never exposed. This helps especially if you're traveling or moving and need access to your wallet.

The downside is of course, forgetting your seed which is easy to do if you don't do something like recite it everyday.

Thus, it not only takes more mental effort to first memorize your seed but takes continual effort to keep it memorized.

In addition, there is the whole "$5 wrench attack", where someone can physically threaten you to reveal your seed phrase. But honestly, this is highly unlikely unless you're a high profile figure who flaunts how much bitcoin they have.

In my opinion, memorizing is great mental backup to your physical backup. Forgetting your seed phrase becomes less of an issue. It's a great method in addition to writing it down.

For more information on the best way to memorize your seed, see here.

Best for: If you're looking for the absolute way to have your seed phrase at all times without it being exposed but with more mental effort short and long term.

Digital

When I say digital, I mean storing your seed phrase on a memory storage device (such as a SD card, USB drive, external SSD, CD, etc.).

This takes some knowledge and know-how to do securely without compromising your seed on an exposed device(e.g. using an encrypted bootable OS installed on a USB drive is the most common).

Regardless, digital storage devices (like paper) are still prone to the same physical threats as paper (physical and environmental). It can also still be physically lost.

Data loss is also a real threat. Memory storage devices don't have an indefinite lifespan. Corruption can occur due to time or damage (both electrical and physical).

It's not recommend for most people. Seed phrases wouldn't exist if the recommended way to store your seed is digital. Seed phrases were intentionally made to be written down; that's why they are words.

Best for: Experts who know what they're doing (which most likely would not be reading this)

Adding a Passphrase

Adding a passphrase to your seed phrase is a commonly suggested method to add a sort of encryption to your seed phrase.

It is an optional, advanced security feature that will create a new wallet with an additional custom word/phrase. Adding a passphrase improves security in the sense of unauthorized access to your seed but increases complexity and logistics. It can also potentially let you be a bit more lax in terms seed storage.

For more information on passphrases, see here.

Final Thoughts

The biggest threat to your seed phrase is often yourself. Not only does that include losing your seed or falling for a scam but, it includes *trying* to be more "secure".

Trying to get smarter with your security is not very smart. The next worst thing after losing your seed is being unable to access your seed.

The more layers of security and logistics you add, the more likely you yourself will get locked out of your seed phrase.

Keep it simple (for you).

Balance security with accessibility.

Be private and don't become a target.

Do as much or as little that lets you sleep at night. How you store your seed phrase is personal to you and only you can decide what that means.

For more resources and discussion on seed storage, visit www.reddit.com/r/seedstorage/