# **Private Key Storage Best Practices To Secure Your Bitcoin & Other Cryptocurrencies**

With the ever-increasing adoption of Bitcoin and the popularity of other cryptocurrencies around the world, the need for more education and reminders of proper key management to secure your private keys/seed words for any of your crypto wallets is at an all-time high.

## **When should you start to properly secure your private keys?**

Ideally, as soon as you start, even with a low amount of funds, but if you haven't already then you should up your security measures when your coins have high value, which may vary from person to person.

For example, a person might not care much about their funds if they get stolen, and may get somewhat annoyed that they lost $10 or up to $100 for example, but once they have a large sum like $1,000 or more, where they may cry because it got stolen or lost, then they'd start looking into best practices to increase the safety and security of their funds.

## **Best practice steps to generate your initial private keys/seed-words**

First things first, when you generate your Bitcoin or any other crypto wallet, the best way would be to generate it on a secure device, and the current best method to do so is on a cold storage device known as a hardware wallet. Although, if you can't get such a device, then the next best thing would be to use your (hopefully clean) mobile phone, by first downloading a known application like [BlueWallet](https://bluewallet.io/), which is a Bitcoin-only wallet, or a multi-crypto wallet like [Exodus](https://www.exodus.com/) from Google Playstore if you're using an Android device, or the App Store if you're using an iOS device.

Once you've downloaded a Bitcoin/crypto wallet app, see if you can turn off your wifi and Bluetooth (by simply going into airplane mode) before you open the application. Make sure you are in a private location like your house, nobody's around you are no cameras somewhere.

After you made sure that you're in a safe location, open up the app and generate your wallet(s), write down your private key or seed words on a piece of paper, put that paper in a small plastic bag if you have one, and then store that sensitive data somewhere that you know is safe and secure, where only you and/or a select few that you trust your funds with know.

After that, don't try to check out your seed again and start using your wallet normally.

## **General best practices on key management**

* When you create a Bitcoin/cryptocurrency wallet, your private key or seed words are what needs to be secured, and it doesn't matter whether someone knows your public key/s or not. Unless you care about privacy and want to take measures to increase that, then that's a different topic that needs a discussion of its own.
* Do not complicate things. Don't think that increasing the number of security layers, like using a multisig setup when you don't properly understand what you're doing, will help you because it will most likely harm you, where you either forget how to gain access to your private key(s)/seed-words and lose your access to your funds because of dealing with things that are more complicated than your current level of understanding.
* Test everything. Make sure that your phone is in airplane mode like seeing if you're visible on a Bluetooth scan or making a call to yourself. Make sure that the private key or seed words are written down and backed up correctly, before you put funds in it, by deleting that generated wallet and trying to restore it.
* Spend more to increase security. See if you can get a hardware wallet and have it as cold storage for your funds, to keep your private key(s)/seed words from any connection (making it an air-gapped device), as well as getting a more durable item to write down your private-key/seed-words like a stainless steel plate, one that would protect it against fire, water, shock, and bend.
* Do not store your private key/seed words in a password manager and/or on a cloud service nor your mobile or computer.

There are more things to take note of about the best private key storage and their best practices to keep them safe and secure, but these are most of the main points to consider when generating your crypto wallet. If there's still a major way that we didn't cover or know about, we'd love to hear it from you so we can update this article.