Avoiding a Seed Phrase Compromise

10/25/2024 12:30 am EDT

Safe and secure store of any wallet seed phrases should be of utmost concern to any cryptocurrency user as a breach of the seed phrase directly allows any party, anywhere in the world that happens to obtain the seed phrase to can steal all cryptocurrency from the wallet. There is no safeguard like Multi-Factor Authentication should the seed phrase be compromised, so it's users must ensure they store it securely, and keep it secure.

A seed phrase compromise can be avoided 99.5% of the time by following a few simple rules (that people who lose funds due to seed phrase compromises almost never adhere to).

1. Do not store the seed phrase online in any form. Do not email it to yourself. Do not store on your Google Drive. Don't store on your Dropbox account. Don't store in Evernote. And don't store in Google photos or iCloud photos. Don't store it even in an encrypted form online.

2. Do not enter or record the seed phrase on any digital device, even if only storing offline/locally. Don't store it on a standard USB key in a word document. Don't store it in a note file on your laptop. Don't store it in the notes on your phone.

3. Consider using a hardware wallet to ensure that even encrypted versions of the private keys are not stored locally on any internet-connected device.

4. Store the seed phrase either on a physical piece of paper, written by hand, or on engraved steel. Either way, it should be a physical form only. Whether or not a second physical copy of the seed phrase should be made is not widely agreed upon but the owner's living situation and preferences may affect what is best.

5. Ensure the seed phrase is stored in locations that won't be accidentally found or stumbled upon by a third party, but also in a location where it won't accidentally be thrown out or forgotten.