Your Secret Stash: Seed Phrases, Password Managers, and Secret Hygiene

Author	josh
Date	2024-03-24

Overview

Storing a backup of your cryptocurrency seed phrase is a crucial security practice. Every user needs a seed backup in the event the original wallet software, device, or keystore is lost. However, there are often questions as to *where* to store that seed phrase safely. Users may be curious about store seed phrases on paper, metal, or in an encrypted form such as a secure password manager. Depending on the type of wallet, where you put your backup may reduce or compromise your security. As such, it's important to understand the relationship between the type of wallet (hot or cold) you are using and appropriate backup procedures.

First, A Note on Password Managers

A *password manager* is specialized software designed for storing, generating, and even auto-filling passwords. This software is designed with the secure storage of secrets such as passwords in mind. A password manager's user must only remember one very long, strong passphrase known as a *master passphrase*. This phrase is used to *encrypt* all of the passwords and other secrets stored in the password manager vault.

A password manager is an excellent security tool, as it allows users to store much stronger passphrases than they can remember for all their different accounts. Passphrases can be randomly generated strings or even random *diceware* passwords consisting of words. These phrases are longer and stronger than typical passwords and thus less susceptible to attack. If a user's password hash is leaked from a company's database, it's less likely an attacker will *crack* that strong passphrase and take over the account.

A password manager also helps prevent *password reuse*. Since the user only has to remember their master passphrase, the password manager can store a unique passphrase for each account. If one account's password is somehow compromised, this prevents an attacker from using the password to gain access to another account. For example, using a unique passphrase prevents a breach at your electric provider from being used to attack your Coinbase account.

Password managers can be used to store more than just passwords. Many allow you to secure credit card information, cryptographic keys, notes, 2 factor backup codes, or other key data such as seed phrases.

Seed Phrases and Password Managers

Since password managers are purpose-built for storing secrets, is it wise to store seed phrase backups in them? It's certainly a bad practice to store seed phrases in *plaintext* - such as a screenshot or Google/Word document. But password managers do encrypt the secrets stored within, so what about seed phrases? The answer, like many issues of security, is *it depends.*

Generally speaking, storing the seed phrase for a *hot wallet* in a password manager is reasonably secure. To understand why it's likely okay for most use cases, we should think about the concept of hot wallets and possible attack surface for those wallets. A *hot wallet* is a crypto wallet that generates and stores the keys on a *general purpose computer* - such as a laptop or phone. These wallets include apps like Coinomi or Exodus, Electrum desktop, or the Metamask browser extension.

The key here is that storing an encrypted seed phrase in a password manager offers *roughly the same* security level/attack surface as the wallet itself. The wallet already generates the keys on a general-purpose computer, and stores the keys *encrypted* on that device (protected by a PIN, password, or other mechanism). If you store a copy of the seed in an encrypted password manager, you're also *encrypting* the keys on a general-purpose computer. In either case, a theoretical attack includes malware or some other exploit allowing an attacker to access the encrypted keys. If they can guess the password to the encrypted vault using *password cracking* techniques, they can ultimately steal the coins.

The security of your funds with a hot wallet really lies in the quality of the *master passphrase* for the wallet or password manager in most cases, so it's critical to choose a very strong, random master passphrase for your vaults.

But what about *cold wallet* seed phrases? Should you store the seed for your Trezor, Ledger, or other hardware device in a password manager? The answer is no, you should *never* store the seed for an offline wallet in a password manager.

Why is this recommendation different from that of a hot wallet? Again, the answer lies in the security level and attack surface the wallet is designed to have. The whole purpose of a hardware wallet/cold storage is that the keys are generated and stored *offline, on a single-purpose computing device.* A hardware wallet is designed to keep your crypto keys away from malware and networks, where there are more opportunities for an attacker to steal them. A hardware wallet only stores crypto keys and signs transactions offline, and does nothing else. By putting your hardware wallet seed into a password manager, you reduce the level of security to that of a hot wallet. You're now only as secure as that PC or phone, and the passphrase protecting your manager vault. You don't have *cold storage* anymore, you've effectively turned your wallet into a *hot wallet.*

Password Manager Breaches and Crypto Theft

Recent news surrounding the 2022 LastPass data breach has brought forth questions about the security of storing seed phrases in password managers. Some users of LastPass affected by this breach have reported the theft of cryptocurrency where no other avenue of compromise seems likely. So how does an attacker steal crypto from a user in this case?

In this breach, the attackers gained access to the *encrypted* password vaults. The data stored inside (passwords, seed phrases, etc.) can only be unlocked with the proper key. The *master passphrase* for the vault is used to derive the encryption key. In order to gain access to the keys, the attacker has to use *password cracking* techniques to essentially guess the right password. With a copy of the encrypted password vault available, the thieves could use specialized software to guess many possible password combinations using common wordlists or other techniques.

The critical line of defense in this case is the strength of the *master passphrase.* A master passphrase for a password manager should always be as *long and as random as possible.* The use of a long, difficult to guess sentence can make it infeasible for password cracking software to find a correct match. Users with *weak master passwords* had those passwords guessed, and once they were found the attackers could decrypt the vault and simply use the seed phrases to take the crypto in that wallet.

Seeds and Storage

When thinking about backing up seed phrases using a password manager, one must evaluate the overall security profile of their wallet. If it's a hot wallet, it is likely okay to store a copy of the seed in a password manager for safekeeping since the security level is roughly the same. For a cold wallet, it is never appropriate to store the seed in a password manager. And regardless of whether or not you choose to store seeds in a password manager, you should choose a very long, random, strong master passphrase to protect the secrets in that vault.