Swan

Swan Vault Best Practices

Securing your Swan Vault

Swan Vault uses a 2-of-3 multi-signature set-up to give you enhanced security over your bitcoin. Three private keys protect your bitcoin, and at least two keys are required to move bitcoin out of your Vault. You hold two keys using two separate signing devices, and Swan holds the third one on your behalf.

Once you've created your Vault, please follow the instructions in this guide to secure your Vault properly.

Security Items

Beyond yourself (the Bitcoin holder), there are six security items to consider. These are:

1. The Swan Vault Recovery Kit
2. Signing device A
3. Recovery phrase A (for signing device A)
4. Signing device B
5. Recovery phrase B (for signing device B)
6. Your collaborative custody partner (Swan)

Next, we will review the purpose of each security item.

Swan Vault Recovery Kit

The recovery kit is a backup of your Vault. You can think of it as a treasure map to your bitcoin, as it contains all the information to recover your Vault. We recommend printing a physical copy and either storing a digital copy in a cloud storage service such as Apple iCloud, Google Drive, Microsoft OneDrive, etc, or in a password manager.

Suppose someone gets access to just your recovery kit. In that case, they will be able to view your bitcoin balances and transaction history, but they will not be able to steal your bitcoin.

If you lose your recovery kit, log into your Swan account and download it from the Swan Vault dashboard. You can import your Vault into Specter, an open-source Bitcoin wallet software, and manage your Vault independently of Swan.

Signing device
A signing device, also called a hardware wallet, is a physical device designed to securely store the keys required to move bitcoin out of your Vault. Swan Vault is designed for use with Jade devices, which are manufactured by Blockstream, a global leader in Bitcoin technology.

You will be instructed to create a PIN during the Jade device set-up. This pin encrypts your recovery phrase and prevents unauthorized access to your Jade. If your Jade device is lost or stolen, the finder will not be able to access your device without knowing the PIN. This buys you some time to move your bitcoin to a new vault.

Recovery phrase
A recovery phrase, also called a seed phrase, is a unique list of 12 words you can use to recover your key if needed. The recovery phrase is generated during the initial set-up of your Jade device. You should write your recovery phrase in the recovery sheet that comes with your Jade. Please keep your recovery phrase secret, as these 12 words encrypt your keys. You should never share your recovery phrase with anyone, nor should you take a photo or make a digital copy.

If your Jade device has malfunctioned, you can use the recovery phrase to restore the words to a new Jade device and immediately use your existing Vault. Similarly, suppose your Jade has been stolen or lost. In that case, you can utilize the recovery phrase to restore the words to a new Jade device, and you should immediately transfer your bitcoin to a new Vault. Please get in touch with our Support team for help.

Your collaborative custody partner (Swan)
You can manage your Vault within the Swan Vault dashboard. For security reasons, please ensure your email account is secure, and your Swan account has 2FA enabled via an authenticator app.

- Swan holds one of your keys, your cloud key, on your behalf. Since Swan only holds only one key, it cannot unilaterally move your bitcoin. You have to authorize Swan to use your cloud key.
- You can use any two keys to move your bitcoin. However, for the reasons we'll explain below, we recommend you use one of your keys and authorize Swan to use your cloud key to move funds from your Vault.
- When you use the cloud key there is a 72-hour security hold period before we broadcast the transaction to the Bitcoin network.
- Swan can help you move your bitcoin to a new Vault if you lose a single security item or suspect tampering.
- If you lose these four security items: signing device A, signing device B, recovery phrase A, and recovery phrase B, Swan cannot help you recover your bitcoin. Your bitcoin will be permanently lost.

Next, we will review the best practices for securing each security item.

Best practices

We recommend storing your keys in separate geographical locations and not on the same premise. You should physically protect your security items as follows:

Swan Vault Recovery Kit	Secured in a password manager, cloud storage service, printed format, or USB drive: • Download from the Swan Vault dashboard • Copy into your password manager • Copy into your cloud storage service • Print out two physical copies and store them alongside each of your signing devices • Copy into two USB drive and store alongside each of your signing devices • To ensure that no one can copy your recovery kit without your knowledge, we recommend placing it within a tamper-proof bag • Delete your downloaded copy, including from your trash folder (MacOS), recycle bin (Windows)
Signing Device A	Secured in the first of two separate, physical locations: • A bank safe deposit box • A family member's safe (could be an heir) • A securely bolted down safe inside your primary residence • A securely bolted down office safe • A safe located in a secondary property you own
Recovery Phrase A	Secured in the same physical location as Signing device A. To ensure that no one can copy your recovery phrase without your knowledge, we recommend placing it within a tamper-proof bag
Signing Device B	Secured in the second of two separate, physical locations: • A bank safe deposit box • A family member's safe (could be an heir) • A securely bolted down safe inside your primary residence • A securely bolted down office safe • A safe located in a secondary property you own
Recovery Phrase B	Secured in the same physical location as Signing device B. To ensure that no one can copy your recovery phrase without your knowledge, we recommend placing it within a tamper-proof bag

Physically separating your keys this way reduces the risk of single-point-failure due to malicious (e.g. theft) and non-malicious (e.g. natural disaster) attack vectors. With this setup, any single location can be compromised, and you can still recover your bitcoin.