How to Keep Your Private Keys Safe

One of the common ways to keep your private keys safe is by generating and printing a paper wallet. This cold wallet storage is immutable to cyber-attacks, but it also puts a lot of value (and future potential value) into something that cannot be recovered if it is lost. Not to mention the inefficiency of then needing a secure location to store the paper wallet, like a safe or a safety-deposit box.

Another common means of storage for private keys is on your phone or computer. Whilst it is a convenient way to access and move your funds, it is considered a hot wallet. Attempting to keep your private keys safe by leaving them on an internet-connected device leaves you open to hackers, phishing scams, viruses, and other malware.

The best method to keep your private keys safe lies in an offline storage device. The Secure Wallet combines the best of hot and cold storage to provide unparalleled security with the convenience of a bank card. The wallet is never connected to the Internet, however, you can interact with it wirelessly through the companion app. This lets you choose how and when to use the wallet, and provides a means to recover your assets if you lose the device.

Key Security Features of the Secure Wallet

* CC EAL5+ certified- the highest security standard for government level deployments.
* Truly portable- does not require a wired connection as with other cold storage devices.
* One-time-password generator. This additional security feature means that every transaction leaving the wallet has to be physically confirmed by you, the owner.
* Convert your crypto from within the app itself, so you never risk losing your tokens on an exchange.
* Zero fees to move your assets (other than standard blockchain mining fees).
* Up to 4 weeks of battery life per charge, 15 degrees of flex, waterproof and incredibly durable