What's the difference between a hot and cold wallet?

10/25/2024 12:29 am EDT

A hot wallet is a type of self-custodial wallet whereby the private keys are stored in some form (usually encrypted) on an internet-connected device. Desktop wallet clients and mobile wallet applications are generally both examples of hot wallets since in the local installation files, they contain (usually) encrypted versions of the private keys needed to send transactions.

A hot wallet is less secure than a cold wallet because if most thefts occur via a compromise of the seed phrase or the applicable private keys. If there are no private keys or seed phrase on any electronic device in any form, then it is impossible for a hacker to remotely obtain such information that would result in the wallet being compromised.

A cold wallet is a type of self-custodial wallet whereby the private keys are not stored on any internet-connected device. Hardware wallets such as Ledger, Trezor and Ellipal are prime examples of cold wallets since the private keys stay on these devices, which do not directly connect to the internet, and such private keys cannot be exported, apart from using the backup seed phrase that is initially provided when the user sets up the wallet.

For this reason, cold wallets are considered to be more secure than hot wallets. Nonetheless, how secure a specific cold wallet is will depend on the operational security practices the owner utilizes.