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

Last Modified on 08/19/2026 9:04 pm PDT

A **hot wallet** is a cryptocurrency wallet that stores or accesses the private keys needed to send transactions on an internet-connected device. Desktop wallets, mobile wallet apps and browser-extension wallets are common examples. Hot wallets are convenient because they make it easy to send, receive and manage cryptocurrency.

The downside is that hot wallets have more exposure to online threats. Malware, phishing attacks, malicious browser extensions or a compromised computer or phone could potentially expose the wallet's private keys or recovery phrase. If an attacker obtains this information, they may be able to access and transfer the cryptocurrency stored in the wallet.

A **cold wallet** keeps the private keys separated from the internet-connected device being used to manage the cryptocurrency. Hardware wallets such as Ledger, Trezor and ELLIPAL are common examples. Transactions are typically signed inside the hardware wallet, meaning the private keys do not need to leave the device or be exposed to the connected computer or phone.

Cold wallets are generally considered more secure against remote attacks because the private keys are kept isolated. However, the wallet's **seed phrase or recovery phrase** must still be protected carefully. Anyone who obtains the recovery phrase may be able to restore the wallet on another device and gain access to the funds.

For this reason, cold wallets are often preferred for storing larger amounts of cryptocurrency or funds that will not be used frequently. Hot wallets may be more convenient for everyday transactions, while cold wallets provide an additional layer of protection for long-term storage. Regardless of the type of crypto wallet used, security ultimately depends on protecting private keys, recovery phrases and carefully reviewing transactions before approving them.