

Secure your crypto in 10 steps

Shellcrew Vault · shellcrew.com

- ☐ 01 **Crypto from an exchange to your own wallet**
An exchange can fail, freeze your account or be hacked. On your own wallet the funds are yours for as long as you hold the keys.
- ☐ 02 **A hardware wallet, not an app**
The key never leaves the device. A computer with a virus can do nothing with it. Trezor, BitBox, Coldcard: buy straight from the maker, never second-hand.
- ☐ 03 **Your seed on steel, not on paper**
Paper burns and gets wet. A steel plate for a few dozen euros survives a house fire.
- ☐ 04 **A copy in a second place**
One copy is no copy. The second should sit where the same fire, thief or flood can't reach it.
- ☐ 05 **Nobody sees the seed, not even us**
You enter the words only on the hardware wallet. Never on a website, in an app, in an email, or "for verification" to someone from support.
- ☐ 06 **A 2-of-3 wallet for larger amounts**
Three keys in three places, two needed for a transfer. Losing one changes nothing, and a thief with one sends nothing.
- ☐ 07 **A recovery test before you deposit**
Restore the wallet from the backup on an empty device. If it fails, better to find out now than after a loss.
- ☐ 08 **A small amount as a trial**
The first transfer to a new wallet should be small. Move the rest only after a successful recovery test.
- ☐ 09 **Instructions for your family**
Someone close should know that the crypto exists, where the keys are and what to do step by step. No amounts, no seed in the text.
- ☐ 10 **A review once a year**
New phone, new software version, a move. Once a year repeat the recovery test and check that the instructions still fit.

Shellcrew Vault isn't an exchange, a wallet or an investment adviser, and doesn't store clients' keys. This list is general. shellcrew.com · contact@shellcrew.com