

The Bitcoin security checklist

Twelve points. Tick what is already in place; the rest is your to-do list.

Most of what people lose in bitcoin is not lost to the market. It is lost to a phrase nobody wrote down, a backup nobody tested, a password reused across accounts, or a message that looked real. Security rests on habits, not on a tool, and there is no password reset, no customer service and no appeal. **Doing these twelve things removes most avoidable losses.**

THE TWELVE POINTS

- ☐ **1 My seed phrase is written by hand on a durable medium. It is not photographed, and not in an online service, an email or a notes app.**
The phrase is the wallet: it rebuilds every key. A copy sitting in a photo library, an inbox or a notes app is a copy that anyone reaching that account can use.
- ☐ **2 I keep two copies, in two different places.**
A single copy kept beside the device is a single point of failure. One fire, one flood or one burglary takes the device and the backup together.
- ☐ **3 I tested a full restore before depositing a significant sum.**
A backup that was never tested is an assumption. Many people find out that a word is missing, unreadable or out of order on the day they need it. The test costs ten minutes.
- ☐ **4 I enter my phrase on no website and tell it to no one. No legitimate support asks for it.**
The phrase alone moves the funds, from anywhere in the world, and the transfer cannot be reversed. Legitimate support never needs it; a request for it is the request itself that gives the scam away.
- ☐ **5 I use an email address reserved for my platform accounts.**
Customer lists leak. In December 2020 one wallet maker's stolen database was published online, and those customers then received fake messages demanding their 24 words. A reserved address makes an unexpected message stand out.
- ☐ **6 Each account has a unique password, kept in a password manager.**
One password reused across accounts turns a single leak elsewhere into access here. A manager is what makes unique passwords practical rather than theoretical.
- ☐ **7 Two-factor authentication uses an app or a physical key, not SMS.**
A code that arrives by text can be asked of you by whoever calls, and that is exactly what fake support does. Never read a code to anyone who contacts you.
- ☐ **8 Before a withdrawal, I check the start, middle and end of the address, then send a small amount first.**
Some malware replaces the address you pasted, and scammers plant lookalike addresses in your history with a tiny deposit. Only the start and the end match, so the middle is what catches it.
- ☐ **9 My devices and software are up to date and downloaded from the official source, whose address I type myself.**
A sponsored link or a lookalike domain can put a copy of the app in front of you: one digit standing in for one letter is enough. Type the address yourself, or use a bookmark you saved earlier.
- ☐ **10 When the platform allows it, only withdrawal addresses registered in advance are permitted.**
If someone takes over the account, a list of addresses approved beforehand means the funds cannot be sent to an address of the attacker's choosing.
- ☐ **11 I do not talk about my holdings, online or around me.**
What people know about you is used to deceive you, or to find you. Discretion is a protective habit, exactly like a strong password.
- ☐ **12 A way to pass things on exists, and the person named knows what to do.**
Without the phrase nobody has access; with the phrase anybody has. Separate the explanation from the secret, never put the phrase in a will or a letter, and check that the person named can say what they would do.

IF SOMETHING GOES WRONG

1. **Stop all payments.** Pay no "release fee", no "tax", no "last deposit". Being asked to pay before you can withdraw is a scam signal, not a formality.
2. **Call your bank or card issuer at once** if a bank transfer or card payment is involved. Use the number printed on your card or statement. Fast action can sometimes stop or flag a payment.
3. **Keep everything.** Messages, website addresses, destination addresses, statements, screenshots. Evidence collected on the first day is the evidence that still exists later.
4. **Report it to your local police** and to your **national financial regulator**, which keeps warning lists and registers of authorised providers. Many countries also run a cybercrime or fraud reporting centre. A police report creates an official record that other bodies often require.
5. **Tell the platform or exchange you used.** It can sometimes freeze an account, and its records may help investigators.
6. **Expect to be contacted again** by people offering to recover your money for a fee paid in advance. That is a second scam aimed at the same victim. Real recovery starts with your bank and the police, never with a stranger's invoice.

Names and services differ by country. Search for your own national police, regulator and fraud-reporting service, and use the contact details printed on official sites you reach yourself.