Twitter Thread by Ben Kaufman



Ben Kaufman
@_benkaufman



I've received many questions lately, but by far the most common question is “What's the best way to secure #Bittcoin?”

■So here’s a thread with my opinion on securing #Bitcoin

The first thing to understand is that there’s no "best way", but always a tradeoff.

You can always find ways to make it harder for someone to get your #Bitcoin, but if you over-complicate it, you could end up making it even too hard for yourself - many lost their funds this way.

Your goal should be to balance usability and security the way which works best for you.

This means very different things for different people, depending on your technical experience, understanding of Bitcoin, how much you are holding, etc.

For some, that means leaving Bitcoin on an exchange.

I strongly recommend at least learn to hold your own keys before buying, but if you can’t wait, it’s better to leave it there than holding yourself if that’d make you feel like you have no clue what’s going on.

If you feel ready to take self-custody, you could start with a hot wallet on mobile or desktop. That’s a good step forward, as it means you’re holding your own keys. But this introduces some more new concepts you should get familiar with.

So before doing that, make sure first that you know the basics: how to send and receive, test out with small amounts, try deleting everything and restoring from backup, then continue with real funds, just go at your own pace and don’t rush with what you don’t understand.

Next option is using hardware wallets. This should still be manageable for most “normal” people, without great effort, but again introduces more complexity.

You should make sure to never enter your backup words on a computer, learn to verify addresses on the device, and so on.

If you got that and feel ready to go further to upgrade your security, the next step is learning to use your own node.

Using your own node is an important improvement in terms of security and privacy, as you cease to rely on 3rd parties for interacting with the Bitcoin network.

Without using your own node, you're relying on someone else to interact with the network.

That someone could:

- Know which txs you're interested in - privacy issue
- Provide false information - security issue
- Go/ get shut down - resilience issue

Using your own node fix this

If you have reached this far - using a hardware wallet with your own node, you already made enormous progress. By this point, you should already have some understanding of what’s an xpub, how to verify an address, and why those things are important.

The next step is exploring the different types of hardware devices.

Here again, there are many options and a lot to learn, like supply chain attacks, retirement attacks, and other security concerns. You might come up with different answers for your specific needs.

You should pay extra attention to the trust issue of using just a single option, especially in the case of consumer hardware wallets.

You can consider using an airgapped laptop or an old phone to mitigate that, but there are pros and cons for any choice.

That’s why the final step I could recommend to explore here is using a multisig wallet.

Multisig lets you mix different devices to reduce trust in each one of them, and in case one is compromised - you are still in control of your funds.

There are more options along this scale with different tradeoffs, you could use a hardware wallet with a passphrase, you could do a guided multisig setup with some service provider, and many other options.

My suggestion is to find your personal point where you feel the balance between usability and security matches your needs best.
I just outlined the order I would sort by the most common approaches from the most user-friendly to the most security-minded, now it's on you to choose.

So take your time to learn, read, test, and understand the tradeoff and pitfalls. Ask questions, make sure you know what you’re doing, play with small amounts, then upgrade, just go at your own pace and continuously improve your security.

And just to clarify, I'm not a security expert, just a pleb sharing some experience.

Most cases I've seen of losing funds were because holders didn't care to understand what they use or backup properly, so that's why I warn mostly on that, but DYOR.

Stay safe, stack sats.