Twitter Thread by Ben Kaufman



Ben Kaufman
@_benkaufman

■Thread: 10 Rules for Verification on a #Bitcoin Hardware Wallet ■

Rule #1: DO NOT TRUST THE COMPUTER SCREEN.

The very reason for using a hardware wallet is that your computer IS compromised, trusting it makes using the hardware wallet an expensive security theatre (or 2FA at best).
Always verify on the HWW device screen!

Rule #2: Verify your "receive" addresses BEFORE accepting funds.

A compromised computer can be tricked into displaying addresses that belong to an attacker. The only way to make sure you own the addresses is to display them on the HWW device and verify they match.

Rule #3: Verifying change address should be done by the device when sending funds, not before like receive addresses!

It is pointless at best, and misleading at worst, to verify them beforehand like receive addresses...

All hardware wallets support verifying the change address belongs to you AT TIME OF SIGNING A TRANSACTION. Verifying before that is pointless and error-prone.

Now let's talk some multisig...

Rule #4: Verify the xpub of each hardware wallet used in a multisig quorum on the device it belongs to.

This is not 100% mandatory - but if you're no expert - you really should do it.*

*If a hardware wallet doesn't support displaying the xpub, (like Trezor), it could be fine to just verify each address on it - so long as you verify consistency on all other devices as well, but I wouldn't recommend such a device for non-experts.

Rule #5: Verify "receive" addresses on EVERY device of the multisig quorum.

This is especially true for at least one address (see next rule) but recommended for all. If using a device that you haven't verified the xpub of on-screen, you should verify all receive addresses on it!

Rule #6: While it is best to verify each receive addresses on ALL devices in the multisig setup - you might choose to trust a specific one, verifying the xpub/ first address on all - then the rely only on the "trusted" device - ONLY IF YOU ALSO VERIFY XPUBS...

By that, I mean verify on the "trusted" hww used for general verification, that the xpubs are consistent for all cosigners.
This is needed only once with wallets like ColdCard, Cobo Vault, Bitbox02, and Specter DIY - since they allow saving the multisig xpubs on the device.

With Trezor T - you have to verify the xpubs of cosigners every time - which is why it's not recommended for that purpose - with Trezor One it's simply not possible...

So while you might use a Trezor in a multisig, I would not recommend it to non-experts.

Rule #7: Do NOT use Ledger in a multisig setup! (unless you are an expert or have a very good reason...)

Ledger currently does not allow verifying multisig addresses on the device - nor displaying the XPUB on its screen.

This means you have no way to verify it was not swapped by an attacker in your multisig setup - EVEN IF YOU DO A SUCCESSFUL TEST TRANSACTION!

It is still possible for a (very) sophisticated attacker to make you think it worked, while it was him signing for you...

Rule #8: For convenience, you may print out/ write down a large batch of your receiving addresses - verify all at the same time, and rely on that paper list for your day to day verification.
This is very useful for multisig! - where devices might be distributed in various places.

Rule #9: Multisig change verification should be the same as with Rule #3 - on the device at the time of signing.

Popular devices (besides Ledger as said), can verify that the address you send from and the change address used belong to the same multisig wallet (from same xpubs).

If they fail to verify the change address - they will show it as a standard, independent, recipient - in that case YOU SHOULD NOT MAKE THE TRANSACTION.
This is valid for both single sig and multisig! (although even more relevant for the latter).

Rule #10: Hardware wallets cannot verify your balances - and that's great!

Verifying balances requires getting information from the Bitcoin network - i.e. you need to be online - which would make hww more vulnerable...
This is where a full node comes in!

It is strongly recommended that you run your own Bitcoin full node - and use it as your main source for verifying your balances and transaction history!
For redundancy, you could double-check against block explorers or another node (use a different device for either!).

One last thing: These rules apply to any device you use as a segregated signing device - be it a "traditional" hardware wallet, an airgapped laptop, a mobile phone etc.

If you want to separate your keys without having a security theatre, you should verify on your signing device!

Please note: Some things here might not be fully accurate for the expert user (especially around multisig address verification), but for the less advanced users' sake, I have tried to be on the safe side when things get tricky...

That said, if you see inaccuracies or mistakes (or just have questions), please comment!!

Also check out some more info on multisig setups over at:
https://t.co/dwsl52QeD8 (@mflaxman guide)