

Forum:[Hack Forums](#)

Thread: [entering to a Trezor hardware wallet](#)

SIM-3336514 - January 27, 2022, 1:40 am

just found on youtube, keep ur wallets safely, if anybody got their hands on or steal ur wallet its possible to get in to funds.

guy explains how to bypass power off features & entering to debugging & coping memory & entering. interesting

<https://www.youtube.com/watch?v=dT9y-KQbqi4>

BrainDD - January 27, 2022, 2:25 am

i have never understood why one would use a hardware wallet its one of the most stupid ideas i every heard since i started into crypto last year.

Physical device can be stolen corrupted or broken and for me its very hard to just keep in a safe place, we don't have safety deposit boxes for example...i maybe because im new to this but i prefer custom encrypting the keys and putting them in a text file and Veracrypt it with a long and strong password and email the file to my self and all my friends has more chance to recover the wallet in 5 years than a hardware wallet.

shreder - January 27, 2022, 1:54 pm

(Jan 27, 2022 03:25 AM)BrainDD Wrote: [\[CITE\]](#) i have never understood why one would use a hardware wallet its one of the most stupid ideas i every heard since i started into crypto last year.

Physical device can be stolen corrupted or broken and for me its very hard to just keep in a safe place, we don't have safety deposit boxes for example...i maybe because im new to this but i prefer custom encrypting the keys and putting them in a text file and Veracrypt it with a long and strong password and email the file to my self and all my friends has more chance to recover the wallet in 5 years than a hardware wallet.

If you have no clue what you are talking about then don't talk. Hardware wallet stops your private key from getting exposed.

IQhacker - January 27, 2022, 3:02 pm

I still prefer the Ledger wallet x

T0Bi - January 27, 2022, 3:07 pm

(Jan 27, 2022 03:25 AM)BrainDD Wrote: [\[CITE\]](#) maybe because im new to this but i prefer custom encrypting the keys and putting them in a text file and Veracrypt it with a long and strong password and email the file to my self and all my friends has more chance to recover the wallet in 5 years than a hardware wallet.

Definitely because you're new to this and don't know/understand how hardware wallets work.

So to clarify a few things for you:

A hardware wallet (like all other wallets) has a seed phrase. It has 12-24 words and should be stored securely (like you store your private key). If you ever lose/break/what ever your hw wallet, you can always use the phrase to recover everything.

A hardware wallet (e.g. Ledger Nano X) has a 8 digit pin code and deletes itself after 3 wrong entries, so losing it isn't that tragic.

They biggest risk with having a private key like you is how are you going to use it?
Unless you have an air gapped pc and sign your transactions offline, your key will be exposed once you load it into a wallet.

You cannot be sure that your PC is not infected and the only way to not expose your private key is either an airgapped PC or a hardware wallet.

So for people who'd like to actually use their crypto, a hardware wallet is a must have.

Additionally, a hardware wallet is fantastic to check the tx before signing it without the possibility of an attacker changing the address without you noticing.

BrainDD - January 28, 2022, 5:24 am

(Jan 27, 2022 02:54 PM)shreder Wrote: [\[CITE\]](#) If you have no clue what you are talking about then don't talk. Hardware wallet stops your private key from getting exposed.
thanks i'm aware of that but the cons of owning one outweigh the pros.

(Jan 27, 2022 03:44 PM)Beau Wrote: [\[CITE\]](#) You are new to this.

A vetted and secured hardware wallet even if stolen would not do much since it would not be vulnerable to physical attacks. Additionally, the thief would need the PIN to unlock the hardware wallet to sign any transactions. You would need to protect the physical seed from adversaries, but it's much easier to protect (and conceal) the physical seed than an electronic device.

To supplement what [shreder](#) posted. It's better saying "I don't know" rather than jumping to silly conclusions due to a lack of comprehension.
thanks beau i like your name, i have some knowledge & searched into this and watched a lot of coinbureau & others in depth boring video that explains all sort of wallets before jumping into crypto, check out my replay to T0Bi

(Jan 27, 2022 04:07 PM)T0Bi Wrote: [\[CITE\]](#) Definitely because you're new to this and don't know/understand how hardware wallets work.

So to clarify a few things for you:

A hardware wallet (like all other wallets) has a seed phrase. It has 12-24 words and should be stored securely (like you store your private key). If you ever lose/break/what ever your hw wallet, you can always use the phrase to recover everything.

A hardware wallet (e.g. Ledger Nano X) has a 8 digit pin code and deletes itself after 3 wrong entries, so losing it isn't that tragic.

They biggest risk with having a private key like you is how are you going to use it?
Unless you have an air gapped pc and sign your transactions offline, your key will be exposed once you load it into a wallet.

You cannot be sure that your PC is not infected and the only way to not expose your private key is either an airgapped PC or a hardware wallet.

So for people who'd like to actually use their crypto, a hardware wallet is a must have.

Additionally, a hardware wallet is fantastic to check the tx before signing it without the possibility of an attacker changing the address without you noticing.

thanks for the in depth explanation, all of you guys have a valid point but owning a hardware wallet is just a big NO for me, even if no one could break into it,

its a physical proof that im owning crypto, in my case and my country i could go to jail.

in other cases:

<https://futurism.com/robbers-tortured-man-drill-steal-cryptocurrency>

<https://twitter.com/bantg/status/1338607596803137537>

+physically storing keys is not a possibility to everyone:

https://www.reddit.com/r/ledgerwallet/comments/qgr0zd/ledger_wallet_hacked_over_20k_gone/

or its just wont work for whatever reason (like what happened to omni)

i prefer my method of storing the keys instead of a pre-made one,

for example radix: i installed a clean windows system that is connected to a physical PFSENSE firewall device & Spyshelter firewall software & shared 4g internet from my phone with no other thing installed except radix wallet,

split my tokens accross multiple validators and closed the software, i toke that hard drive and plugged it into my original ssd and gave the access to the usb only to the virtual machine,

from the clean installed windows on virtual machine i converted the whole system into an ISO file and veracrypted it, then toke the final encrypted file and split it with winrar to 2 separate zip files with different password than veracrypt password, then i wiped all the radix drive using DBAN.

then i toke one of the zip files and put it in the drive with many porn videos, and created new folder named thumbnail and put few pictures in it along with the zip file with different .ico and locked the thumbnail folder using ATTRIB command

the drive is named rdx porn and its an intel SSD S4500 series with the HIGHEST TBW(i doubt it will fail) has 1 zip file & 2nd zip is stored on a google drive email im not using for anything.

if i had a memory loss i doubt i be able to recover that system myself. and if anyone was able to get the keys before i split the system i wont be mad he deserves it.

With the video SIM shared & all of this in mind you guys should know that the government have their top-notch Engineers and developers i bet they already cracked into at least the top 2 hardware wallets.

think about this in case things went south for you...

Blue Eye Samurai - January 28, 2022, 5:41 am

This is very old though, the trezor had firmware dated back from 2017 when this exploit was still possible. this was already fixed in end 2017

?Ñâzg?l - January 29, 2022, 11:36 am

(Jan 27, 2022 03:25 AM)BrainDD Wrote: [\[CITE\]](#) i have never understood why one would use a hardware wallet its one of the most stupid ideas i every heard since i started into crypto last year.

Physical device can be stolen corrupted or broken and for me its very hard to just keep in a safe place, we don't have safety deposit boxes for example...i maybe because im new to this but i prefer custom encrypting the keys and putting them in a text file and Veracrypt it with a long and strong password and email the file to my self and all my friends has more chance to recover the wallet in 5 years than a hardware wallet.

Corrupted and/or broken? no big deal use your seed phrase and you can recover all your funds if it's stolen however you must act fast if the thief is smart enough to break into the wallet

