

# Forum:[Hack Forums](#)

Thread: [Securing your wallet.](#)

**Gunrox** - June 17, 2017, 6:43 am

This is one of the most important things you can do when it comes to dealing with any amount of bitcoin/crypto currency. You wouldn't hand your wallet to someone and give them the pin numbers to your debit and credit cards. Would you? So there are some very easy to do steps that everyone should take to ensure that your hard earned money stays safe.

Multi wallet system.

You don't carry around your life saving in your pocket everyday, most likely you keep it in a bank. You withdraw small amounts as needed from ATM or bank teller. This same concept should be applied when dealing with cryptocurrency. Keep a spending wallet and a savings wallet this simple step could save you large sums of money if something is compromised. The larger sum should be kept offline with thumb drives being so cheap store and encrypt the wallet with large sums on a USB thumbdrive. Use it to add funds to your spending wallets as needed.

Back up your wallet.

I can't stress the importance of wallet backups enough. Being digital, wallets are subject to being lost if your hard drive becomes corrupt or you have a hardware failure. This would be really unfortunate if you had this happened and didn't have a backup to restore from. A good way to handle backups is you make an encrypted backup using your wallet. Store it on a USB thumbdrive in a fire proof box with your other important documents. You can also produce a paper copy of your wallet which is just a printed version of your address and private key. I would highly recommend that you compress the backups and password protect the zip file for another layer of protection.

Another good thing to look at would be offsite online storage. I would use a company that is most likely going to stand the test of time and be around for more than a few years. Services like google drive who will most likely always offer their service. Just upload the password protected backup to your cloud storage option and BOOM you have a secure offsite storage for free.

It is very important you use password/passwords or phrase that you will never forget. Once you encrypt your wallet that's it there isn't an undo button.

Be sure to make this process part of your regular routine, making backups of all your wallets regularly will save you heart ache in the future.

Encrypt your wallet.

Encrypt all of your wallets even on your mobile phone. It may seem like a pain in the neck when you want to transfer Bitcoin but it will ensure that no one but you can authorize a transaction. One less thing to worry about when you misplace your phone at the bar, or on the train.

Be sure you NEVER forget your password you should pick something that you are likely to remember for years. Because there isn't a password recovery system for lost or forgotten passwords. Make sure you select a good and strong password as well.

If your computer is compromised with keylogging viruses, the party who infected your computer has

the password you used to encrypt your wallet.

Be sure you keep virus software updated and full scans regularly.

Keep your software up to date.

Make sure that you don't neglect to update wallet software to help prevent issues with active wallets. New software releases can provide fixes for discovered vulnerabilities that you can take advantage of if you are updated.

Conclusion.

This is a very exciting and easy financial platform to get wrapped up in, the ease of use and convenience.. But you need to not forget the importance in safeguarding your assets. With the value expected to increase significantly it would be in your best interest to tell loved ones where and how to access your backups so if something were to happen to you those assets aren't lost for good.

<https://allcryptotalk.com/index.php?/topic/209-securing-your-wallet/>

**Kill Joy** - June 17, 2017, 2:27 pm

I had a thumbdrive back in the day with about \$50 on it if I remember correctly. It failed/broke and I no longer use that for storage. From my personal experience I don't recommend it.

**Gunrox** - June 17, 2017, 2:28 pm

(Jun 17, 2017 02:27 PM)Kill Joy Wrote: [\[CITE\]](#) I had a thumbdrive back in the day with about \$50 on it if I remember correctly. It failed/broke and I no longer use that for storage. From my personal experience I don't recommend it.

Always a possibility for that to happen. You could've stored it somewhere else as well just to take extra precautions, but again that isn't my place to judge. Thank you for giving the positive feedback & criticism.

**Kill Joy** - June 17, 2017, 2:31 pm

(Jun 17, 2017 02:28 PM)Gunrox Wrote: [\[CITE\]](#) Always a possibility for that to happen. You could've stored it somewhere else as well just to take extra precautions, but again that isn't my place to judge. Thank you for giving the positive feedback & criticism.

Yes, it was my fault for not keeping extra backups. But that was back in the day when this was all new. Keep up the HQ posts. ;)

**NightForce** - June 17, 2017, 2:32 pm

Great post Gunrox, really informative. I was thinking of getting the Ledger usb.

**Gunrox** - June 17, 2017, 2:38 pm

(Jun 17, 2017 02:32 PM)NightForce Wrote: [\[CITE\]](#) Great post Gunrox, really informative. I was thinking of getting the Ledger usb.

Ledger's hardware wallets are architected around "secure elements" or secure chips. This is the same technology that find in chip and PIN payment cards or SIM cards. These chips bring guarantees against physical attacks and raise the level of security of your private keys. I would only purchase this if you're a hardcore trader/investor. If you want to purchase it, its your call, there are things to consider though.

There is only one con with this device and it's the lack of support for passphrases other than that and affordable safe.