

FireToken Tutorial

NANO LEDGER IS NOT AN AIR-GAPPED WALLET



Hello FireToken Community

In this tutorial, our team will go over Air-Gapped Wallet setup and the security benefit of an air-gapped wallet (Also called Cold Storage)

Air-Gapped wallet is a type of storage system for cryptocurrencies. The term Air-Gapped describes the nature of its connectivity to the Internet. The wallet private key is generated offline and the transactions are never signed while the wallet is connected to the Internet.

The most common misconception is that a HardDrive Storage such as Ledger Nano is a Air-Gapped Wallet. However, IT IS NOT AN AIR-GAPPED WALLET.

When you plug the HardDrive wallet into your Internet connected computer, you connect the Hard Drive wallet to the Internet and thus risking the possibility of compromising your cryptocurrency. Yes, it is harder to compromise a HardDrive wallet, but a monitoring malware can easily monitor your online activity while the HardDrive wallet is connected to your online computer and steal you private key.

Once your private key is stolen, it **doesn't matter** if your HardDrive wallet is connected to the internet or not. The thief and unlock your blockchain wallet using any online wallet services such as blockchain.info or [MyEtherWallet.com](https://myetherwallet.com) and steal your fund.

The Best way to store your cryptocurrency safely is to set up a Cold Storage Wallet, also known as Air-Gapped Wallet.

This tutorial will show you how to set one up an securely store large amount of cryptocurrency without worrying about your account being hacked. IT IS **IMPOSSIBLE** TO WIRELESSLY HACK A COLD STORAGE WALLET.



So how do you set up an air-gapped wallet?

Here are what you need in order to set up an air gapped wallet:

- 1) 2 computers (1 must be capable of online connection)
- 2) A flash drive
- 3) A wallet service
- 4) A safe place where you can storage your written down private keys
- 5) A person, preferably you for the most secured setup

1) Why do you need 2 computers? because you will need to have 2 wallet interfaces. One computer will be completely OFFLINE and never be connected to the Internet again during the course of its duty as an Air-Gapped Wallet Storage. the term air-gapped literally means there is an air gap between the computer and the internet. This computer is where you will create your wallet and write down your private key. Because the wallet was created offline, the private key is completely safe as it was never exposed to the internet. Why does it matter? many malware can monitors your online activity, this includes screen monitoring, keyboard recording... If you think your internet activity history is private, you have no idea.





2) You will also need a Flash Drive. This could be any flash drive. It's best to buy them in bulk and replace them once in a while for additional security measure.



3) A wallet Service. Many wallet services offer Cold Storage capability. Do a little bit of research and see which one will fit your need. For this tutorial we will be showing you how to set one up using MyEtherWallet, this will only be applicable for Ethereum. Bitcoin, Monero and many other cryptocurrency are available as well from many other wallet services that offers Cold Storage capability.



4) A safe place to store your written down private keys. This step is not technically required but highly recommended in the event you are the forgetful type. Or with recent example of unexpected death, which resulted in your next of kin unable to recover your cryptocurrency wealth.

5) A person. For security reason, the best person for this job should obviously be you. But let say you are running a multi-million dollars operation and simply cannot do this on a daily basis, a trust-worthy person also works fine. This person serves as a physical link to transfer data (unsigned transactions and signed transactions) between your two computers, using the flash drive.



Also use only one tech guy when you spared no expenses



The FUN part: Setting it all up.

Download MyEtherWallet Zip files into your flash drive, using your online computer.

PLEASE VERIFY THAT YOU ARE DOWNLOAD THE REAL ZIP FILE.


Here is the link to the Zipfile on GitHub, but don't talk my word for it. Somebody could've phish this tutorial and replaced the link as well. Always practice safe security measures when it comes to money.

<https://github.com/kvhnuke/etherwallet/releases/tag/v3.21.12>

Transfers the file over and install MyEtherWallet into your offline computer using the flashdrive. NEVER CONNECT YOUR OFFLINE COMPUTER ON THE INTERNET.

Once you install MyEtherWallet in your offline computer, you can launch it using your web browser just as you are online. Did i mention to never connect your offline computer to the internet? Turn off wifi, bluetooth, file sharing... and keep them off.

DON'T GET PHISHED, please! 🙏 Thank you! 🙏
1. BOOKMARK MYETHERWALLET.COM 2. INSTALL EAL or MetaMask or Cryptonite

 MyEtherWallet

3.21.12 English Gas Price: 41 Gwei Network ETH (myetherapi.com)

The network is really full right now. Check Eth Gas Station for gas price to use.

[New Wallet](#) [Send Ether & Tokens](#) [Swap](#) [Send Offline](#) [Contracts](#) [ENS](#) [DomainSale](#) [Check TX Status](#) [View Wallet Info](#) [Help](#)

Create New Wallet

Enter a password

Do NOT forget to save this!

Create New Wallet

Already have a wallet somewhere?

- Ledger / TREZOR / Digital Bitbox / Secalot : Use your **hardware wallet** . Your device is your wallet.
- MetaMask Connect via your **MetaMask Extension** . So easy! Keys stay in MetaMask, not on a phishing site! Try it today.



You can now generate your wallet offline. Because your wallet is now generated offline, you are no longer running the risks of any malware sending sensitive information to unauthorized sources and compromising your account private key.

Make sure you physically write down your private key and store them somewhere safe. Create multiple wallets and switch them occasionally to increase your security measure. They are free to created and free to use, why not create 10,000 wallets?



Do not use your printer, writes down your private key on a piece of paper and put it in your safe deposit box. Do not takes picture of it and stores it on your phone either. Definitely do not store it on your Air-Gapped computer. If you really need to print them, use the flash drive to transfer the file over to the printer.

You are now ready to use your cold storage wallet! Launch your operation and direct fund into your wallet public addresses, switch between multiple wallets occasionally to maintains good security practice and discard them as you please.

On the next section, we will discuss the process of signing your transaction offline and broadcasting it on your online machine.



SIGNING TRANSACTIONS:

To retrieve your fund from your Air-gapped wallets, you need to copy and transfer the address you would like to send your fund to your flashdrive (receiver of your fund)

(*This particular step is only relevant for Ethereum, but you need to find your nonce number and the gas price as required by the network. You can do so on your ONLINE machine, visit MyEtherWallet and enter your Cold Storage Wallet PUBLIC address here)

New Wallet Send Ether & Tokens Swap **Send Offline** Contracts ENS DomainSale Check TX Status View Wallet Info Help

Generate & Send Offline Transaction

Step 1: Generate Information (Online Computer)

? From Address

0xDECAF9CD2367cddb726E904cD6397eDFcAe6068D

Generate Information

Now, using your OFFLINE machine, launch MyEtherWallet offline interface and navigate to SEND OFFLINE tab on the top menu.

DON'T GET PHISHED, please! Thank you!

1. BOOKMARK MYETHERWALLET.COM 2. INSTALL EAL or MetaMask or Cryptonite

MyEtherWallet 3.21.12 English Gas Price: 41 Gwei

The network is really full right now. Che

New Wallet Send Ether & Tokens Swap **Send Offline** Contracts ENS DomainSale Check TX Sta

Generate & Send Offline Transaction



Scroll down to “ How would you like to access your wallet?” You can enter your private key here. HERE AND ONLY HERE at your OFFLINE computer is where it is safe to enter your private key. There should never be a time you need to enter your private key online unless you plan to never use that wallet ever again.

How would you like to access your wallet?

- ☐ MetaMask / Mist
- ☐ Ledger Wallet
- ☐ TREZOR
- ☐ Digital Bitbox
- ☐ Secalot
- ☐ Keystore / JSON File ?
- ☐ Mnemonic Phrase ?
- ☒ Private Key ?
 - Parity Phrase ?

Paste Your Private Key

✖ This is not a recommended way to access your wallet.

Entering your private key on a website is dangerous. If our website is compromised or you accidentally visit a different website, your funds will be stolen. Please consider:

- [MetaMask](#) or [A Hardware Wallet](#) or [Running MEW Offline & Locally](#)
- [Learning How to Protect Yourself and Your Funds](#)

If you must, please double-check the URL & SSL cert. It should say <https://www.myetherwallet.com> & **MYETHERWALLET INC** in your URL bar.

Private Key

As you can see, even MyEtherWallet gives you a similar warning regarding the use of private key. Your private key can be use to access your fund by anyone if you are careless enough to enter it online even in the safest website. FIRETOKEN WILL NEVER ASKS FOR YOUR PRIVATE KEY. Once you entered your private key ONLINE, that wallet is no longer safe to use.

Once you enter your private key in the OFFLINE computer MyEtherwallet interface, it will unlock the function below.

Generate Transaction

Raw Transaction

Signed Transaction



You will need to fill out all the required informations for your transaction such as your receiver address, the value you would like to send, the gas limit (21000 average) and the gas price (41,000,000,000 average), the nonce number will also need to be entered. This is your output transaction number. The number will increase with each output transaction you create. (0>1>2>3>4...) You are still in your OFFLINE computer.

Step 2: Generate Transaction (Offline Computer)

To Address

0xDECAF9CD2367cd6397eDfCae6068D



Value / Amount to Send

01110000011100100110100101110110011000010110001101111001

ETH ▾

Gas Limit

21000

Gas Price

41000000000

WEI ▾

Nonce

1

After all required informations are entered, scroll down and click on the “Generate Transaction” button. FIRETOKEN WANTS TO REMIND YOU THAT YOU ARE ON YOUR OFFLINE COMPUTER THIS WHOLE TIME.

Generate Transaction

Raw Transaction

```
{"nonce":"0x00","gasPrice":"0x098bca5a00",  
"gasLimit":"0x5208","to":"0xDECAF9CD2367cd  
bb726E904cD6397eDfCae6068D","value":"0xa0d  
4304d9e322c2d4e0a8bc08785caef98ee71f59e8a0  
326a2081bc40000","data":"0x","chainId":1}
```

Signed Transaction

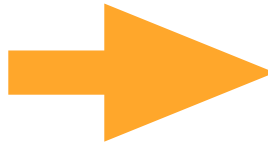
```
0xf8828085098bca5a0082520894decaf9cd2367  
cd6397edfcae6068d9ea0d4304d9e  
322c2d4e0a8bc08785caef98ee71f59e8a0326a2  
081bc400008026a0548929cc0519e8eaaca2  
088cc826e459c7798ccfc48e0bab7c815a7b1b50
```



Copy the strings of number code into your flashdrive, removes it from your OFFLINE computer when you have it saved in your flashdrive.

Signed Transaction

```
0xf8828085098bca5a0082520894decaf9cd2367
cddb726e904cd6397edfcae6068d9ea0d4304d9e
322c2d4e0a8bc08785caef98ee71f59e8a0326a2
081bc40008026a0548929cc0519e8eaacaaaca2
088cc826e459c7798ccfc48e0bab7c815a7b1b50
```



Move over to your online computer and visit myetherwallet.com. Extract the strings of code from your flash drive using COPY and PASTE function. Enter the code into your broadcast box and broadcast your transaction to the Ethereum Network. (Different cryptocurrencies will have different nodes you can broadcast your transactions from, and multiple wallet services will have this option as well in their WATCH ONLY wallet interface)

Step 3: Send / Publish Transaction (Online Computer)

Paste the signed transaction from Step 2 here and press the "SEND TRANSACTION" button.

Signed Transaction

```
0xf8828085098bca5a0082520894decaf9cd2367cd
bb726e904cd6397edfcae6068d9ea0d4304d9e322c
2d4e0a8bc08785caef98ee71f59e8a0326a2081bc4
0008026a0548929cc0519e8eaacaaaca2088cc826
e459c7798ccfc48e0bab7c815a7b1b50a050174060
5c557c8e45722ac9540fcc393ca69cb4a29a7a2741
22c79c91f3d262
```

Send Transaction





FireToken Team has show you how to set up a Cold Storage, Air-Gapped Wallet. The steps will be slightly different for each cryptocurrency and different wallet services but the concept stays the same. YOUR PRIVATE KEY IS STORED OFFLINE, THE TRANSACTIONS ARE SIGNED OFFLINE. Your private key is never exposed to the internet, thus keeping your fund safe from any remote or unwanted monitoring for malicious intents.

Certain wallet services also utilizes multi-signature system for their Air-Gapped wallets. This system enable the wallet to have 2 wallets (or a combination of wallets but 2 interfaces), one for WATCH ONLY which is their online computer, and other one for COLD STORAGE which is our OFFLINE AIR-GAPPED computer. This resulted in the fund amount being split into multiple wallets when the transaction is broadcasted. The wallet balance will show the correct amount, but the fund will not be present in the wallet address, as shown in the diagram below:

