

# 5 basic steps to protect your BitCoin account

When reading this article, many people will wonder what BitCoin is? It can be said that BitCoin is one of the best ideas ever in the virtual market, this is a system to use and convert virtual money units into real money, operating under a trade model. commercial, has a very high stability before so far ...

**TipsMake.com - When reading this article, many people will wonder what BitCoin is? It can be said that BitCoin is one of the best ideas ever in the virtual market, this is a system to use and convert virtual money units into real money, operating under a trade model. commercial, highly stable beforehand.** With BitCoin account, you can send and receive money with anyone in the world from your computer without using any banking services. In the following article, we will introduce you some of the most basic operations possible to protect BitCoin accounts from the eyes of hackers on the Internet.

## The main problem: your money can be lost anytime!

In essence, the BitCoin application stores all user account information in a file named wallet.dat. Like other normal data files, during the entire operation, this file is unencrypted and can be 'peeked' by hackers at any time. And so, we can easily link the concept of security and usability. If you have enough knowledge and experience to participate in BitCoin, the information below may not be unfamiliar, but as an argument that has existed for a long time, the more carefully protected things are, it is attracting the attention of everyone, and the hacker is not an exception.

Imagine that there are hundreds of thousands of computers running on the Internet that use the BitCoin program, and the hackers we are talking about here are one of those users, he writes. issue a virus program with the ability to spread via email and normal forms of messages, after entering the victim's computer, the virus program will find ways to find the wallet.dat file, then sent to the hackers' prepared mailbox.

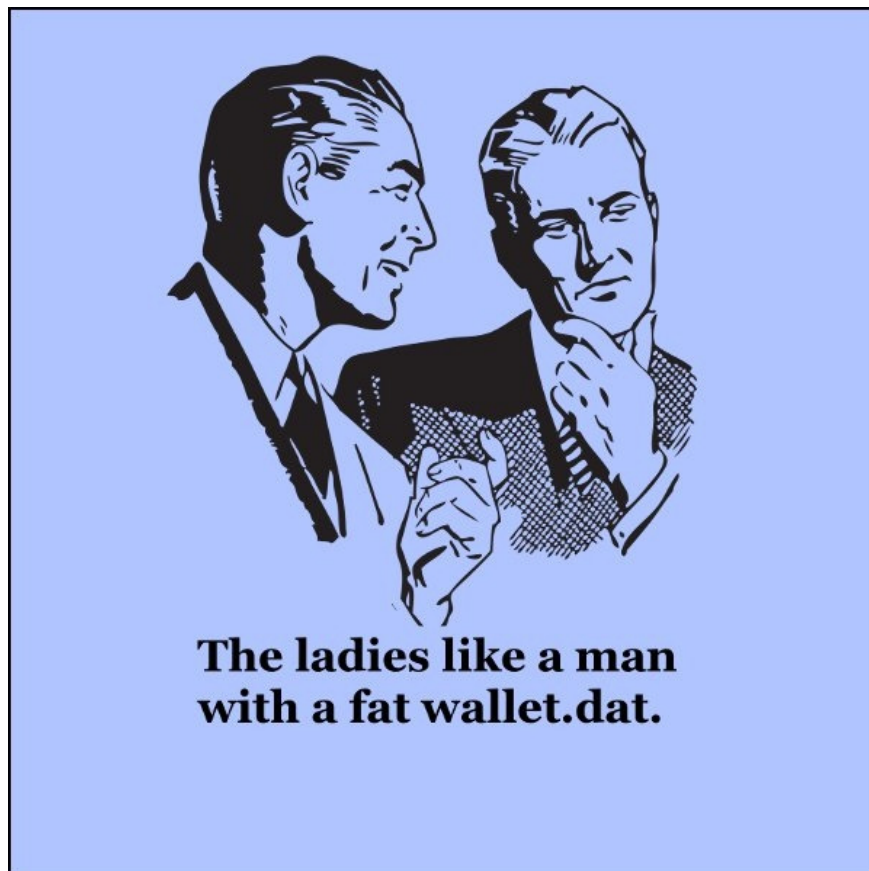
Continue to imagine that the success rate is 1%, and at the time of this writing there are about 6,809,350 BitCoin - BTC accounts in a unit of 14 \$, equivalent to a total value of 95 million USD. And the rate of 1% of the figure of 95 million USD is not small, if the hacker succeeds. According to the most recent statistics, particularly on June 14, the number of hacked BitCoin users increased dramatically, and lost about 25,000 BTC (equivalent to US \$ 350,000). And certainly this number will continue to increase if the user community does not take measures to enhance the security of their account.

## 1. Use 2 Wallet:



Because of the need to use, we can access BitCoin account at any time, above all, we must use the BitCoin program at the highest possible level. And in order to be able to receive BitCoin, we must have the wallet.dat file always in active, unencrypted state. Therefore, we use separate **bank wallet** and **operating wallet**, this concept is relatively easy to use: operating wallet will be used to receive money, and bank wallet to store. Besides, keep in mind that always keep the minimum amount of BitCoin in the **operating wallet**.

## 2. Rename Wallet file:



Regarding the operating principle, virus programs and some malicious code targeting BitCoin are to find the **wallet.dat** file. Therefore, renaming this file to any other file, eg **bank.dat** , then moving to another storage folder on the partition, just a small change like that will help We are safer in the fight with hackers.

### 3. Encrypting Bank Wallet file:



Technically, the user bank wallet should be placed in encryption mode. Currently, there are quite a lot of comments about this, such as placing the file on a partition, the encrypted drive, but in practical terms this is not feasible, because of us. can't use any device in such a way, with a workflow almost non-stop. In other cases, if the user sets the automatic mode to combine this encrypted partition into the system after rebooting, then the bank wallet file is accidentally returned to an unencrypted state. Therefore, the method of using GPG encryption is always widely used by people, this technology is based on a system that creates a public / private key, so it can be used to encrypt basic data very quickly. And with the bank.dat file encryption, even in the case of losing this file, the user can still be assured because the hackers cannot use it.

### 4. Backup Bank Wallet file:



After successfully performing the above process, we need to continue to do the next step, which is backing up the file. Users should ensure these backup files are absolutely secure in different locations on the hard drive partition. Because the wallet file is encrypted using GPG (or PGP) keys, users can use it in any way if they feel comfortable. Besides, you can consider and use Mozy tool to support online data backup process, to prevent the risk of occurrence of user data.

## 5. Do not rely too much on backup data:



We are referring to the financial-related field here, so the principle of never changing is not to trust absolutely in any form of backup! Always keep a backup copy of Bank Wallet on your device or encrypted hard drive partition, 'protect' that storage device at any cost possible, only trust yourself users should not rely too much on security banks, organizations or services.

Besides, finding BitCoin's data files on different operating system platforms is quite complicated, so we will provide the following specific path:

*Windows XP:*

*C: Documents and SettingsUSERNAMEApplication DataBitcoinwallet.dat*

*Windows Vista and 7:*

*C: UsersUSERNAMEAppDataRoamingBitcoinwallet.dat*

*Ubuntu / Linux:*

*/home/user/.bitcoin/wallet.dat*

*Mac OSX:*

*/Users/user/Library/Application Support/Bitcoin/wallet.dat*

In case your system has been compromised, please do the following:

- Create a completely new BitCoin wallet account on a secure computer
- Transfer all BitCoin to this new wallet (do not delete the wallet on the infected computer)
- Change passwords (especially passwords on encrypted hard drive partitions, some password management applications such as KeyPass and other online support services)
- Ensure the safety of Bank Wallet
- Restore the entire system

Good luck!

You finished reading the article "**5 basic steps to protect your BitCoin account**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.