PIVX Best Practices

Cryptocurrency is brand new technology that has new concepts, procedures, terminology, and security risks to learn about. Even if you are familiar with other cryptocurrency, there are some unique parts of PIVX that you may need to know.

1. Always encrypt your wallet file with a 16+ character passphrase. This will protect your PIV in case someone steals your wallet.dat file physically or digitally
2. **Always back up your wallet.dat file. Minting zPIV requires a new backup**. The software automatically does this for you, but for extra caution you can also do it manually. Replicate all new backups to all backup locations (only add to them, do not overwrite old backups)
3. Never ever delete or overwrite a wallet.dat file or your backups folder. Instead, rename the existing file and add it to your backups.
4. Do not forget your encrypted wallet's passphrase. If you do, your funds are lost. If you need to record the passphrase somewhere, make sure you use an offline, secure method that you will not lose access to and nobody else can access.
5. Do not run the same wallet in multiple locations at the same time. This can corrupt your wallet files and cause your minted zPIV to be difficult to find.
6. Do not back up your wallet.dat file to a cloud provider or shared storage without a second layer of encryption like 7zip or veracrypt container.
7. When designing your backup scheme, consider what level of protection you want for your balance. Do you have an offsite backup? Could your active wallet.dat and cold storage backups be lost to theft? Floods, tornados, hardware failure, fires, or hackers may also be things to consider.
8. Do not ever send your wallet.dat file to anyone for any reason. At best this would violate your privacy and at worst put your coins at risk. There is no support reason to request your wallet file, so if anyone asks you for this report them to the PIVX team immediately.
9. Do not ever share the information from dumpprivkey, exportzerocoins, or masternodeprivkey with anyone. This would give them access to your money. If anyone asks you for this information, contact the PIVX team immediately.
10. Do not accept or solicit support over Private Messages, this is where scammers prefer to work

Revision #1

Created 1 year ago by Danielle

Updated 1 year ago by Danielle