

Forum:[Hack Forums](#)

Thread: [How to use tor securely, a response to: "NSA wants you to use Tor!"](#)

Coiner - August 7, 2014, 2:54 am

This is a response to: <https://hackforums.net/showthread.php?tid=4377737>

While everything in that thread is true, that thread doesn't tell you everything.

First of all, that thread is only about SOCKS5 use of Tor. Hidden services are safe. However, javascript based attacks are completely different and you can secure yourself from those by using "NoScript" browser add-on.

Now, I will tell you how to use Tor securely even with SOCKS5 while browsing Clearnet. This is not free, the guide is but you need a VPS or Dedicated where you can host a Exit relay. Now when you have setup a exit relay, you look at vidalia logs. You will see something like:

Code Your Tor server's identity key fingerprint is 'Name Fingerprint'

Copy that Fingerprint and open up your torrc file. Now add these lines:

Code ExitNodes Fingerprint

StrictExitNodes 1

If possible, host and use more than one exit node but one is enough. Remember, it will take a couple hours before you are able to explicitly use your exit node because it won't be registered on the Relay list.

Now, why this works? This works, because the only way to deanonymize you is timing based attacks which are possible only when both Entry and Exit relay are controlled. Now you are using a 100% trusted exit relay(your own) and timing based attacks are now completely impossible and your anonymous once again.

Note:

Before anyone asks, this is not the same as using your VPS as SSH proxy. This is better. When using your VPS as a plain SSH proxy you are exposing your IP Address to your VPS, but this way you are not.

This is a must do for every Tor user.

jackharper - November 25, 2015, 11:57 pm

Seems worth a try. but makes me think why hasn't anyone commented on this thread

SIM-1073426 - November 26, 2015, 12:58 pm

What if someone gets control of your now 1 exit node?

__Joel - December 11, 2015, 8:48 am

Interesting share, thanks for posting this.