

Forum:[Hack Forums](#)

Thread: [What would be considered "secure"?](#)

PostSynaptic - November 10, 2018, 3:49 pm

Beginner here, just wanted to know if anybody knew how to be fully secure? Like what would be a good set up, VPN + Linux set up and what kind of browser?

Thank you

Smexy - November 10, 2018, 3:49 pm

You should use a browser like Tor to overdo security.

PostSynaptic - November 10, 2018, 3:51 pm

But aren't Tor Exit Nodes sometimes insecure themselves?

Elvira - November 10, 2018, 3:54 pm

(Nov 10, 2018 04:49 PM)Sm?exy Wrote: [\[CITE\]](#) You should use a browser like Tor to overdo security.

yes do this :D

(Nov 10, 2018 04:51 PM)PostSynaptic Wrote: [\[CITE\]](#) But aren't Tor Exit Nodes sometimes insecure themselves?

they can be, yes

sh4moon - November 10, 2018, 7:48 pm

there's no such thing as complete anonymity. but the key is to layer it. make as many points of failure as you can. here's the most secure setup I can think of off the top of my head. steal a laptop, install your os on a virtual machine, and encrypt the hard drive. you have to wipe the vm after every use. use different WiFi networks every time you go online. use tor and vpn (vpn paid for as anonymously as possible and preferably overshores). compromise a minimum of 8 different computers and install tools on them to use them as proxies.

Terry A. Davis - November 10, 2018, 9:06 pm

You'd need to invest a bit into decent privacy, make sure your stuff is encrypted so even if the feds get your hardware they can't see what's on it is a good first step

CyberStrike - November 10, 2018, 11:05 pm

Have bubblewrap/firejail a sandbox as well, a while back we had someone whom I personally believe where the sandbox saved the day from a few exploits used, against the tor browser. In all truth up to a certain point it's just mitigations, even a VM or a VM within a VM it doesn't factor in determined or well funded attackers. For example if people break into your home break your nose real quick grab up family members threaten to kill one .. I think most people would give up passwords/money under stressful situations. Never underestimate the "Rubber Hose Attack", and yes this is a valid technique in some circumstances. At this point doesn't really matter what protections are in place

Exeter - November 11, 2018, 1:04 am

There is nothing like 100% Safe, it all illusion.

FriendZone - November 11, 2018, 3:08 am

(Nov 10, 2018 04:49 PM)PostSynaptic Wrote: [\[CITE\]](#) Beginner here, just wanted to know if anybody knew how to be fully secure? Like what would be a good set up, VPN + Linux set up and what kind of browser?

Thank you

About tor remember to change some of nodes (some country are safer than others)

Then take a look here

<https://tails.boum.org/index.en.html>

PostSynaptic - November 11, 2018, 6:18 am

Thank you for all the replies :)

I've got enough to go on to at least have a relatively secure set up from all this I take it?

Of course I'm not planning anything highly illegal which will warrant any kind of investigation anyway.

Profile1 - November 11, 2018, 6:20 am

Use Tor and try not to be around viruses and programs which can be infected.

FriendZone - November 11, 2018, 6:43 am

(Nov 11, 2018 07:18 AM)PostSynaptic Wrote: [\[CITE\]](#) Thank you for all the replies :)

I've got enough to go on to at least have a relatively secure set up from all this I take it?

Of course I'm not planning anything highly illegal which will warrant any kind of investigation anyway.

If you are considering anonymity as security (vpn+linux quoting you, and it still has good safety in general) I really suggest you to check Tails maybe I didn't give you an idea of what is it.

From Wikipedia (is really clear)

Tails or The Amnesic Incognito Live System is a security-focused Debian-based Linux distribution aimed at preserving privacy and anonymity.[5] All its outgoing connections are forced to go through Tor,[6] and non-anonymous connections are blocked. The system is designed to be booted as a live DVD or live USB, and will leave no digital footprint on the machine unless explicitly told to do so. The Tor Project has provided financial support for its development

It can be still improved by the user settings anyway and some modified configurations.