

Forum:[Hack Forums](#)

Thread: [Remain anonymous while surfing the web](#)

Suppletive - May 8, 2017, 6:14 am

Hello Folks,

So I have came across internet navigation security, to be more precise, what is the best method to remain anonymous while surfing trough the Internet?

I know there's already a big discussion around this topic, however I can't find one that's concise and give the, let's not call the best, but the safest method,

Taking into the account the following methods:

- Buy VPN from a "trustable" provider;
- Rent a cloud VPS(in an "offshore" country) and run a VPN, like OpenVPN, trough the VPS;
- Socks proxy SSH tunnel to an AWS Virtual Machine.

I guess there are more methods, feel free to share them.

Im trying to get the most information as possible regarding this theme. I would appreciate if you can help me with the topic and share your substated opinions.

Have a nice day.

Stenly21 - May 8, 2017, 6:20 am

-tor

- proxy's

And for VPN's i recommend [censored] or Mullvad

Suppletive - May 8, 2017, 6:31 am

(May 8, 2017 06:20 AM)Stenly21 Wrote: [\[CITE\]](#) -tor

- proxy's

And for VPN's i recommend [censored] or Mullvad

Thanks for your answer.

However, using proxys, I think it's not a safe method, since they can be monitored by anyone. Even using proxychains and setting a couple of IPs, it's probably a risk, since someone can MITM the proxies, is my guess correct?

5chn4pp - May 8, 2017, 6:34 am

tor

that's basically everything you need.

Suppletive - May 8, 2017, 6:42 am

(May 8, 2017 06:34 AM)Satudarah Wrote: [\[CITE\]](#) tor

that's basically everything you need.

Thank you sir. I'm aware of Tor, however I would like to add more layers for security reasons, maybe it's paranoia :).

Even using TOR, if I wan't to download something, trough line command, let's say using FTP, even using Tor, I guess I will have to configure to use socks proxy trough the tor network, am I correct?

5chn4pp - May 8, 2017, 6:43 am

(May 8, 2017 06:42 AM)Suppletive Wrote: [\[CITE\]](#) Thank you sir. I'm aware of Tor, however I would like to add more layers for security reasons, maybe it's paranoia :).

Even using TOR, if I wan't to download something, trough line command, let's say using FTP, even using Tor, I guess I will have to configure to use socks proxy trough the tor network, am I correct?
If you want to download files using tor, you should use [tails](#), one of the most secure solutions.

Suppletive - May 8, 2017, 7:07 am

Thanks for your answer.

Question apart, let's imagine the following case: If you connect to an IRC channel, and you proxied trough tor network. Your IP will be masked to all the others users, however, the op's of the channel are able to see your real IP?

5chn4pp - May 8, 2017, 7:10 am

IRC is not my strong side, but if you proxy though tor, your ip should be hidden from everyone.

Faith Connors - May 8, 2017, 7:14 am

Reminder that TOR does not in any way shape or form keep you anonymous. There are way more precautions to take. TOR or a VPN is enough to just surf the web for personal use but it only goes part of the way to keep you anonymous. Check the sticky in the PrivateInvestigation section.

5chn4pp - May 8, 2017, 7:16 am

(May 8, 2017 07:14 AM)Faith Connors Wrote: [\[CITE\]](#) Reminder that TOR does not in any way shape or form keep you anonymous. There are way more precautions to take. TOR or a VPN is enough to just surf the web for personal use but it only goes part of the way to keep you anonymous. Check the sticky in the PrivateInvestigation section.

of course you need to use different usernames, passwords, correct grammar and not leak private info about yourself but thats just common sense, if you dont leak anything then your fine.

Asdethprime - May 8, 2017, 7:31 am

(May 8, 2017 07:07 AM)Suppletive Wrote: [\[CITE\]](#) Thanks for your answer.

Question apart, let's imagine the following case: If you connect to an IRC channel, and you proxied trough tor network. Your IP will be masked to all the others users, however, the op's of the channel are able to see your real IP?

Actually they will have no clue what your IP address is. The address IRC would get would be the IP address of tor's exit node. That is a randomly choosen router, in a random country that happens to pass your message on.

In fact even the exit node has no idea what your orginal IP is. Entry node is the only node that has your actual IP. The entry node however does not where the message has come from or where it is headed.

Faith Connors - May 8, 2017, 7:52 am

(May 8, 2017 07:16 AM)Satudarah Wrote: [\[CITE\]](#) of course you need to use different usernames, passwords, correct grammar and not leak private info about yourself but thats just common sense, if you dont leak anything then your fine.

...

And watch for DNS leaks.

And watch for javascript which can profile you.

There were exploits in the past that really fucked over TOR users.

Nozreon - May 12, 2017, 12:48 am

Use vpn my friend. And after you use vpn use tor (your internet connection will slowdown but you will still anonymous).

blazingfiremonster - May 12, 2017, 6:29 am

Is [censored] no-logs? Is using it recommended?

Nomad.Null - May 12, 2017, 7:44 am

Make sure you burn off your fingerprints too. You can never be too paranoid. ?

Faith Connors - May 12, 2017, 7:53 am

(May 12, 2017 07:44 AM)True Demon Wrote: [\[CITE\]](#) Make sure you burn off your fingerprints too.

You can never be too paranoid. ?

And wear gloves because you might get fingerprint traced by the CIA if you dont burn them enough.

Key Punch - May 12, 2017, 8:01 am

My recommended method.

Get a laptop with either soldered/glued in ram or Intel memory scrambling technology. (mitigate cold boot attack)

Choose an distrobution that recieved frequent bug testing and security fixes (arch linux/debian) and install it to your operating system with LUKs encrypted LVM.

burn a live distrobution of linux(custom live image/tails/blackarch/kali/parrot to a DVD-R (Non Re-Writeable)

Buy a 500 Meter+ wifi usb antenna(access distant wifi), raspberry PI(intermediate component for distant wifi to the tor router, anonabox (Tor router) //You could have another device connecting from the tor router to your laptop.

For illegal activity then liveboot your burned disc(linux distro).

Optional: Purchase a vpn service like [censored] and only start the tunnel when you are using the remote wifi tor setup so the vpn doesn't log your ip (logs the tor ip).

SSH into a more powerful bulletproof VPS that you paid for anonymously with bitcoin cleaned with a mixer.

Hack from that VPS.

Expect 300-500MS delay and only communication with your team by text and not voice which you shouldn't be doing voice coms anyway

To clarify:

Use the installed operating system to do legal things and talk on hackforums.
Use the Liveboot operating system to do illegal hacking related activity

and remember

Don't operate from your home

You don't have to encrypt what you don't say

and when you hack something SHUT THE FUCK UP half of hackers get caught because they talked about something they did. (example: fappening)

edit: Mitigate all fingerprinting techniques (browser/os) and keep up to date on tor vulnerabilities(set news alerts)

nightkyze - May 12, 2017, 5:09 pm

tor can work or buy a bunch of proxys and download a proxy auto switch

Chercher - May 12, 2017, 5:33 pm

mfw skids suggesting TOR as a supplement to staying safe on the internet.

yeye just go outside and connect to your local mcdonalds or whatever luxurious restaurants you find around you, use a proxy, make sure you use tails or some other OS that is meant for privacy & security, something like whonix or parrot os i guess?

plus you'll get off your lazy ass so thats a :+1:

it doesn't really matter if there's a lil faggot watching what you're doing on the proxy's datastream, it's not as if s/he knows your home network's IP address, and as long as you don't sign into anything you can basically play solitaire without getting ddosed and tracked by unnamed agencies. presuming whatever gnu/linux-based distro you're running even has a packagemanager and has proprietary graphic drivers (usually they do) to even load solitaire (tails doesn't). u could just not be alil bitch and stop being so spooked about some skid having ur ip address.

people treat ip addresses like fucking bank accounts what is this mongol era i have bee born into

5chn4pp - May 12, 2017, 5:40 pm

(May 12, 2017 05:33 PM)Chercher Wrote: [\[CITE\]](#) mfw skids suggesting TOR as a supplement to staying safe on the internet.

yeye just go outside and connect to your local mcdonalds or whatever luxurious restaurants you find around you, use a proxy, make sure you use tails or some other OS that is meant for privacy & security, something like whonix or parrot os i guess?

plus you'll get off your lazy ass so thats a :+1:

it doesn't really matter if there's a lil friend watching what you're doing on the proxy's datastream, it's not as if s/he knows your home network's IP address, and as long as you don't sign into anything you can basically play solitaire without getting ddosed and tracked by unnamed agencies. presuming whatever gnu/linux-based distro you're running even has a packagemanager and has proprietary graphic drivers (usually they do) to even load solitaire (tails doesn't). u could just not be alil bitch and stop being so spooked about some skid having ur ip address.

people treat ip addresses like fucking bank accounts what is this mongol era i have bee born into
>>mfw skids suggesting TOR as a supplement to staying safe on the internet.
>>make sure you use tails

You just called yourself a skid?

Chercher - May 12, 2017, 5:46 pm

(May 12, 2017 05:40 PM)Satudarah Wrote: [\[CITE\]](#) >>mfw skids suggesting TOR as a supplement to staying safe on the internet.
>>make sure you use tails

You just called yourself a skid?

:thinking:

i meant use tails for it's ability to change the DE to something like Windows XP or whatnot

but

i did suggest
whonix

so
be gone thot

?

UkVenoM - May 13, 2017, 4:44 am

VPN to secure network traffic, TOR to anonymize your identity online.

Add a SOCKS5 proxy on a compromised machine before connecting to either to further obfuscate your identity.

The-hunter22 - May 13, 2017, 4:53 am

(May 8, 2017 06:34 AM)Satudarah Wrote: [\[CITE\]](#) tor

that's basically everything you need.

Tor isnt always the best options tho. For blackhat shit tor isnt enough. Worked with police cyber teams and they got the victim. Spoiler, he only used tor (and was a little bit stupid)

(May 12, 2017 08:01 AM)Dildo Shwaggins Wrote: [\[CITE\]](#) My recommended method.

Get a laptop with either soldered/glued in ram or Intel memory scrambling technology. (mitigate cold boot attack)

Choose an distrobution that recieved frequent bug testing and security fixes (arch linux/debian) and install it to your operating system with LUKs encrypted LVM.

burn a live distrobution of linux(custom live image/tails/blackarch/kali/parrot to a DVD-R (Non Re-Writeable)

Buy a 500 Meter+ wifi usb antenna(access distant wifi), raspberry PI(intermediate component for distant wifi to the tor router, anonabox (Tor router) //You could have another device connecting from the tor router to your laptop.

For illegal activity then liveboot your burned disc(linux distro).

Optional: Purchase a vpn service like [censored] and only start the tunnel when you are using the remote wifi tor setup so the vpn doesn't log your ip (logs the tor ip).

SSH into a more powerful bulletproof VPS that you paid for anonymously with bitcoin cleaned with a mixer.

Hack from that VPS.

Expect 300-500MS delay and only communication with your team by text and not voice which you shouldn't be doing voice coms anyway

To clarify:

Use the installed operating system to do legal things and talk on hackforums.

Use the Liveboot operating system to do illegal hacking related activity

and remember

Don't operate from your home

You don't have to encrypt what you don't say

and when you hack something SHUT THE FUCK UP half of hackers get caught because they talked about something they did. (example: fappening)

edit: Mitigate all fingerprinting techniques (browser/os) and keep up to date on tor vulnerabilities(set news alerts)

Great post! you look experienced ^^

(May 12, 2017 08:01 AM)Dildo Shwaggins Wrote: [\[CITE\]](#) half of hackers get caught because they talked about something they did.

5chn4pp - May 13, 2017, 5:15 am

(May 13, 2017 04:53 AM)The-hunter22 Wrote: [\[CITE\]](#) Tor isnt always the best options tho. For blackhat shit tor isnt enough. Worked with police cyber teams and they got the victim. Spoiler, he only used tor (and was a little bit stupid)

For me it was enough, police didn't find any of my tor related stuff, although they search for over 4 months for it.

Malicious Intent - May 13, 2017, 5:18 am

I just wanted to remind folks about ipv6 leak and also show you some interesting concept:

<https://github.com/samyk/proxygambit>

Malta - May 13, 2017, 5:21 am

TOR is not good if you are doing serious shit.

TOR just gives you a time advantage.

yusufmalikul - May 13, 2017, 5:38 am

Use virtual Machine when browsing. In that virtual OS install TOR. If something bad happen you can just delete the Virtual Machine.

The-hunter22 - May 13, 2017, 5:47 am

(May 13, 2017 05:21 AM)Malta Wrote: [\[CITE\]](#) TOR is not good if you are doing serious shit.

TOR just gives you a time advantage.

True. It takes a long time but if the police is serious about you, they will get you with it.

Mythical_aF - *May 13, 2017, 2:45 pm*

thanks for these tips bro.?