

Forum:[Hack Forums](#)

Thread: [OPSec & Anonymity Setup - Hiding from the Government & Others](#)

Zayzo - April 9, 2016, 11:36 am

With people out there trying to cause you harm, or the simple government who utilize a \$52 billion budget used for intelligence, it is important to maximize your safety & maximize your privacy.

Please build up on what I suggest,

"Each layer is like a blanket, the more blankets you wear the warmer you are." - A Good Friend

Step 1: Attaining a Secure VPS

Making sure, you don't work on your main computer is a huge first step. The best thing you can do is work/conduct your activities off a VPS. Now many VPS's are DMCA compliant/not off-shore. These two key components allow you to be tracked much, much easier.

First head over to this site: https://maxided.com/dedicated-servers/dmca_ignor

I already selected the filter option for only VPS's that ignore DMCA to show up. Your job is to buy a VPS from this list, make sure the VPS is hosted off-shore.

Once purchased follow the steps, you can access your VPS details via the program "Remote Desktop Connection". By inputting the server details that will be sent to you after payment.

Step 2: Ascertain a Secure VPN

Now, most VPN's advertise no logs, but actually do contain logs and use this line "No Logs" as a marketing scheme. I won't be calling out any VPN's but it is pretty obvious if you have the slight bit of intelligence. (Side Note: The goal is to ascertain a VPN that contains no logs & is not DMCA compliant)

With this in mind, I can make the recommendation to

https://www.ipvanish.com/anonymous/index-d.php?a_aid=563749ce0713e&a_bid=48f95966&chan=ipvmt1&data1=sidebar

I would recommend purchasing this VPN, for your VPN of choice. Not DMCA compliant, truly does not contain any logs (to my knowledge) best over-all-fit.

Now, this is an easy alternative to my MAIN suggestion. My MAIN suggestion would be to create your own VPN on your own server utilizing openswan. Now I will not go into that today, however in the near future I plan to. That is a tutorial on its own.

Step 3: Having SOCK5 Proxies Available

Personally, I have only used vip72 proxies for personal preference. As well as they are the proxies that I trust the most as well as the most safe in regards to privacy.

<http://www.vip72.com/>

Step 4: Utilizing a Secure Browser

Many browsers, for obvious reasons; track you. 99% of browsers, the government is able to track you with ease. There are definitely plugins for each browser & settings you can utilize to minimize the ability of you being able to be tracked. But let's just skip the plugin tbh.

<https://www.torproject.org/>

I would recommend downloading Tor, for your browsing purposes. Now to say Tor is 100% secure, is false. However, Tor is indeed pretty secure, and will hide you for the most part.

In conjunction with all our other steps, you will maximize your safety behind Tor.

Step 5: Using Our Tools

Now we have all our Tools set up for safety.

My process goes: VPS > VPN > Sock5 being routed > Tor

Now this is a pretty easy setup that is not very complex. Fairly easy to follow, and will maximize your safety. You can maximize your safety by throwing in: Using a cracked wifi, utilizing SSH tunneling, using multiple VPS's for different purposes, and really there a plenty of other ways to maximize your safety and add on to this fairly standard setup.

I can say that this is my standard day to day set up, and if I realm into anything more serious extra precautions are taken.

Last Steps

Now you have all the tools, you have the setup.

1. You need to make sure that you have different passwords, for everything you use; emails, aliases, clients etc.. (16 char atleast for all PW's)
2. Do not mix PW's.
3. Do not mix BTC addresses
4. Do not use the same aliases/emails/ANYTHING on your main computer with your VPS activities.
5. The most important thing is to keep your identities seperate. With each identity, is a set of PW's, BTC Addresses, IP's etc and you need to keep this ALL seperate.
 - 5a. If need be, buy multiple VPS's

Conclusion

There are plenty things to consider and analyze on your route to becoming fully anonymous. I believe anything past this setup (for the average internet user) starts wandering in the realm of

complex.

I will continue to update this tutorial, and add in variations to this setup with more complex plugins in mind.

Side Utilities

1. Be familiar with PGP Encryption as I have recently been familiarizing myself with it too.
2. For all IM communication please check out XMPP/Jabber and the client "Pidgin" to safe guard all your messages when communicating with someone else.
3. I recommend everyone crypt a partition where you store sensitive information, with Veracrypt.

alphaalex - April 29, 2016, 1:40 pm

hey zayo, i think your the person i need to help me with a problem i have been having with a cheater. i made this profile just to find someone with your skill set so i cannot private message you. Is there any way i can get in touch with you?

Ooze - April 29, 2016, 2:14 pm

Posting to read this later tonight,
Any programs for managing passwords?
Also what encryption software do you recommend

'OverSight - April 29, 2016, 3:39 pm

(Apr 29, 2016 02:14 PM)The JOker Wrote: [\[CITE\]](#) Posting to read this later tonight,
Any programs for managing passwords?
Also what encryption software do you recommend

Keepass/Veracrypt are pretty good.

Also about getting a VPS thats hosted in china or russia, I figured that would be a bad idea as they actually care alot? Ru for sure is hard for cyber crime and China... well im not sure about them.

Ooze - April 29, 2016, 3:40 pm

(Apr 29, 2016 03:39 PM)OverSight Wrote: [\[CITE\]](#) Keepass/Veracrypt are pretty good.
Also about getting a VPS thats hosted in china or russia, I figured that would be a bad idea as they actually care alot? Ru for sure is hard for cyber crime and China... well im not sure about them.
Ya but Russia won't care if you are hacking in the us I believe

'OverSight - April 29, 2016, 3:42 pm

(Apr 29, 2016 03:40 PM)The JOker Wrote: [\[CITE\]](#) Ya but Russia won't care if you are hacking in the us I believe
but that means they know im from the us... lol rip

Voxi - April 29, 2016, 5:14 pm

VPS > Tor > VPN > Socks5

Open Tor first because it anonymize's you and then your VPN because it encrypts your data, if you opened tor afterwards no data after Tor would be encrypted. Correct me if I'm wrong.
My person preference is VPS > Tor > VPN > Socks5

Peptide - April 29, 2016, 5:15 pm

(Apr 29, 2016 05:14 PM)Voxi Wrote: [\[CITE\]](#) VPS > Tor > VPN > Socks5
Open Tor first because it anonymize's you and then your VPN because it encrypts your data, if you opened tor afterwards no data after Tor would be encrypted. Correct me if I'm wrong.
My person preference is VPS > Tor > VPN > Socks5

Honestly it should be VPN > VPS > TOR > SOCKS5

Voxi - April 29, 2016, 5:41 pm

(Apr 29, 2016 05:15 PM)Peptide Wrote: [\[CITE\]](#) Honestly it should be VPN > VPS > TOR > SOCKS5
Yeah Its up to you if you want to use the VPN in your vps or not.

Mr. Robot - April 29, 2016, 5:46 pm

Quote:My process goes: VPS > VPN > Sock5 being routed > Tor

I personally connect to a btc paid VPS with a RAT for control then follow your setup.

One more important note to add, the FBI have stated they are able to connect your online times of your handles with when your vpn traffic is online.

A NEW ERA... - April 29, 2016, 5:47 pm

(Apr 29, 2016 01:40 PM)alphaalex Wrote: [\[CITE\]](#) hey zayo, i think your the person i need to help me with a problem i have been having with a cheater. i made this profile just to find someone with your skill set so i cannot private message you. Is there any way i can get in touch with you?You're fucking sad, go learn some decent dignity before you get with a female. Without trust there is nothing in your relationship.

[img]<http://thesource.com/wp-content/uploads/2016/04/Screen-Shot-2016-04-27-at-1.43.46-PM.png>
/img]

Overall though, great simple tutorial for all the hacking newbies Zayzo. Should add something about paying for all these with BTC, and furthermore tumbling that BTC.

Mr. Robot - April 29, 2016, 5:53 pm

(Apr 29, 2016 02:14 PM)The J0ker Wrote: [\[CITE\]](#) Posting to read this later tonight,
Any programs for managing passwords?
Also what encryption software do you recommend
Don't use any of those password managers. I personally hash:salt my own passwords for example.

TheJ0ker2016HackforumsUb3rKidH4x0r

Encrypted with MD5 and the salt 04302016 which is todays date.

Would then become a890e6655023173b093c433e48ea8154

Then that password goes into the website and gets encrypted with what ever that website uses.

__Joel - April 29, 2016, 5:55 pm

This should probably help quite a few users.

Thanks for the share.

Zayzo - April 29, 2016, 7:21 pm

(Apr 29, 2016 02:14 PM)The J0ker Wrote: [\[CITE\]](#) Posting to read this later tonight,
Any programs for managing passwords?
Also what encryption software do you recommend
Never trust any program to manage passwords. Write down ALL your passwords.

(Apr 29, 2016 03:39 PM)OverSight Wrote: [\[CITE\]](#) Keepass/Veracrypt are pretty good.
Also about getting a VPS thats hosted in china or russia, I figured that would be a bad idea as they actually care alot? Ru for sure is hard for cyber crime and China... well im not sure about them. Not true at all, those are great off-shore countries for a VPS to be located.

(Apr 29, 2016 05:53 PM)Mr. Robot Wrote: [\[CITE\]](#) Don't use any of those password managers. I personally hash:salt my own passwords for example.

TheJ0ker2016HackforumsUb3rKidH4x0r

Encrypted with MD5 and the salt 04302016 which is todays date.

Would then become a890e6655023173b093c433e48ea8154

Then that password goes into the website and gets encrypted with what ever that website uses.
No, still would not advise you to do this. Write down ALL Pw's.

Mr. Robot - April 29, 2016, 7:45 pm

(Apr 29, 2016 07:21 PM)Zayzo Wrote: [\[CITE\]](#) No, still would not advise you to do this. Write down ALL Pw's.

See that's the thing. If I do use plain text for example.

ZayzoSaysToWriteDownPasswords5232016

I would encrypt that before writing it down.

For the above example that you quoted me on -
TheJ0ker2016HackforumsUb3rKidH4x0r

I would write down TheJ0ker2016HackforumsUb3rKidH4x0r and the salt on a piece of paper, when I want to login to the website, I encrypt it again and login.

If possible on the webpage, try use spaces in passwords as it can help bypass keyloggers (even though you shouldn't be infected in the first place)

You can try KeyScrambler for scrambling your input through a enigma type system when entering information to help bypass keyloggers too.

One other thing I didn't mention, try use () for example in the above passwords you could do:
(TheJ0ker2016HackforumsUb3rKidH4x0r)

As your password

Or then encrypt in something else with a salt of your choosing.

- Last but not least one of the biggest issues with passwords like these is idiots who use them on multiple websites.

Doesn't matter the websites encryption or how tough your password is to get if it's used elsewhere and this is why.

SPAM stored passwords in plain text.
Plain text passwords get added to a dictionary file used for decrypting hashes.
Website gets hacked using say Hash:Salt of any variety.
Dictionary used against the hash:salt list and guess what. Your password is in there.

'Cynical - April 29, 2016, 7:50 pm

I would recommend saving alias data in a notebook, too.

If you know you're going to be raided, it's much easier to burn a small book than to wipe a few drives and servers.

Faster, too.

'OverSight - April 29, 2016, 8:14 pm

(Apr 29, 2016 07:50 PM)Cynical Wrote: [\[CITE\]](#) I would recommend saving alias data in a notebook, too.

If you know you're going to be raided, it's much easier to burn a small book than to wipe a few drives and servers.

Faster, too.

not when you got a big ass magnet, destroying a hd is faster. lol.

Zayzo - May 2, 2016, 9:25 pm

(Apr 29, 2016 08:14 PM)OverSight Wrote: [\[CITE\]](#) not when you got a big ass magnet, destroying a hd is faster. lol.I have a decent-sized shredder in my office. I'd rather stick 5 pages from my notebook into the shredder than fuck with a magnet.

powerl105 - May 2, 2016, 11:42 pm

should add....doing all this from a bootable tails drive.

?BORNE? - May 2, 2016, 11:45 pm

Nice tutorial Zayzo... bookmarked:)

Cady - May 12, 2016, 7:32 am

Good tutorial, really. ?

Thanks bro.

Superman57 - May 12, 2016, 9:14 pm

thanks for the tutorial it all sounds good to stay private

Zayzo - May 15, 2016, 12:18 pm

Appreciate the comments. Will update it soon.

Emms - May 16, 2016, 9:48 am

Hey, i cant send a PM yet on this account (My old account got comprimised and Im waiting to get it back but I still want this future asap). How could we get in contact?

San1ty1 - May 23, 2016, 5:32 pm

Posting to take a look at this later. Looks pretty nice though

The Silenced - May 23, 2016, 5:38 pm

This is a very good opsec tutorial..very knowledgeable.

placeholdera - May 24, 2016, 4:12 am

This guide's a joke. Why would you want to add multiple points of failure like this?

Zayzo - May 24, 2016, 7:17 am

(May 24, 2016 04:12 AM)placeholdera Wrote: [\[CITE\]](#) This guide's a joke. Why would you want to add multiple points of failure like this? Multiple points of failure? Lmao, this a great standard setup and easy to use. There can be more complicated setups, of course? Never did I say this was the most complicated setup nor was that the goal of this tutorial.

You have no idea what youre talking about.

placeholdera - May 24, 2016, 8:56 pm

This is the same as having 5 couriers for your package instead of 1 courier. It only makes sense if you have full control over the chain.

Here's what usually happens:

You > ISP > Internet

Your ISP knows what you're doing.

Your retarded diagram:

You > ISP > Internet > VPS > VPN > Sock5 being routed > Tor

You don't know if your VPS provider is secure.

You don't know if your VPN is secure.

You especially don't know who the fuck is hosting your SOCKS5 proxy since you're buying lists. Any dipshit with a few console commands can host a SOCKS5 proxy.

Tor is reasonably secure by design. Anyone that read the fucking Wikipedia page can tell.

Why complicate this shit by buying stupid services?

-_-Error 404-_- - May 25, 2016, 6:38 am

This will probably get you in jail

Tor is not safe , not even socks proxies since most of them are used as honeypots and most of the time they monitor all your traffic

Also, if you are not using a VPN to connect to your VPS Server they will log your ip address which is not good if they trace back your vps's ip

Zayzo - May 25, 2016, 7:30 am

(May 25, 2016 06:38 AM)-_-Error 404-_- Wrote: [\[CITE\]](#) This will probably get you in jail

Tor is not safe , not even socks proxies since most of them are used as honeypots and most of the time they monitor all your traffic

Also, if you are not using a VPN to connect to your VPS Server they will log your ip address which is not good if they trace back your vps's ip

"This will probably get you in jail" Lol never did I say this was the most secure setup, but a easy to setup and fairly secure setup it is.

VPS - offshore, -DCMA ignored, will not log your IP Addresses.

Tor is the most safe browser. There's no other alternative. Tor is 95% safe, and that's gonna have to be good enough.

Shadow4222 - May 26, 2016, 4:29 am

(May 25, 2016 07:30 AM)Zayzo Wrote: [\[CITE\]](#) "This will probably get you in jail" Lol never did I say this was the most secure setup, but a easy to setup and fairly secure setup it is.

VPS - offshore, -DCMA ignored, will not log your IP Addresses.

Tor is the most safe browser. There's no other alternative. Tor is 95% safe, and that's gonna have to be good enough.

So, should I be connected to VPN when connecting to offshore VPS (DMCA ignored) or is it safe to connect to it without VPN ?

Zayzo - May 26, 2016, 7:06 am

(May 26, 2016 04:29 AM)Shad0w_ Wrote: [\[CITE\]](#) So, should I be connected to VPN when connecting to offshore VPS (DMCA ignored) or is it safe to connect to it without VPN ?If you buy an off-shore VPS (DMCA Ignored) you will be fine. Could it hurt to connect additionally with a VPN? No, so if you are paranoid and want to be extra safe you can.

Raven Kidd - May 27, 2016, 6:21 am

Did anyone try to use i2p?

Is it secure?

Zayzo - May 27, 2016, 6:27 am

(May 26, 2016 04:29 AM)Shad0w_ Wrote: [\[CITE\]](#) So, should I be connected to VPN when connecting to offshore VPS (DMCA ignored) or is it safe to connect to it without VPN ?Some can be paranoid and not trust the VPS provider, however if your purchasing from that site, personally I would trust them.

It's safe to connect w/o a VPN, for extra security add a VPN before.

SIM-3022874 - May 27, 2016, 8:34 am

Really helpfull, thank you!

-_Error 404-_ - May 27, 2016, 12:17 pm

(May 27, 2016 06:27 AM)Zayzo Wrote: [\[CITE\]](#) Some can be paranoid and not trust the VPS provider, however if your purchasing from that site, personally I would trust them.

So, im i paranoid? ?

eartha2 - May 27, 2016, 1:13 pm

nice guide op thx really need this

Zayzo - May 27, 2016, 5:28 pm

(May 27, 2016 12:17 PM)-_Error 404-_ Wrote: [\[CITE\]](#) So, im i paranoid? ?Not sure about your english, but there's no viable reason to have a VPN before it anyhow.

Extra security, but it's not needed.

Francis Gallagher - May 28, 2016, 8:52 am

Posting so I can set everything up later tonight. From what I read, seems great so far.

AAA+ - May 30, 2016, 8:47 am

Good setup but for storing passwords yall can use an encrypted usb or hdd with another layer of

encrypted files ? if you really want to stay off the grid you will.

Zayzo - May 30, 2016, 11:22 am

(May 30, 2016 08:47 AM)AAA+ Wrote: [\[CITE\]](#) Good setup but for storing passwords yall can use an encrypted usb or hdd with another layer of encrypted files ? if you really want to stay off the grid you will. Write it down or encrypted partition with veracrypt.

Zayzo - June 10, 2016, 6:03 pm

Bringing this to the top, in case anyone needed help. Expect more tutorials soon

AcroClipz - June 11, 2016, 10:59 am

You could instead try these with a secure configured system...

- 1) Windows 8.1 / Tails OS (Operating System)
 - 2) Bit-Defender Internet Security (System Security Software)
 - 3) Blancco Computer Data Eraser (Data Destruction Software)
 - 4) System Mechanic Pro (System Maintenance Software)
 - 5) HitmanPro Alert (Anti Malware Software)
 - 6) SpyShelter (Anti Keylogger Software)
-
- 1) Sigaint Mail / MyMail / Protonmail (Anonymous Email Providers)
 - 2) Kali Linux (Advanced Penetration Testing Tool)
 - 3) Nessus (Network Vulnerability Scanner)
 - 4) Wireshark (Network Protocol Analyser)
 - 5) Snort (Network Intrusion Detection System)
 - 6) Netcat (Network Utility Tool)
 - 7) VCP oVPN (Anonymous SSH/SSL VPN)
 - 8) Tor Browser (Anonymous Web Browser)

Zayzo - August 10, 2016, 2:52 pm

Bumping this, may add more if more interest is shown.

skelly76 - August 10, 2016, 3:46 pm

(Aug 10, 2016 02:52 PM)Zayzo Wrote: [\[CITE\]](#) Bumping this, may add more if more interest is shown. Add more. :P

libc - August 11, 2016, 7:11 pm

Might want to include information about virtual machines. Doesn't matter how many proxies and VPNs you have if the feds decide to use a 0day browser exploit on you.

libc - August 11, 2016, 7:38 pm

(Aug 11, 2016 07:16 PM)Max The GOD Wrote: [\[CITE\]](#) So by adding a virtual machine in, the authorities can't "0day browser exploit" us?

If you're using [Whonix](#) correctly, then client side attacks won't compromise your opsec.

forsakenone - August 18, 2016, 6:55 pm

hiding from the government...? stop promising these kids lies

FlyingBlanket11 - August 18, 2016, 9:54 pm

<https://www.deepdotweb.com/2015/04/15/so-you-want-to-be-a-darknet-drug-lord/>

Written by nachash, great help. Read through it and understand opsec.

You should take the SOCKS5 portion out as the server in which it's hosted on can intercept

information.

~ **Left HF For Good** ~ - August 19, 2016, 8:23 pm

Damn.

Zayzo, back at it again. Keep up the amazing tutorials, would love to see more of these tutorials.

Pew ? - August 19, 2016, 8:24 pm

Russia is now making all hosts to log information for at least the first 6 months of use. Do not use Russian based services if you want to keep your trail anonymous.

146918496 - August 29, 2016, 11:01 am

Hello OP,

Not sure if you'll be able to read this,

But I read this and I'm interested in your doxing service. (tid=4797987)

Due to my low amount of posts, I am unable to send you a PM regarding this topic,

It would be must appreciated if you could send me a PM with contact info.

Thanks in advance.

201 - August 31, 2016, 5:28 pm

nice tut, posting here to come back later;)

-Distribution - August 31, 2016, 8:02 pm

very very nice tutorial, this will help many people become more secure.

Zayzo - August 31, 2016, 9:16 pm

(Aug 29, 2016 11:01 AM)146918496 Wrote: [\[CITE\]](#) Hello OP,

Not sure if you'll be able to read this,

But I read this and I'm interested in your doxing service. (tid=4797987)

Due to my low amount of posts, I am unable to send you a PM regarding this topic,

It would be must appreciated if you could send me a PM with contact info.

Thanks in advance. Contacted you per your request.

(Aug 31, 2016 05:28 PM)Bam Margera Wrote: [\[CITE\]](#) nice tut, posting here to come back later;)

(Aug 31, 2016 08:02 PM)-Distribution Wrote: [\[CITE\]](#) very very nice tutorial, this will help many people become more secure. Thank you for the comments. I will add more since I have had multiple requests to do such.

Gamer Fusion - August 31, 2016, 9:17 pm

Nice tutorial mate, I'm posting here to come back in the future.

\$AMMi - September 1, 2016, 12:41 am

Nice tutorial never hurts to have more blankets :D

Zayzo - October 2, 2016, 5:09 pm

Appreciate the responses.

Max P™ - October 2, 2016, 6:05 pm

Really nice tutorial, Thanks Zayzo!

user088 - November 18, 2016, 11:51 am

Nice tutorial Zayzo
Thanks for the share.

xanity - January 10, 2017, 1:47 pm
Thanks for the share

Why complicate this by buying services

Zayzo - February 15, 2017, 10:16 pm
(Oct 2, 2016 06:05 PM)Max P™ Wrote: [\[CITE\]](#) Really nice tutorial, Thanks Zayzo!
(Nov 18, 2016 12:51 PM)user088 Wrote: [\[CITE\]](#) Nice tutorial Zayzo
Thanks for the share.
(Jan 10, 2017 02:47 PM)xanity Wrote: [\[CITE\]](#) Thanks for the share

Why complicate this by buying servicesAppreciate the comments, should update it soon.

L33tness - February 24, 2017, 3:25 am
Interesting ! I have learned so much from you guys its not even funny. Thanks all you HF Legends.

Praet0rian - February 24, 2017, 1:30 pm
Seems like a good solid guid efor starters, you didn't mention Tails OS or Whonix or Qubes OS, one of the new fancy 'security-'oriented OS's, but so far pretty good.

Revived1337 - February 25, 2017, 10:24 am
very good anonymity setup , i guess helpfull for some people

Koutei - November 3, 2019, 4:50 pm
so interesting, posting this to come back in the future.

rusticx - December 7, 2025, 12:11 pm
thanks gango