2024 Darknet OPSEC Bible

ORIGINALLY WRITTEN AND PUBLISHED BY VivianCPussi on Dread.

Link: http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/1968795420333261495 0/#c-7c2f1f5af40e27b563

———————————-

Hi, I write the 2020,2021 Darknet OPSEC Bibles that mentioned Libreboot laptops. Im back with a updated guide.

●Buy a laptop just for the darknet. I personally use a Lightweight linux distro, with UFW Firewall enabled, and update daily.To get Linux installed on many laptops, you'll have to disable "SecureBoot" in the BIOS. I also had to install a WIFI driver to get WIFI working, to do this I have a Ethernet to USB adpater, and installed the WIFI Driver then was ready to go.

●On your Operating System, make sure you update the OS daily, and install a open-source Firewall. I use Linux, and I use UFW firewall. "sudo apt-get install ufw" , "sudo ufw enable". then Reboot OS.

●Install PGP software, on Linux, I use 'gpa' "sudo apt-get install gpa" , an open source PGP software.

●I personally always use Public WIFI for placing orders, logging into the DNMs. Just make sure you arn't on camera. I go to the corners of librarys, look around for cameras, and then tilt my screen so its hard to see my screen. Public WIFI means your Connections to the Tor Market will only lead back to the public wifi network, much better tracing back to your house.

●I enable MAC address randomization, and set a random hostname. MAC address randomization ensures that each and every time you connect to a WIFI network, your WIFI MAC address is RANDOM MAC address. This makes tracking your devices connections to WIFI Routers, harder. I also set a random hostname, every day.

Randomize MAC address:

https://raddle.me/wiki/MacAddressRandomization

Set new Linux Hostname:

"sudo hostnamectl set-hostname NEWHOSTNAME"

Example:

sudo hostnamectl set-hostname AbellaLexington.

check your new hostname with 'hostname' terminal/cli command.

●Obtain Bitcoin, then swap/convert BTC to XMR. I use Kilos, and Elude to swap BTC to XMR. I don't buy Bitcoin Anonymously, because I convert it to XMR. If the IRS/Gov were to ask me about my Bitcoin holdings, I'd say I donated it all to various charities/lost the wallets. I hold my Monero with FeatherWallet.

●Once you have XMR Monero, your ready to buy some goods on the darknet markets. Find a real DNM and find a highly-rated vendor, who has logged in recently, read DNM Bible.

●Once your ready to order, PGP-Encrypt your Shipping Address, using your real name and address, to the vendors PGP public key. Always encrypt your address on your device itself. Don't rely on/trust the Market to encrypt your address safely. Always encrypt your Shipping Address on your personal device.
●Send the exact amount of XMR for the order, to the provided payment address, or load your DNM account with more than enough XMR to place an order.
●Send in order, and wait. Once your package is actually shipped, expect to receive your order in 2-7 days. If your order hasn't arrived after being marked shipped, after 2 weeks/14 days, Private Message your vendor asking for a status update.
If you request the USPS tracking number, always have the vendor send you the tracking number ENCRYPTED with your Public PGP key. Check tracking on 3rd party USPS tracking websites such as trackingmore
etc
Never check your tracking number on the official USPS website, with or without Tor. Using Tor to check your USPS tracking number can FLAG your package for INSPECTION. I typically just go to public wifi (real local IP, not VPN, not Tor IP) and check the tracking number on a 3rd party tracking website.
Once your order arrives, burn, or throw away the package and get the package out of your house as fast as you can. I also reccomend opening orders outside of your house, incase there is a tracking device which activates when you open the package, if you are in a public bathroom opening your pack for example (dirty) but you can flush the drugs/decoy drugs easily as the alarm is sounding and GPS location being sent to police.
So I always open my packs in clean, public bathrooms, and I keep the pack in an empty backpack, then once I open the pack, I place the Goods back into my backpack, and I throw the empty package away in a random public trashcan a few block away.
Great, now if you get raided by police, they can't prove you got the drugs/medicines on the dark net due to the package not being at your house, good.
In an FBI documentary on DarkNet Raids, they said "We look for packages and shipping materials" so packages once opened can be used to prove you ordered drugs online, which both "burns" the vendor because now the vendors return addresses he used for your pack and other peoples packs are assosciated with drug orders, and you get a nice Legal Charge "Interstate Drug Trafficking, using the Postal Service, and possession charge". You see, if you had just gotten rid of the package early/as soon as possible, you'd have just a simple possession charge.
Sometimes I take an empty package to a burn-pit at my local beach, and soak it in lighter fluid or 70,90% rubbing alcohol and burn my package in the burn-pit. Evidence to ashes. =)

Don’t tell your friends about your DarkNet usage, at all, in any way.

I told one friend I was ordering weed on the darknet one single time, and months later, at a random party I was at, a friend of the friend I had told, said LOUDLY “Hey *name* are you still getting weed shipped in the mail?” This was also when weed was still illegal in my state. So keep your darknet usage to yourself, it may keep you out of jail.

If you ‘Need’ to talk about your darknet usage, talk here, safely on Dread.

Imagine getting raided by the police. What evidence would be found?

Empty Packages from your vendor?

Reccomended Answer: No packages here, I got rid of my packages the same day I got my orders. No inter-state drug trafficking charge for me.

Bookmarked, saved Darknetmarket URLs on your Desktop in a Text file, or bookmarked on your Tor Browser?

Reccomended Answer: No, I load dark.fail > dark.fail onion, or tor.taxi > tor.taxi onion service each time I load the DNMs.

Drugs in your dresser, drawers, closet etc?

Reccomended Answer: I vaccume seal all of my drugs/medicines to minimize smell/detection ability of drug dogs.

*any drugs in your house, will probably be found. But I have had friends avoid police from finding drugs by having a fake backing in a closet. They could remove the back wall in the closet and replace the space by sliding the back wall panal. Then, once they got a search warrant applied to them, (The police didnt kick the door down instantly), they hid their cannabis behind the fake panal, and then let the cops in to search. This was just a routine probation-officer search, and the person had to let the police in because somebody called

the police and said they noticed we were smoking weed and it was coming out the window, and the person had to let the police in because he had prior issues with the law.

Generally, if the police ever knock on your door, simply don't answer it. It's that easy. Go to a back-room where the police can't see you through the windows, turn your loud music off, and go hide in the bathroom until the police leave. If they break your door down, instantly flush your drugs/illegal goods. You may get one or two flushes before the police break into your bathroom. But the cops can easily turn your water off, or recover the flushed drugs if you only got one or two flushes in. Typically, a standard house has to flush like 5-10 times to get the flushed goods fully out and away from the house and out of the "plumbing trap". I reccomend fake walls, fake floors, hollow walls and floors etc if you can do so.

Never discuss/deal drugs with your cellphone.

Don't take pictures of your drugs with your phone, dont sell drugs with your phone, not with Snapchat or even encrypted messaging apps. Its just too easy to hack phones these days, or for your buyers to get caught and snitch/rat/turn you in, save/screenshot messages, take photos of you while you hand them drugs, I just reccomend not dealing drugs at all, and if you do deal drugs, just find people in-person for one-time deals, just don't use cellphones for anything illegal at all.

Of course, yes, it CAN be done, all parties use self-deleting, encrypted messages, you only hand people their drugs outside of your house at a public place or their car etc, but generally I just reccomend not dealing at all

Encrypt your Hard Drive/SSD.

Linux allows you to encrypt you hard-drive/SSD upon Operating System Installation options. You may also be able to use VeraCrypt to obtain Full-Drive Encryption.

Vendor Specific Advice:

1. Clean your coins before you cash out. Try to cash out on LocalMonero type sites where people mail cash paper money to your PO-Box, make sure you don't have any fake bills.

I'd try to avoid exchanges such as CoinBase who can seize your coins/BTC at all. LocalMonero is popular enough to cash out large amounts of money.

However there is always a risk of somebody getting your PO Box addresse and robbing you once they know your address, city of the PO box. To protect against robbery, try to find a 24-hour PO-Box/Private Mailbox, and pickup your cash payments at random hours, preferably at night such as 1am.

That's how I'd do it anyway, 24 hour Mailbox lobby access, pickup cash payments, check for fake bills, release Monero XMR.

2. Ship every package as if its being received by, or mailed to a Federal forensics lab. Make sure your pack doesnt contain fingerprints, DNA (skin oil, eyelashes, hair).

3. Make sure your Shipping payment methods are anonymous.

4. Change your Shipping Receiver Address frequently. I'd reccomend using Apartment complexs addresses and making up a name for the Sender/Return Address, but make sure the Unit/Apartment number actually exists.

For example

Return Address:

Adam Franklin

182 Apple Ave Apt 104

Houston TX ZIPCODE

Because Apartment Complexes change their tenants/people living there frequents any database that lists who lives at a specific address wont be updated for Apartments, due to the large amount of constantly changing tenants/people.

5. When delivering your packs to the USPS Blue Boxes, have your cellphone OFF and at home.

Assume your phone is awlays listening, recording VIDEO via cameras, and AUDIO via microphones. Imagine a hacked cellphone (hacked by DEA/FBI) listening to you in your house/apartment, or taking photos of everything your phone can see while you check your phone while vaccume sealing orders. Phones are dangerous, I reccomend the Edward Snowden approach and removing the Cameras and Microphones on your phones. Communicate via Encrypted, Self-Deleting Messages such as Signal for any sensative messages. But again I don't reccomend using phones at all.

At least, cover your phones cameras with black camera-covering stickers. I use the "Blocked" brand of camera-covering stickers.

Don't say anything illegal around your cellphone if it has working microphones.

6. Keep your doors and windows locked at all times.

7. Your Car could have a GPS-tracker on it, recording you delivering packages. Statistically, most FBI/Law Enforcemenet GPS Car Trackers arn't ever noticed by the person of interest. Act as if your car is being tracked via covert GPS tracker.

7a. Remove your Cars inner microphone. I removed my cars Interior Microphone in about 10 seconds, via unplugging it, then, I plugged it back in to fix/restore the microphone function when I later sold my car.

8. Cover/remove your laptops cameras and microphones. If you can't remove the camera and microphone, then at least cover the camera and put super-glue into the microphones. Test both mitigation options, check to see if you can see through your camera, and activate the laptops microphone and see how clearly it can detect audio, can It hear noise, but not define exact words? Probably good enough.

9. Keep your evidence minimal. Image your phone, laptop in police forensics laboratory. Minimize the amount of evidence you keep in the first place. Encrypt your devices with 30+ charater passphrases. I use

book, movie titles then repeat them to create long passwords, then I add numbers and or special characters.

Example of a good password I'd use:

TheShawshankRedemptionTheShawshankRedemption4&&33

48 characters, upper, lowercase letters, numbers, special characters, great.

These passwords are long, secure, and easy to remember. (1 movie title, and 2 or so repeating numbers and special characters).

10. Don't save customer addresses. Think about it, saving addrresses proves that your a vendor.

Think about where your devices may be saving shipping addresses. Does your printer save a copy of everything you print? Is your printer connected to the internet, and backing up/uploading all printed documents to a CLOUD SERVICE?

Make sure, your label printer isn't connected to the internet, perhaps connect to your printer via CABLE or BLUETOOTH, but make sure your printer ISN'T on WIFI/Doesn't Connect to WIFI.

11. If you ever get raided, don't say anything. Excercise your right to 5th ammendment, protection against self-incrimination.

If your doing everything right, here's how your vendor setup would work.

Your drugs are stored vaccume sealed, in a fake wall, fake furniture piece, fake flooring etc, hard to find.

Your devices are all heavily encrypted, with 50+ character passphrases. I use passphrases of over 100+ characters for my laptop, and my phone has an 8 didgit pin. My phone doesn't have any illegal data so it's lower security passphrase.

Your use real, local addresses for your Return Address, where the return address has the same zip code of where your shipping the package from. The return address is real, with a apartment complex and real unit number used. Don't make-up a unit number, walk around the apartment complex and mentally remember the units avaible for your usage as return addresses.

I'd connect to a VPN, then load Google Maps, and find an apartment complex, then I'd go to it, and find the real unit numbers in use, unit numbers are the numbers on the doors usually. So I'd record the Address on Google Maps, and add a realistic looking name, and real unit number and correct zip code, and ship the package from a blue box in the same or very nearby ZIP code.

Thank you, I've been reading OPSEC guides, and buying goods from the DarkNets since Original Silk Road. Silk Road Forums, reddit /r/ darknetmarkets, Dread, The Hub, etc so on.

I belive this advice is 90% comprehensive and mostly correct. If theres any corrections or additions, feel free to post in the commends.

Also, I grant permission to add this post to the Good Opsec posts masterlist if desired.

Thank you