DNM's Buyer Bible (As of 3/22/18)

Table of contents

Use CTRL-F to browse through the guide.

About

Hello and welcome to the Darknetmarkets bible for buyers. The buyer's DNM bible aims to be a complete guide that covers all steps that users have to take in order to buy securely from darknetmarkets.

It orientates itself on OpSec best practices and, if exactly followed, will greatly minimize the risk of you getting caught. There never will be 100% security, but with the help of the buyer's DNM bible you can make it extremely hard and not worthwhile for law enforcement to catch you.

If you are a complete new user and have heard nothing or close to nothing about topic like Tails, Bitcoin and PGP, you will need several hours to go through this guide and follow the instructions. In fact you will probably not be able to buy from darknetmarkets tomorrow or the day after tomorrow. It takes time to get the secure setup, which is described in the DNM bible, working. Once you finished the initial setup it will be pretty easy though. For future orders you just have to repeat the same steps for ordering on the secure setup that you already have.

However buying from DNMs is **not** for everyone. If you have little computer experience and are not willing to invest much time, then you should stick to real life sources and stay away from the DNMs. They will only get you into big legal trouble if you do not use them correctly.
If you are willing to learn and invest some time, then please read and follow every single step of the guide. If you run into problems please check if the DNM bible or the sidebar of /r/DarknetMarketsNoobs already has that issue covered. If not feel free to make a post on this subreddit with a *detailed* description of your issues.
Some parts of this guide have gifs added to them which show how to do some of the steps. However these are just as additional information because software often changes and these gifs can quickly become outdated. Please read the guide first and the resources that are linked **before** blindly doing what is shown in the gif. If you get stuck somewhere you can watch the gifs which may clear things up for you.
The DNM bible is only possible because a lot of awesome people dedicated countless hours of their free time to writing the tools you will use when following the guide. So please show your appreciation to them by making a donation to the torproject, Tails and/or GnuPG once in a while. If you have money to buy drugs, you also have money to reward the people who make it possible for you to order drugs safely to your front door.

If you happen to not know for what an abbreviation stands for and what a certain term means, please check out the Darknet Dictionary by deepdotweb.
One last thing: if you notice some dead links or outdated information, please send a message to /u/wombat2combat[+1]

Happy reading and stay safe.

Author: /u/wombat2combat[+1]
Co-Authors: /u/Seraphim_X
Special thanks
to: /u/torr0t, /u/lslst, /u/My_s3cr3t, /u/Joskins, /u/b00mtown_Vendor, /u/hugsfordrugs, /u/darknetsolutions and /u/Vendor-Bubblehash, /u/calsuthrowaway, /u/CookyDough for creating valuable resources that were used in the DNM bible too
Proof-Readers: the community of /r/DarkNetMarkets and /r/DarkNetMarketsNoobs
PDF Formatting: /u/MrOwnageQc

Before you start

So you are about to read how to commit felonies and reduce the risk of getting caught. While nobody except you and reddit knows what exact pages you visit on reddit, it is strongly recommended to not use your default browser for any DNM related reddit activities. For example your browser could store the visited sites in his history and somebody else sees it when using your computer. Or reddit sells the account data it has collected from you to other companies (e.g. for advertising purposes) and so others know that you are very interested in buying illegal drugs online. Reddit also tracks you across different sites and links your different identities (e.g. your facebook account) together so they might even get your real name at some point.

It is **extremely easy** to protect yourself so that nobody knows that you even know about DNMs. So **please** take a look at the following chapter and follow the advice on there. It would be a shame if something that trivial ends up getting you prosecuted, wouldn't it?

About video tutorials

There are also video tutorials available but it is **not** recommended to use them. There are several reasons for that:

- You compromise your OpSec when watching them because youtube for example knows that you are interested in buying drugs online (since you can not watch youtube videos in the Tor browser, but you can easily read this guide using the Tor browser).
- They also miss a lot of crucial aspects that you need to know when buying.
- They are not cross checked by many community members like the DNM bible but just produced by one single person and then published.
- . . .

tl;dr stick to the DNM bible and if you still have questions that are not solvable by googling, you can make a post on /r/DarknetMarketsNoobs.

Using Reddit with Tor

What is Tor?

If you have not heard about Tor yet or are not very familiar with it, please take a few minutes to read this interesting explanation of it. It is absolutely crucial that you understand it, because the whole guide builds on that knowledge.
Note: the Tor network not only allows you to browse normal, clearnet sites (like reddit.com) but also onion-sites (also called hidden services). These are special websites which allow the visitor and the operator of that special website (the hidden service) to stay anonymous. So nobody knows the identity of each other. The DNMs you will use later in this guide are an example for such a hidden service.

About using reddit

You can log in and browse Reddit with all JavaScript (a programming language that can be used to de-anonymize you) blocked, but replying to comments or voting will not work. Unfortunately you also need to enable JavaScript for viewing Selfposts on NSFW marked subreddits (like /r/DarkNetMarkets or /r/DarkNetMarketsNoobs). However you can avoid that by using this Add-on. If you need to post replies to comments or make posts, follow the instructions in this article.

Instructions

Set security slider to high

The first thing you should do **every time** when you start the Tor browser is to set the security slider to high. That disables Javascript globally and does some other security enhancements.

When using the Tor browser on Tails you will have to do this every time you boot Tails again, because you can only store bookmarks for your Tor browser, but no other Tor browser configuration files.

Whitelist on NoScript

Now when the above is done, click on the "S" symbol in the top left of the Tor browser and select "Options" fromt eh drop down menu. Then switch to the "Appearance" tab and:

- check the checkbox for "Temporarily allow", and
- uncheck the checkboxes for "Allow scripts globally (dangerous)" and "About NoScript"

Now confirm the new settings by clicking on "OK". The you just have to go to reddit.com, click on the "S" symbol again and click on the drop down menu entry "Temporarily allow https://www.reddit.com".

Done! You can now create an account and make posts, write comments and vote with that account.

Solving the captchas

On reddit and other sites Tor users usually have to solve captchas at some point, especially for account creation or sending a PM (actions that are being abused often by spammers). You should be able to solve it by having enabled JavaScript for the site you are currently on (not globally or allow all scripts for this site, just reddit.com if you are on reddit for example). Google's so called reCAPTCHA is a special captcha where you have to select certain images. It should work with the above steps but sometimes you get an error like "Your computer or network may be sending automated queries. "To protect our users,we can't process your request right now."

They usually come right at the beginning when trying to solve the captcha. However to circumvent it simply get a new identity with the Tor browser button on the top left. You may have to do this a few times but eventually it should work. If you did it several times and it is still not working, wait some time and try again later. It should only be a matter of time to get around that error.

Account Creation

It is **highly** encouraged to create a new account for browsing, commenting and posting on darknetmarket related subreddits.
If you are still not convinced to create a new account take a look at snoopsnoo and check out how much information is publicly available about your account.

Note: although it currently looks like you need an email address for the account creation, you can just skip it by clicking the "Next" button. The same goes for choosing the 5 default subs you want to subscribe to at the beginning.

Post Account Creation

Go to your account preferences and:

- check the option "I am over eighteen years old and willing to view adult content"
- uncheck the option "label posts that are not safe for work (NSFW)"
- uncheck the option "make my votes public"
- uncheck the option "allow my data to be used for research purposes"
- check the option "don't allow search engines to index my user profile"
- uncheck the option "allow reddit to log my outbound clicks for personalization"
- go to this page, uncheck all the checkboxes and click on the 'save options' button.
  By the way: you can see your past logins. When you use Tor this will just be a long list of different IP Addresses and no identifying information about you. However you should assume that reddit stores much more data than just the data shown to you.

Browsing

- **Don't** post information that can be used to identify you.
- **Don't** log into the account outside of Tor.
- If your account is shadowbanned due to a bad Tor node, you can message and request the admins to remove the ban/shadowban on your account. If you are not sure if your account is shadowbanned, make a post on /r/ShadowBan.

Commenting

Please note that you need an extra free line between two of your paragraphs so that they get displayed as such. So just press enter twice after a sentence and you will write the future text in a new paragraph. That means it should look something like this:

```
paragraph 1
                          <free line here>
paragraph 2
```

Also if you want to reply to a comment, please click on the "reply" link directly under that comment and then type the answer in the newly appeared field. That way the user you are replying to gets a notification and can answer to your new comment.

Do you want to add more information to your initial post? Instead of making a new comment in your thread, click on the "edit" link directly under the text from your post, add the info you want and then confirm with save.

Mentioning usernames

To mention users, you have to write them like this: /u/wombat2combat[+1] so the targeted user gets a notification that he got mentioned. These notifications are turned on by default but keep in mind that they can also be turned off (although you should not do it if there is no good reason for it).
If you do the username mentions it the text of a selfpost (a post on reddit which just contains text, like this one), users will never get notified though. Therefore you have to do it in comments.
But if you mention more than three users in one comment (with '/u/username', writing their names normally like 'username' is okay), none of these users will get notified. So either mention three or less users in one comment or split the mentioning up into several comments.

Formatting PGP encrypted messages, signed messages or keys properly

To format PGP encrypted messages, signed messages or keys properly on reddit please follow these instructions.

Spotting possible shills

Shilling is an attempt by a user or vendor to discredit another person, promote their own product by acting like a satisfied customer, or any other attempt to raise or destroy business by using alternate accounts to pretend to be someone else. Here some tips on how to spot them.

Tails

Tails is a live operating system that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

- use the Internet anonymously and circumvent censorship (because all connections to the Internet are forced to go through the Tor network)
- leave no trace on the computer you are using unless you ask it explicitly and
- use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging

As you can see it is a pretty useful operating system for doing things that you do not want others to find out. An it gets even better: you do not need to install any additional tools for using darknetmarkets! Everything you need as a buyer is already installed.

Here is the default desktop of Tails. Pretty neat isn't it?

Note: you can not run Tails and another OS like Windows or OS X at the same time since they are both operating systems and your computer can only run one at a time.

Is Tails necessary?

YES. Even if you are think you are just a small fish and nobody will go after you. Let me give you an example: you use the Tor browser on Windows to make your order and everything seems to go fine. However unfortunately your package gets caught by customs because the vendor did not package it correctly. Now law enforcement starts to investigate because someone tried to send illegal drugs to you. One possible consequence is that they will deliver the package to you but raid your house shortly afterwards because you are in possession of illegal drugs (called a controlled delivery). Since Windows is not secure, they will find all the evidence they need to prove in court that you made the order. You would not have these issues with Tails because nobody can say what you did on there or say what files you stored on your persistence volume. Tails does not even leave a trace that it was booted on your computer!

So as you can see, Tails is not only to prevent you from getting caught but also for greatly minimizing the damage done if you get caught.

Do I need a VPN?

Normally, no.

Here an excerpt form the Tails website about VPNs:

Some users have requested support for VPNs in Tails to "improve" Tor's anonymity. You know, more hops must be better, right?. That's just incorrect -- if anything VPNs make the situation worse since they basically introduce either a permanent entry guard (if the VPN is set up before Tor) or a permanent exit node (if the VPN is accessed through Tor).

Similarly, we don't want to support VPNs as a replacement for Tor since that provides terrible anonymity and hence isn't compatible with Tails' goal.
Quoted from the official tails website

The main goals of a VPN would be to a) hide your tor usage from your ISP and b) add another security layer.

a) If you want to hide the fact that you are using Tor from your ISP, then you can select the "More Options" button on the Tails greeting screen and then select the Option "This computer's Internet connection is censored, filter or proxied". However if you are not living under an oppressive regime in which it is illegal or not possible to use Tor normally, it is not recommended to use that options since it only takes away resources from people who really need it.

b) Assuming that law enforcement would break the Tor network and get the IP address that you used to connect to the Tor network, they would know your real identity (or at least the one of the owner of the WiFi that you used). If you would use a VPN they would only get the IP address of the VPN server that you used (assuming that you set up Tails and the VPN correctly). However it is extremely unlikely that LE would try to attempt this just to bust a buyer that bought a few grams. There is no known case where a buyer got busted by a Tor de-anonymization attack and there will probably never be one.

There are **many** other OpSec factors which are more important and have a greater impact on your well-being, so please take care of them first before dealing with the Tails with a VPN topic.
If you still want to use Tor and a VPN, please read this.

Ordered without Tails before?

If you did not use Tails for previous orders you made a mistake. The problem is not that much that law enforcement will catch you now because of it, but rather that if you get in trouble later they can still find proof for your past orders and then prosecute you. Therefore it is important to remove the evidence immediately and step up your OpSec for future purchases.

The first step is to uninstall all the tools you used to order on your insecure OS. That includes the Tor browser, PGP tools, Bitcoin wallets, . . .

After that you have to overwrite the free disk space on your hard drive. That is to make it harder to recover the deleted tools (and therefore evidence that can get you in trouble) but it will not delete any other files you have on your hard drive. That means the uninstalled tools will get overwritten but your personal documents (e.g. your pictures in your home folder) will not be affected by it.

Here is how to do it on windows, mac and linux.
Note: this is not 100% secure. There are always log files that you OS might have created which still show that you used tools that are common for DNM buyers (e.g. PGP tools). Therefore it is important that you follow the steps mentioned above and keep **everything** related to DNM purchases on Tails in the future.

Using Tails on a personal/work computer

Using Tails on a computer doesn't alter or depend on the operating system installed on it. So you can use it in the same way on your computer, a friend's computer, or one at your local library. After shutting down Tails, the computer will start again with its usual operating system.

Tails is configured with special care to not use the computer's hard-disks, even if there is some swap space on them. The only storage space used by Tails is in RAM, which is automatically erased when the computer shuts down. So you won't leave any trace on the computer either of the Tails system itself or what you used it for. That's why we call Tails "amnesic".

This allows you to work with sensitive documents on any computer and protects you from data recovery after shutdown. Of course, you can still explicitly save specific documents to another USB stick or external hard-disk and take them away for future use.

Quoted from here.

tl;dr you can use Tails on your normal computer and do not have to buy a burner laptop.

Using Tails on your own WiFi

If you use Tails (or Tor in general) on your own WiFi, your ISP will only know *that* you are using Tor but not *what* you are doing exactly. If you do not want your ISP to know that you are using tor you can tell Tor to use bridges on the Tails greeting screen (select "Yes" for the more options question and after pressing forward select the "My computer's Internet connection is censored, filtered or proxied" option). That will obfuscate the fact that you are using Tor from your ISP although it is not necessary as long as you are not living under an oppressive regime which blocks Tor and/or makes the use of it illegal. If that is not the case, please do **not** use bridges as it would take away resources from people who actually need them.
So only reason for using another WiFi than your own is that an attacker would not get your real IP address in case of a de-anonymization attack but the one from the network you are using (e.g. the starbucks WiFi). However these attacks are unrealistic for buyers and the risks that this method brings along (e.g. someone shoulder-surfing or a camera recording your face and/or screen) make it not worth it for buyers. Therefore using your own WiFi along with following **all** the other tips in the DNM bible is a much better solution.

Is it okay to use a WiFi with login?

Sometimes you will have to log into WiFis with credentials that in some cases are also tied to your real identity (e.g. a college WiFi). Tails spoofs all MAC addresses by default, that means that a system administrator would only see that a seemingly other device than your default one logged in with your credentials. That adds some plausible deniability, because you can claim that someone stole your login credentials and logged in with them on another computer. Furthermore nobody knows what exactly you are doing since the whole internet traffic that Tails produces is routed through the Tor network and is therefore encrypted and nobody knows where it goes. So to make it short: yes you can use Tails in a WiFi that requires you to log in.

Are DNS leaks an issue?

When using Tor your computer does not make the DNS requests for the sites you visit but the exit node (the last node in the chain of relays that route your Tor traffic) makes the DNS requests for you. That is done because Tor does only support TCP but not UDP traffic. So just use Tails, which routes all your traffic through the Tor network, and you will not have to worry about it.

I want to buy a new computer anyway, which works best with Tails?

Many computers are able to run Tails, but if you have the choice you should keep the following tips in mind when picking a computer:

- Do not use a mac, macbook or any other apple device because they can not always run Tails.
- Make sure that no hardware parts in the computer are on the list of known issues.
- If possible choose one that has not windows 8 or 10 installed because they are more likely to cause issues than the ones with older windows versions or no OS at all.

Some users also report that alienware computers are working good with Tails. And here is a list of laptops that work good with Tails too.

Is running the latest version of Tails necessary?

Yes. It is absolutely crucial that you always use the latest version of Tails since the updates usually fix security vulnerabilities to which you are vulnerable by not upgrading. So take the few minutes and upgrade Tails**as soon** as you get the notification that an update is available.

Compatible hardware

If you run into problems with Tails and your hardware, you might want to buy one of these if you can try using Tails on another computer:

USB sticks

The following listed USB sticks will work with Tails (tested with Tails 3.0).

Note: some USBs are giving the error message "_____USB is configured as non-removable by manufacturer and tails will fail to start on it" This is even happening to drives that were known to work fine before. The Tails team are aware of this and have offered a work around that can be found here. If you want to read more about the bug report you can do so here. Should be fixed in Tails 3.1, due out Aug 8.

- Kingston Data Traveler SE9 G2 16GB
- Lexar Twist/Turn Jump Drive 16GB
- Mushkin Atom 16GB
- Onn 32GB (Walmart brand)
- Transcend Jetflash 700 16GB

All of the drives above can be found online easily. They range from $6-15 each. The Onn is a Walmart brand and can be found in most stores. The Lexar can be found in most Target stores.

The Onn is manufactured by Sandisk as a private label for Walmart(just found this out but since passed testing left it in there)

Original post

USB WiFi adapters

Note: before you buy extra hardware, try using an Ethernet cable that you plug in your router and your computer. It is usually the easiest solution and recommended over buying a new WiFi adapter.

These USB WiFi adapters are known to work with Tails:

- https://www.amazon.com/CanaKit-Raspberry-Wireless-Adapter-Dongle/dp/B00GFAN498/
- https://www.amazon.com/Edimax-EW-7811Un-150Mbps-Raspberry-Supports/dp/B003MTTJOY/
- Belkin N300 high-performance WiFi USB adapter

USB Ethernet adapters

These USB Ethernet adapters are known to work with Tails:

- http://plugable.com/products/usb3-e1000
- http://plugable.com/products/usb3-hub3me

Can I buy USB sticks that already have Tails installed on it?

No. Nothings prevents the seller from modifying the Tails installation which is on the USB stick so that it for example sends all the passwords you use to them. Always download, verify and install tails by yourself.

Why is JavaScript enabled globally by default and the security slider set to low?

There are a lot not so tech savvy Tails users who would have a hard time dealing with all the different settings if they were all set to high and they would have to make adjustments. Therefore the developers decided to set the default settings to not so strict values to make the Tails experience better for these users.

You however, have to make sure that you set the security slider to high every time you start the Tor browser (because it is not possible to save the security slider settings between the reboots, even with persistence enabled).

Got Problems?

Common issues

As mentioned previously, Tails works on *almost* any computer. So it is possible that your installation will not go as flawlessly as it usually should. However there are many way to solve issues that might come up. Please go through the following options one after another if you have difficulties getting tails on a USB stick or to boot:

- Did you disable secure boot?
- Look at the list of known issues and check if there is hardware on it that you use too (for example a USB brand or a certain network card). If it is on the list please check if there is also a solution described, if yes try it. Sometimes it is best to try booting Tails on another computer to see if it is working there, so you know if your computer is the problem.
- Tor is not ready or other internet connection issues? Boot Tails, log in and do something else for about 5 to 10 minutes. Then go back and check if Tor is ready now by opening the Tor browser. If you still get the "Tor is not ready" warning, reboot Tails and try again. If that does not work try disabling MAC address spoofing on the Tails greeting screen when rebooting (select "More Options", click on "Forward" and click once on "Spoof all MAC addresses").
- Are some password not getting accepted although they should be correct? Please check that you set the correct keyboard layout on the Tails greeting screen as described here.
- Having trouble booting Tails although you followed the instructions on the Tails website? Check that your USB stick is not on the list of problematic USB sticks (e.g. SanDisk USB sticks are not a good choice for a Tails installation). Also try one of these USB sticks and see if they work.
- If Tails freezes after you press enter in the boot screen, try not pressing enter to boot but letting Tails count down itself. If Tails worked previously but suddenly has freezing issues, try rebooting a couple of times. Some users report that it worked after about 5 tries.
- Does Tails freeze and only shows you a blue screen? A user reported that the following worked for him: When Tails first boots up (before choosing tails or tails failsafe version), press tab to open up the console. Don't modify anything, just type all of the following commands: nouveau.modeset=0 modeset.blacklist=nouveau noslash One of

the commands above should get you past the blue screen. Unfortunately you will have to enter the commands every time you boot but it's better then it not working at all.

- Having issues accessing your persistence data? You may be able to fix your problem by simply re-running the persistence configuration tool: Applications > Tails > configure persistent volume and enable the same options that you had before. Then reboot.
- For OS X: If Tails does not show up when holding the alt key upon restart, try the following. Install rEFInd (if you use a Mac with El Capitan or later, rEFInd may not install properly). Then temporarily disabled SIP: hold command + R when you see the Apple logo after restarting, then go to Utilities -> Terminal, then type "crsutil disable" in the Terminal window then press Enter, then restart as normal and install rEFInd, then repeat the process but this time type "crsutil enable," turning SIP back on.
- Can you not connect to your WiFi because it keeps asking for the password but you know you entering it correctly (e.g. it just asks for password after a few minutes of trying to connect)?. It could be an issue with Tails not recognizing drivers, so a solution would be to use a WiFi adapter or a wired connection (i.e. plug in an ethernet cable that is connected to your router).
- Does the Tails installer does not work when clicking an option? Try this.
- Do you get asked for a password when you want to install Tails by cloning? If the process is like this: you click on "install by cloning" it shows the USB stick you want to clone Tails to, so you click on "install Tails", then get asked to confirm the device selection, which you do, and are then told that authentication is required to "unmount General UDisk (/dev/sda1)" mounted by another user" (or a similar message) - which is when it asks you for the password. If that is the case, follow the instructions here (for the USB stick that you want to clone Tails on) but use *fs=fat32 quick* instead of *fs=ntfs quick* in step 9. If that does not work please try using two different USB sticks and avoid using the ones that are on the list of known issues.
- If you have trouble with copying the persistence volume with these steps, please read the following thread and see if the final solution there works for you.
- Can not open Electrum any more? Follow this.
- Issues with your screen resolution? Check out this.
- Are you using a mac and have issues installing/booting Tails? Try following these steps.
- Icons and information located on the top right corner of the screen disappeared?
- Boot problems and an error message like this "(initramfs) unable to find a medium containing a live file system on custom Live USB"? A user reported that using rufus and choose a different partition scheme helped. Also try holding the power button down for

10 seconds till the computer turns off and then turn it on again to see if it works with the second boot.

Still not solved?

Research your problem. That means using a search engine and the search function of the /r/DarknetMarketsNoobs subreddit to search for solutions for your problem. If that does not help you can make a post on /r/DarkNetMarketsNoobs **but** remember to give it a meaningful title (i.e. "When booting Tails I just get a blank screen" instead of "need help plz").

Installing Tails

The Tails website has a very detailed documentation on how to install Tails from various OS, please follow them here.

Note: if you use another keyboard layout than the default American one, you need to change it on the Tails greeting screen. Just click on the drop down list on the bottom right and scroll through the list. If you can not find yours, select the "Other..." entry at the bottom of that list and then start typing the name of your keyboard layout, i.e. if you want the Serbian one, start typing "ser" and it will automatically jump to it. After you selected the correct one on the list, press enter twice and you will be back at your Tails greeting screen with the changed keyboard layout.

If you run into issues, please check the "Got problems?" chapter **before** posting on /r/DarkNetMarketsNoobs about it.

Tip: if you choose the 2 USB option (which uses an "intermediary Tails", which is the one on the first USB stick), you can format that first USB stick after you are done installing Tails and everything is working (e.g. the persistence volume is working too). It is just used to install the final Tails and not needed afterwards.

Note: you can download Tails over the clearnet (i.e. without using the Tor browser or a VPN). It is not illegal to download or use Tails. **But** you have to make sure that you verify the downloaded .iso file afterwards as it is described in the linked guide. Otherwise you could easily end up with a malicious .iso file which sends all your passwords to someone who will later steal all your bitcoins.

Important settings and tips

- **Every time you start the Tor browser, you have to set the security slider to high.** This disables JavaScript (a programming language that websites can use to de-anonymize you) by default and enables some more security features.
- If you use clearnet websites that require JavaScript (like reddit.com if you want to post, comment or vote), change the NoScript appearance so you can easily allow and disallow the scripts that you need as described previously.
- **If a DNM site ever asks you to enable JavaScript, leave *immediately*.** Ideally warn the community on /r/DarkNetMarkets too by making a post there.
- **When shutting Tails down, it is best to wait until your computer is shut down completely before removing the USB stick.** Tails will tell you that you can remove your USB stick now and shortly after that the computer shuts down completely.
- **Is it okay to leave Tails logged in?** No, you should shut it down when you are not using it anymore for a longer period of time (e.g. 10 minutes). Yes, it is a pain in the butt to restart your computer every time, but it is good security practice. Otherwise law enforcement could just visit you and would have all the unencrypted evidence they need even though you used Tails.
- **Is it okay to resize the TorBrowser window?** Changing the default size of the TorBrowser window should generally be avoided because it makes it a lot easier to track you across different sites. Although it is usually only an issue if you also have enabled JavaScript (which you should never do when browsing DNMs), it can also be done using only CSS (a style sheet language that you can not disable like JavaScript). Here is an example how that is possible with CSS. It is not too alarming, however, so just make sure you set the security slider to high every time you start TorBrowser, and do not change the default size of the TorBrowser window.
- **Never run Tails in a virtual machine (VM).** That practice is discouraged by the Tails developers. Only use Tails as a standalone operating system on an USB stick for example. More on this topic.

Setting up the persistence volume

Normally Tails forgets every change you made on it when you reboot (that is why it is called amnesiac). However when you want to order from DNMs you need t save some files. This is possible by setting up the persistence volume which allows you to store data which will not get deleted when you reboot.

Here is how to set up the persistence volume, just follow the instructions there and make sure that you select all the following points when you get asked what data you want to store:

- Personal Data
- GnuPG
- Network Connections (if you use WiFi)
- Browser bookmarks
- Bitcoin Client

Note: if you want to store something in text files for example (after you have enabled the persistence volume and rebooted), these files have to be stored under home/Persistence.
Make sure the persistence volume is actually working before you use it. That means for example set up a wallet like it is described later in the bible and then reboot to see if you can still access and read all the data you created.
Note: you absolutely have to make sure that you do not forget or lose your persistence password. If you lose it, you also lose access to your whole Tails installation which includes PGP keys, market accounts, Electrum wallet if you have not written down your seed (which you should do), . . .

Upgrading

To upgrade Tails just follow the guide on the Tails website.
Does it say there is not enough space? Then you have to do a manual upgrade. If you wonder why there is not enough space on your large USB stick, here and explanation.

Backing up

It is **crucial** that you back up your data. Not just the data you have on Tails but all your other documents too. However this chapter will only deal with how to back up your persistence data which is stored on Tails. You probably do not want to loose access to your market account and wallet with all your money in it, so you **need** to do the following steps.
Yes, nobody likes to make backups but you will be *really* annoyed if you loose your Tails USB stick and your market account and bitcoins with it.

Since it is only reasonable to back up data if you already have some, you have to go back to this chapter after you have set up all the other tools and accounts. So before you make your first purchase you need to go back here and do the backup.

In the following you have to ways how to back up your Tails persistence data:

- **Method 1**: is a bit easier because you have to make less steps, but takes a bit longer and also produces a bigger backup file. It also makes a complete copy of your Tails USB stick, instead of just copying the persistence data, hence the bigger backup file but it will be faster to restore the backup.
- **Method 2**: takes not so long (about 5 to 10 minutes) but requires you to copy and paste a few commands. In case you need to restore your Tails USB stick from that backup it will take a bit longer than the first method.

Choose a method which is more suitable for you.

Method 1

Backing up your entire Tails USB stick

Boot your primary OS (e.g. Windows or OS X) and download and install the tool USB Image Tool. Then plug in your Tails USB stick and use the tool to make an image of it. Then copy that image to another USB stick.

Remember to stash your USB stick with the backup somewhere safe where nobody will find it easily but you can still retrieve it after your properties got searched and your assets seized.

Restoring the backup

You can just plug in the backup USB stick and boot it, since it contains all Tails data files and not just the persistence files.

Method 2

Backing up your persistence data

Reboot Tails and select "Yes" for the More Options question on the Tails greeting screen and enter the password for your persistence volume. Click on "Forward" and set an administrator password. It does not have to be that strong because it will be only used for this session. Confirm by clicking on "Login".

Variant A: Using a script (shorter)

Instead of entering all the commands one by one, you can also use a small script. To do that just click on "Applications" the top left corner, go to the category "Accessories" and select "Text editor". Then paste the code below into it and click on the save button. Store it as script.sh on your desktop and close the editor window after that.

```
#!/bin/bash

DATE=`date +%m-%d-%Y-%H.%M.%S`

FNAME="$DATE-backup.tbz2.gpg"

OUTDIR=/home/amnesia

echo "Creating backup: $FNAME"
echo "Placing in directory /home/amnesia"

cd /live/persistence/TailsData_unlocked
tar cjf - . | gpg --cipher-algo AES -c - > $OUTDIR/$FNAME
chmod ugo+rw $OUTDIR/$FNAME
```

```
cd -
```

Then switch to your desktop, right click on the script.sh file, select "Properties" and switch to the tab "Permissions" on the newly appeared window. Check the box "Allow executing file as program" and close the window again.

When you are on your Tails desktop, click on "Applications" the top left corner and go to the category "System Tools". Select the "Root Terminal" entry and enter the root password you have previously set.

Then enter the following line and press enter:

```
/home/amnesia/Desktop/script.sh
```

After you press enter it will prompt you for a password. Choose a strong one because if law enforcement can guess it, they have all the evidence they need laid out in front of them. Note: when you enter it, the characters will not appear in the terminal. Just enter your password, press enter, confirm it by entering it again and press enter again.

Wait till it is finished, i.e. the last line of the root terminal (at the bottom) starts with "root@amnesia:/home/amnesia#". Then you can close the terminal window and follow the directions under Copying the backup file.

Variant B: Entering commands manually (longer)

You can also choose to enter the commands to make the backup manually all by yourself. To do that just do the following steps.

When you are on your Tails desktop, click on "Applications" the top left corner and go to the category "System Tools". Select the "Root Terminal" entry and enter the root password you have previously set.

Now enter the commands one after another by copying them and then right click in the root terminal and select "Paste", after that press enter. Wait after each one till it is finished, i.e. the last line of the root terminal (at the bottom) starts with "root@amnesia:".

```
cd /live/persistence/TailsData_unlocked/
```

This goes into the directory where all your persistence files are stored.

```
tar cjf - . | gpg --cipher-algo AES -c - > /home/amnesia/YYYY-MM-DD-backup.tbz2.gpg
```

This backs up all files in that directory and pushes them into a file called YYYY-MM-DD-backup.tbz2.gpg in your persistence file folder. Replace the date placeholders with the actual current date so you later know when you made this backup just by looking at the filename (e.g. 2017-02-10-backup.tbz2.gpg).

After you press enter it will prompt you for a password. Choose a strong one because if law enforcement can guess it, they have all the evidence they need laid out in front of them. Note: when you enter it, the characters will not appear in the terminal. Just enter your password, press enter, confirm it by entering it again and press enter again.

```
cd /home/amnesia/
```

This goes into your home directory.

```
chmod ugo+rw YYYY-MM-DD-backup.tbz2.gpg
```

This makes it possible for every user to read and write the backup file. It is necessary because you created the backup file as root and only he would be able to read and write the file. That does not mean that everybody can read the content of your encrypted backup, it just allows you to copy it to your USB stick in the next step. The content of the backup is still only readable if you know the password you set earlier.

Note: you can press TAB once to use the autocomplete function. That means just type the beginning of the long backup filename (e.g. "2017-") and then press TAB. That will add the rest of the filename to your command.

Now you just have to follow the next part: Copying the backup file.

Copying the backup file

Almost done! Now just plug in your USB stick on which you want to store the backup file (it does not need additional encryption because the backup file is already encrypted itself). Then go into your home directory (by clicking on "Home" on your Tails desktop) where you will see the backup file. Copy it to your USB stick that you plugged in by clicking on the name of your USB stick on the left sidebar and then pasting the backup file.

However, it would be a shame if you lost your Tails USB stick but think you at least got a backup of it, just to later discover that there is a problem with it and you really lost all your data permanently. This would suck, so invest one more minute in checking if the backup was successfully:

- right click on the YYYY-MM-DD-backup.tbz2.gpg file and select "Open With Decrypt File". Then you will see a file called YYYY-MM-DD-backup.tbz2 in the same directory. Double click on it and go through the folders a bit to see if your persistence files got backed up correctly (e.g. go into the folder called "persistence" and check if you can open some txt files you stored there).

  If that is the case you can delete the YYYY-MM-DD-backup.tbz2.gpg and the YYYY-MM-DD-backup.tbz2 file from your Persistence folder, but do not delete the YYYY-MM-DD-backup.tbz2.gpg file from the USB stick.

  Remember to stash your USB stick with the backup somewhere safe where nobody will find it easily but you can still retrieve it after your properties got searched and your assets seized.

  It is also recommended to follow the 3-2-1 rule:

  3 copies of your data, 2 different mediums (USB, CD/DVD, Paperkey), 1 stored offsite (Bank Box, Friends/Relatives, etc).

Restoring your persistence data

Now if the worst case happens and you loose your Tails USB stick or it gets destroyed you have to do the following to restore your data. Create a new Tails USB stick and enable the persistence volume on it. Make sure that you enabled the persistent volume for the exact same categories as you had on your old one (e.g. they should be Personal Data, GnuPG, Network Connections (if you used WiFi), Browser bookmarks and Bitcoin Client).

Reboot Tails and select "Yes" for the More Options question on the Tails greeting screen and enter the password for your persistence volume. Click on "Forward" and set an administrator password. It does not have to be that strong because it will be only used for this session. Confirm by clicking on "Login".

When you are on your Tails desktop, click on "Home" and select your USB stick from the left sidebar of the file explorer window. After you left clicked on the USB stick you will see the content of it, it should contain the backup file (YYYY-MM-DD-backup.tbz2.gpg). Now hover over the entry of your USB stick on the left sidebar and

you should see where it is mounted, e.g. if your USB stick is called "backup", the path should be "/live/amnesia/backup". Remember that path.

Then click on "Applications" the top left corner and go to the category "System Tools". Select the "Root Terminal" entry and enter the root password you have previously set.

Now enter the commands one after another by copying them and then right click in the root terminal and select "Paste", after that press enter. Wait after each one till it is finished, i.e. the last line of the root terminal (at the bottom) starts with "root@amnesia:".

```
cd /live/persistence/
```

This goes into the directory where all your persistence files are stored.

```
rm -r TailsData_unlocked/*
```

This removes all files currently stored on your persistence volume since you want to replace them with your old ones from the backup).

```
cd TailsData_unlocked
```

This goes into the directory where all your persistence files were stored.

```
cp /live/amnesia/backup/YYYY-MM-DD-backup.tbz2.gpg ./
```

This copies the backup file from your backup USB stick (which is called "backup" in this example) to the directory where all your persistence files were stored. There may be some issues if your USB stick name contains spaces or other special characters. In that case copy the backup file to your home folder (using the file browser) and then enter the command "cp /home/amnesia/YYYY-MM-DD-backup.tbz2.gpg ./" instead of the above.

Note: you can press TAB once to use the autocomplete function. That means just type the beginning of the long backup filename (e.g. "2017-") and then press TAB. That will add the rest of the filename to your command.

```
gpg -o backup.tbz2 --decrypt YYYY-MM-DD-backup.tbz2.gpg
```

This decrypts the backup file, enter the password for it in the terminal when asked for it.

```
tar xvjf backup.tbz2
```

This extracts the files from the decrypted archive.

```
rm YYYY-MM-DD-backup.tbz2.gpg
```

This removes the encrypted backup file from your current directory because you do not need it any more.

```
rm backup.tbz2
```

This removes the decrypted backup file from your current directory because you do not need it any more.

Now reboot Tails and see if you have your old files back by:

- starting Electrum and checking the balance
- checking the home/Persistence folder for your old files
- checking the browser bookmarks by starting the Tor browser
- checking the PGP keys by clicking on the clipboard icon, selecting "Manage Keys" and then going in the "GnuPG Keys" section on the left sidebar

  If you get an error that the clock failed to synchronize (your old data should still be recovered) just reboot Tails and you should be able to connect to the internet again.

Whonix

When you should use this guide

This guide shows an alternative, but still secure setup. Usually Tails is the easier and faster solution, so try it out if you have not already.
However sometimes users have issues with it that can no be resolved by reading through the DNM bible, googling the issues and asking on dedicated forums (like /r/DarknetMarketsNoobs or /r/tails).

In these cases it is better to follow this guide since it is less hassle for you and still gives you a reasonable secure setup instead of a horrible one which for example involves windows (the get-in-jail-free card).

General

This guide is for installing Whonix on a Linux distribution such as Ubuntu, Debian or Linux Mint. It is important to choose a distribution that offers **Full Disk Encryption** such as the named ones. Otherwise, your whole setup would be useless. If you are not really keen with Linux, it is recommended that you use Ubuntu or Linux Mint in the following as they are easy to use and there are many resources available if you run into issues.
->DO NOT USE WHONIX ON WINDOWS OR OS X.<- They are insecure and cancerous to your OpSec. If you want to play the game, do it right.
Note: more security can be achieved by using Qubes with Whonix. However this is more for technically advanced people and higher profile users and therefore a smaller target group. This guide is for using Whonix *without* Qubes, guides for Qubes will follow at some point in the future though.

Related subs for additional resources:

- /r/Whonix
- /r/VirtualBox

What is Whonix?

It's basically like a sandboxed and *tor*rify'd Linux operating system (OS) which you can run while running your usual operating system (called host OS). That means you boot

for example Ubuntu from a USB stick and then run Whonix (the guest OS) within your booted Ubuntu (an OS in an OS). In Whonix's words:

Whonix is a desktop operating system designed for advanced security and privacy. It realistically addresses attacks while maintaining usability. It makes online anonymity possible via fail-safe, automatic, and desktop-wide use of the Tor network. A heavily reconfigured Debian base is run inside multiple virtual machines, providing a substantial layer of protection from malware and IP leaks. Pre-installed applications, pre-configured with safe defaults are ready for use. Additionally, installing custom applications or personalizing the desktop will in no way jeopardize the user. Whonix is the only actively developed OS designed to be run inside a VM and paired with Tor.

For more information please visit their website.

Note: you could also easily use Tor in combination with a VPN when using this guide. To do that simply run the VPN software on your host OS (e.g. Ubuntu or Linux Mint). **However** this is often unnecessary, especially as a buyer, since DNM users get frequently busted because they made other, more simple mistakes. So it is far more important that you take care of these other factors first by reading and following every page of the DNM bible, instead of jumping on a rather unnecessary OpSec measure (using a VPN).

Here a quick comparison of Whonix with other OS.

Installing the host OS

To be able to run Whonix, you must first choose and install the hos OS, on which you will later run Whonix. Like a program that you run on an OS, only that the program in this case is a full OS itself.

Note: install the host OS on an USB stick with much space or an external hard drive. It should have at least 16GB, more than 64GB are not necessary.
As mentioned at the beginning, if you are not that tech-savvy you should use Ubuntu or Linux Mint. Just follow these and these instrucutions on how to install Ubuntu with Full Disk Encryption (FDE). If you want to use Linux Mint follow these instrcutions and choose the option "Encrypt the new Linux Mint installation for security" during the installation.
Tip: it is recommended to use an external SSD or at least a USB 3.0 stick.

Installing Whonix

Installing

Before you install Whonix, a small note that it consists of two different OS: the Gateway and the Workstation. When you set everything up you do all your work (like using the Tor browser, decrypting PGP messages, . . .) on the Workstation. The Workstation contacts the Gateway in the background (i.e. you do not have to do anything) and sends the entire internet traffic that you produce on the Workstation to it.

The Gateway then connects to the Tor network and sends your traffic through it. That gives you an additional security advantage. So you basically run three operating systems (OS) at a time: your host OS (e.g. Ubuntu), Whonix Gateway and Whonix Workstation. Normally you can only boot one OS at a time on your computer, but with a special software (called VirtualBox) you can run more. Do not worry it is not that complicated, just follow the steps below.

To install Whonix just follow the instructions on this page. For the step 2 (called "Install Whonix") of the linked guide you need to open the Konsole. Do that by simply pressing CTRL + ALT + T and then enter the command from the guide.

Do not forget to verify the downloaded Whonix files as explained in the guide. Also change the default password ("changeme") on the Whonix Workstation and Gateway.

OpSec improvement

Since you are running Whonix, please also consider using this Add-On to warn other users if a DNM executes JavaScript.

Starting and shutting down Whonix

Starting

First, start the Whonix-Gateway. Select the Whonix-Gateway in VirtualBox, and hit the big Start button or double click on the entry in the list on the left.

Tip: enlarge the Gateway and Workstation windows after you started them for improved usability.

Once the desktop environment has loaded (i.e. you see the desktop), open the Konsole by double clicking on the Konsole-shortcut on the desktop and change your password by hitting ENTER after typing

```
passwd user
```

- The default username is: user
- The default password is: changeme

Change the password to what you want it to be. It does not has to be that complex but you should not use the default one either.

Note: to change the keyboard layout, press the Start button at the bottom left -> Computer -> System Settings -> Input Devices -> switch to the "Layouts" tab on the by default selected keyboard category -> check the "Configure layouts" checkbox -> click "Add" and add your desired laypout. Then remove the default English (US) layout and save the settings by clicking "Apply".
Tip: you can copy the commands and then right-click in the Konsole-window (terminal) and select paste. Alternatively you can also press CTRL + SHIFT + V to paste the command into the Konsole.

After that update your system by typing the following command into the Konsole

```
sudo apt-get update && sudo apt-get dist-upgrade
```

Important: Whonix checks on the Gateway and Workstation every 24 hours if updates for the installed software are available. If yes you get a window that contains something like this:

WARNING: Debian Package Update Check Result: apt-get reports that packages can be updated.

[some more text how to open the Konsole]

sudo apt-get update && sudo apt-get dist-upgrade

Simply copy the command, open the Konsole according to the instructions, paste the command and press ENTER. Then it prints out a few lines in the window and asks you with a message like the following if you want to install the updates:

Do you want to continue? [Y/n]

Type y and press ENTER. Then wait till it finish, i.e. the line at the bottom of the Konsole window begins with user@host:~$. Then you can close the window and reboot Whonix (Gateway and Workstation).

Sometimes you also only get updates on the Gateway and not the Workstation, or the other way around. In that case, do not worry and apply the updates as described above.

If the checking for updates somehow fails, reboot the Gateway and the Workstation and see if the checking works this time. If the update check then does not run autmatically (after the reboot), run the update command manually by entering the *sudo apt-get update && sudo apt-get dist-upgrade* command from above manually in the Konsole.

If there are no updates available, i.e. your system is up to date, you will still get a window after the check is finished which shows a few lines of text which contain "INFO" in green font at the beginning of some lines.

Now after all that is done, go back to the VirtualBox window on your host OS, select the Whonix-Workstation, and click the big Start button. Then go back to to the beginning of the "Starting Whonix" section of this guide and do all that stuff in your Workstation desktop environment.

Note: you only need to change your password once (once on the Gateway and once on the Workstation), not every time you reboot Whonix.

After you did the whole updating for the Workstation too, you can download the Tor borwser. To do that, double click the Tor Browser icon on your desktop. Follow the prompts, and get the version you want. Make sure that the version does not contain an "a" or "b" which stands for alpha and beta versions that are not yet ready to be released for all users and may contain bugs.

Then launch the Tor Browser by double clicking on the desktop icon called "Tor Browser (AnonDist)". Now you need to configure it a bit to make it more secure. First set the security slider to high. The link goes to the Tails website but since it is about the Tor browser, it also applies to Whonix. Fortunately, Whonix preserves your settings so you do not need to set the slider to high every time you reboot Whonix.
Now JavaScript (JS) is disabled globally, which is how it should be if you only use DNMs. However if you want to use reddit or other sites that require JS, please follow these instructions.
Tip: On on the top right corner, click on the icon with the three horizontally stacked bars and choose "Customize". Drag the bookmarks and downloads icons up to your menu bar or your tool bar so you can use them easily. Click "Exit Customize" in the green box on the lower right side.
Important: on the Workstation, wait till the small globe icon with the clock is green before starting the Tor browser. That means that the time synchronization was successful. If it is yellow just wait some more time before starting the Tor browser. If it has a small red and white cross, it means that the check failed. In that case restart the Workstation and wait till the symbol goes green.

Shutting down

Always close out Whonix in reverse order. That means, shutd own the Workstation first, then shutdown the Gateway. After the VirtualBox windows for both are closed, you can also close VirtualBox. To finish, shut down your host OS after that.

If you are running terminal-based version of the Gateway for performance reasons, just enter the command

```
sudo poweroff
```

and press ENTER to shut the Gateway down.

Performance tips

Running essentially three operating systems (OS) at the same time can take up some resources from your computer. Especially if you are all doing it from a USB stick and not an internal SSD for example. So in the following some tips which you can follow if you want to improve the performance of your Whonix setup. If everything is running smoothly, you do not need to follow them (if it is not broke, do not fix it).

Make sure you have followed the previous Whonix chapters already so you are improving a secure setup and do not have to start all over again (e.g. because you use Whonix on Windows).

Note: most of the tips that involve changing VirtualBox settings for VMs (the Whonix Gateway and Workstation) require the the the VMs to be shut down. So only boot up your Linux distribution that you use for running Whonix (e.g. Ubuntu or Linux Mint) but do not start Whonix too.

Using more CPUs for the Workstation

Since the Workstation will do the most amount of work, it should also be able to make good use of your CPUs. To ensure that, open the VirtualBox window -> right-click on the "Whonix-Workstation" entry on the left -> select "Settings" -> go to the "System" category -> switch to the "Processor" tab.

Now you should see two sliders: "Processor(s)" and "Execution Cap". If the "Execution Cap" slider is not already set to 100 percent (on the right end), please drag it there. If the "Processor(s)" slider is not disabled, set it to the middle value (i.e. if the maximum is 4 CPUs set it to 2 or if the maximum is 8 CPUs set it to 4).

If you can not move the slider you only need to do one additional step, which is enabling an option called "VT-x technology" in your BIOS or UEFI settings. This may sound complicated but is pretty easy and can give you an enormous performance boost. Here are the steps, you basically need to get into your BIOS / UEFI settings -> search for an option called something like Virtualization or VT-x -> enable it -> save settings and reboot.

Then when you rebooted with the new settings, the "Processor(s)" slider should not be disabled any more. Now you can change it according to the instructions above.

Reducing the RAM for the Gateway

You can reduce the amount of RAM that the Gateway is allowed to take up which helps reducing the overall work load for your computer. Read this first and then you can adjust the memory in VirtualBox.

Open the VirtualBox window -> right-click on the "Whonix-Gateway" entry on the left -> select "Settings" -> go to the "System" category. Now you should see a slider called "Base Memory" under the "Motherboard" tab. As mentioned in the previous link, the minimum requirement for the Gateway is 256 Megabyte RAM. You should set it to a bit more than that (around 300), apply the other performance tips as well and then see if the Gateway and Workstation are running more smoothly. If you then still have performance issues, you can reduce the memory down to 256 Megabyte.

Now you will only see the terminal-based version of the Gateway even when it is fully booted. This saves the computer some resources but you will still be able to do all the tasks you need to do on it (which is essentially only updating the software if there are updates available).

So in the future start the Gateway -> wait till you get the login prompt -> enter your username (default "user") and password (default "changeme") and press ENTER. After that the Gateway will hijack your command line input when it is checking for software updates, meaning that it will print out some lines without showing you the usual input line where you can enter commands. In such cases just wait till it is finished and gives you a message ending with "Please feel free to press enter to return back to your normal prompt".

So press ENTER and check if the above lines (which show the result of the software update check) contain something like "[WARNING] [whonixcheck] Debian Package Update Check Result: apt-get reports that packages can be updated." If you see such a line, enter the command

```
sudo apt-get update && sudo apt-get dist-upgrade
```

and press ENTER. That command should also be shown to you in a few lines under the line which contains the note that packages can be updated. Then when you get the line "Do you want to continue? [Y/n]" press either ENTER (which answers the "Update? Yes / No" question with the answer that was capitalized, in this case the "Y" for "Yes") or type y and press ENTER.

Tip: you can also copy that update command by highlighting it -> right-click on it -> select "Copy" -> left click again to un-highlight it and return to your input-line -> right-click -> select "Paste".

This process replaces the usual update process which shows you the notification window where you copy the update command and paste it into the terminal (like you do on the Workstation).

To shut down the Gateway in the future just enter the command

```
sudo poweroff
```

and press ENTER.

Using an SSD

If you are not already using an SSD for your Ubuntu or Linux Mint installation, consider switching to one. It offers significant speed boosts over a normal USB stick. You can easily buy a cheap external SSD online or in stores. They do not need to have much capacity either for this use-case, 50 or 75 Gigabyte would easily be sufficient. If that is not an option consider using a USB 3.0 stick on a 3.0 port over a 2.0 one which gets you better results.

Bitcoin

Bitcoin is a cryptocurrency and a payment system. To get some basic information please take 5 minutes of your time and read the texts on these two sites:

- bitcoinsimplified.org
- bitcoin.org

F.A.Q.

If the price of bitcoin increases/decreases, does that mean the listing on the DNM become more expensive/cheaper?

Not at all. The price will still be the same. Say if a vendor has a listing for $20, and the price of bitcoin drops, the item will still be $20, but the bitcoin equivalent will change. the vendor will only loose money after someone has made a purchase and the price of bitcoin drops.

Do both Bitcoin wallets have to be online at the same time?

No, to make transactions it is not necessary to have both Bitcoin wallets (the sending and receiving one) to be online. The transaction will be processed automatically, just make sure you follow the tips in the following chapters.

What is a satoshi?

The satoshi is currently the smallest unit of the bitcoin currency recorded on the block chain. It is a one hundred millionth of a single bitcoin (0.00000001 BTC). More details here.

Important tips regarding Bitcoin

- **SAVE YOUR ELECTRUM SEED**. Write it down on a sheet of paper, in a text file and/or remember it. Just make sure that you still have access to it if you loose your Tails USB stick. Then you will always be able to recover all your bitcoins.
- Do I have to do something in order to receive bitcoins? No, you just need to send the bitcoins to one of the addresses under the "Addresses" tab. It is not necessary to fill out the form under the "Receive" tab.
- Use a new Bitcoin address for **every** transaction. You have many different ones to choose from under the "Addresses" tab and you should use them because it does not cost anything to use or create new addresses. It further strengthens your OpSec, so do not use one Bitcoin address twice.
- Make sure you have enough to order and pay for shipping. A little extra left over is ok.

How to buy bitcoins

There are two ways you can obtain Bitcoin. You can mine it, however this requires investment in the appropriate hardware, so most people who use the DNM will purchase their Bitcoin one way or another.

Fortunately there are many different ways how to buy Bitcoin. Some are can be easier and more convenient and some can take a bit longer but do not require you to reveal your identity. Since you are going to buy some not-so-legal items with them it is desirable to not have your identity linked to the bitcoin you bought in the first place, so you do not have to go through the hassle of attempting to obfuscate it later on.

The following are descriptions of several ways to buy bitcoins. The general rule is to **not** visit these websites with the TorBrowser or a proxy that is not in your country. The reason behind that is that you do not want to raise suspicion because buying bitcoins is *not* illegal so why would a user need to log in using the Tor browser? However you can use the WiFi of a cafe (or another network that is not tied to your identity) or a VPN (choose a server that is in your country) to log into these websites. That way you do not raise suspicion but still are anonymous, as long your purchase methods do not reveal your identity to the website.
It is your choice to pick what path you want to go in order to obtain bitcoins. If you are just a personal buyer, it will be still fine if you use a non-anonymous method, like a bank wire transfer, *as long as* you follow the instructions in the Sending bitcoins chapter too.

Can I use fake names/email addresses/. . .?

Sometimes you have to give a real name or other identifying data to create an account on the bitcoin exchange. While buying BTC is not illegal, you do not want to make it too easy for law enforcement in case they investigate you. So the general rule of thumb is to use fake/throwaway data *as long as* you do not break the law with that.

For example it is better to create a new email address than using your existing one to create an account on the exchange. But do not, for example, buy a fake ID to avoid showing your real ID. Keep in mind to not use obvious fake data, i.e. avoid using names like "John Smith."

Methods - How & Where to Buy Bitcoins

LocalBitcoins (LBC)

LocalBitcoins.com is one of the most popular methods of buying bitcoins. On this site, you will find lots of sellers and the price per bitcoin they offer. You can get some great deals on bitcoins, but make sure you check the rate before you buy, do not get ripped off!. It is best to choose sellers that already have some positive feedback to reduce the risk of you getting scammed.

There are many methods which you can use to buy bitcoins: the easy and fast ones (e.g. wire transfer) are pretty common and the rates are lower. However that often comes with the disadvantage of losing your anonymity. Other methods, that are a bit more time consuming and slower (e.g. meeting face to face with a seller), can be more anonymous though.

You normally get your bitcoins within a short space of time. You can then move your bitcoins from your LBC wallet to any wallet of your choice. More on that in the following chapters.

Three of the most often used and more anonymous payment methods are:

- In person - you meet with the seller in a public place, you hand them cash and they send you the bitcoins. Make sure you read this post before doing a cash trade. The main thing is to select a seller that has a good history. Message them any questions you have and they will be helpful so you know what to expect. They'll bring a phone or laptop with them and will send the coins on the spot. Once they are sent it's impossible to cancel the transaction. You can also check the transaction on the blockchain using your phone/laptop. You can also use escrow.
- Bank deposit - open a trade, and the seller gives you their bank and account info. You deposit cash into their bank account, upload a picture of the deposit slip, and they send you bitcoins. Some banks will require ID from you to make the cash deposit into any bank account.
- Cash in the Mail - you send cash to the seller through the mail, and they send you bitcoins.

Paxful

Paxful.com is a P2P trading platform similar to LocalBitcoins where sellers and buyers exchange directly and Paxful provides escrow. It is possible to buy coins without

providing ID verification, though the rates are usually higher. Here is some more information on Paxful such as ID requirements from /r/DarkNetMarkets users.

BitQuick.co

BitQuick.co is a US-based hybrid P2P exchange where BitQuick provides escrow service between you and the trader, or you can buy directly from BitQuick. BitQuick will sell you bitcoins (up to $400 without ID verification), or you can trade with one of the independent sellers who sells bitcoins on their platform by cash deposit at banks and credit unions, MoneyGram payment, or Western Union transfer. It is like LBC and Paxful but with fewer payment options.

Bisq

Bisq, available from Bisq.network (formerly BitSquare.io) is an open-source desktop application that allows you to buy and sell bitcoins in exchange for national currencies, or alternative cryptocurrencies and supports cash transactions. Quoted from their website:
Unlike traditional online exchanges, Bisq is designed to be:

- Instantly accessible – no need for registration or approval from a central authority.
- Decentralized – there is no single point of failure. The system is peer-to-peer and trading can not be stopped or censored.
- Safe – Bitsquare never holds your funds. Decentralized arbitration system and security deposits protect traders.
- Private – no one except trading partners exchange personally identifying data. All personal data is stored locally.
- Secure – end-to-end encrypted communication routed over Tor.
- Open – every aspect of the project is transparent. The code is open source.
- Easy – we take usability seriously.

Mycelium Marketplace

Mycelium Marketplace (previously called "Mycelium Local Trader") is the P2P bitcoin trading marketplace within the popular Mycelium Bitcoin Wallet available on **Android devices**. There is a Mycelium Wallet for iPhones, but the Mycelium Market portion of the app is not allowed by Apple. In the app, go to **Buy / Sell Bitcoin** and then

hit **Mycelium Marketplace**, and you will see any local bitcoin traders for a specified area who posted an ad on Mycelium Market and their feedback on previous trades. Trades are handled through the app, but you meet the trader in person at a public place to make the transaction - usually settled in cash, very similar to a LocalBitcoins in-person trade. Mycelium's headquarters are in the EU, but the app is used worldwide.

LibertyX

LibertyX.com operates the largest cash-to-bitcoin onramp network in the US. It allows you to purchase bitcoin in-person up to $1,000 per day at over 13,000 local stores with only a phone number for SMS verification. For more information, please visit their website, LibertyX.com.

Bitcoin ATMs

There are also Bitcoin ATMs in some places which can be a very easy and reliable way to get bitcoins. Simply search for "Bitcoin ATM map" or "Bitcoin ATMs near <your location>" to see if there are some in your area. If that is the case you should also check out what limits there are, what kind of identifications it requires for certain amounts, what the exchange rates are and if there are cameras. Sometimes you have to visit the ATM to get this information. Here is a short list of resources, for your convenience:

- https://www.coindesk.com/bitcoin-atm-map/
- https://CoinATMradar.com
- https://BitcoinATMmap.com
- https://CoinMap.org

More ways

- https://en.bitcoin.it/wiki/Buying_bitcoins

Tumbling

Foreword

Bitcoin tumbling is a highly debated topic and many people have different opinions on different aspects of tumbling. For example what tumbling method is the best, if and when tumbling is necessary, . . . This chapter sticks to neutral viewpoints based on facts and common sense. It avoids taking part in opinionated discussions about tumbling.

Please also keep in mind that some tumblers are **illegal** itself because they are obviously heavily involved in money laundering and operate without any licenses. So, depending on the tumbler, it may be even illegal to use it. Why do people still use tumblers if they break the law by doing it although they want to specifically hide the fact that they break the law? They usually either do not know that the tumbling which they do is illegal or they would rather get convicted of "using a tumbler" instead of buying the illegal goods they bought.

The charges would be like helping a criminal enterprise (by paying the tumbling fee to the tumbler operators) or money laundering. But keep in mind that this does not apply to every tumbler and law enforcement would still have to prove that you used a tumbler which they would only be able to do if they somehow know that bitcoin addresses of that tumbler (e.g. by arresting the operators and analyzing the data they seized).

Furthermore you are not the only one using the tumbler. There are many more criminals with higher profiles that use it too. Therefore the tumbler also becomes a worthwhile target for law enforcement. You may be affected too if the tumbler for example gives you the "hot" bitcoins of a criminal that is already heavily under investigation.

What is tumbling?

If you do not know what tumbling is, please take 4 minutes to read the Wikipedia article about it. It is necessary to understand the following parts.

Please keep in mind that there is not just one method to tumble bitcoins. You can for example use centralized services which you use through a website interface or even tools that you have to install on your computer. Also tumbling is not 100% effective or

secure and it can **not** guarantee that you are immune to any sort of blockchain analysis. That means adversaries may still be able to follow your money flow despite using a tumbler.

(When) Do I have to tumble?

That is by far the most debated question around tumbling. the general consensus is that you do not need to hide the origin of your bitcoins (which tumbling aims to do), if you identity is not linked to them. That means if you for example bought them in cash in an in-person deal, you identity is usually not tied to them (assuming that you did not show your ID or similar things). If you would have bought them using your bank account, your identity would be tied to the bitcoins you bought since there is a record of you buying them with your name on it.

But just because you do not need to tumble when you identity is not linked to the bitcoins, it does **not** means you can send them straight to an illegal online drug market. You **have** to go the path that is described in the Sending bitcoins chapter. Otherwise you are vulnerable to getting your bitcoin exchange account getting closed or even getting prosecuted.
Note: you do not necessarily have to go through every station of the described path if you bought them anonymously, **but** make sure that there is at least one wallet between your exchange and the DNM. That means a path like Bitcoin exchange -> Electrum on Tails -> DNM would still be okay, **if** your identity is not tied to the bitcoins. It is obviously better if you exactly follow the path from the Sending bitcoins chapter but you can take a shortcut without compromising your OpSec much here if you think it is worth it.

Regardless of how you bought your bitcoins: be smart and do not send them directly to a DNM.

So what about the cases when my identity is tied to the bitcoins? Do I need to tumble then?

The answer is: it depends. If you are a normal buyer, i.e. do not buy several pounds a month, then you still do not have to worry about adversaries looking at the blockchain and analyzing that data to catch you. It is simply not in your threat model. However what you should worry about, is how to send the bitcoins to the DNM. It is obviously still not okay to send them directly to a DNM, so it is **crucial** that you follow go the path that is described in the Sending bitcoins chapter.

Since your are buying illegal goods with the bitcoins you bought, the last thing you want is anybody knowing about your purchases. You can prevent that and get plausible deniability (so you can claim that you never bought drugs with the bitcoins you bought), by simply following the Sending bitcoins chapter.

If you still want to tumble for additional peace of mind feel free to do so, but keep in mind that the tumbling itself can be illegal as explained above in teh foreword.

But what if you are a rather big buyer? Then it may be worth tumbling your bitcoins as you deal with larger quantities of illegal goods and you want to make sure that there are absolutely no holes in your OpSec through which law enforcement could fuck you. To learn how to tumble and what you need to watch out for, read the following paragraphs.

How do I tumble?

When you decide to tumble go this path: **Bitcoin exchange -> normal wallet (e.g. Electrum on windows) -> Tumbler -> Electrum on Tails -> DNM**. That way you do not directly send the bitcoins you bought to a tumbler, which could get you into difficulties as explained in the foreword.
Important: if you use a centralized tumbler, visit the tumbler site on tails, store any information it gives you (e.g. some tumbling services give you a PGP signed message with details for your tumbling process) and write down the Bitcoin address where you have to send the bitcoins to. Then boot your normal OS and send the bitcoins to that address (since you have the bitcoins that you want to tumble in your normal wallet (e.g. Electrum on windows)).
If the tumbler offers a random time delay and/or multiple output transactions, **use them**. It is additional, free OpSec strengthening and only costs you a bit of time. If you do not choose these options it might be trivial to spot your cleaned bitcoins. For example if you send 1 btc to a tumbler, all an adversary has to do is to monitor the Bitcoin transactions over the next few minutes and look out for a transaction that is as big as 1 btc minus the tumbler fee. Now he found the bitcoins you think are "clean". So be smart and use a random time delay and multiple output transactions whenever offered.

What services are there?

The most widely used kind of tumblers are the centralized ones that are operated by anonymous third parties which you have to trust that they clean your bitcoins. You can

find them on the superlist. Make sure to not use links from random other sources, like websites that you found through googling "tumbler onion addresses" since they usually spread phishing links. To cross check the links you find on the superlist, follow the instructions here.
The centralized tumblers are widely adopted since they are easy to use and do not require much user action. However there are also other anonymization methods for bitcoin transactions, like CoinJoin for example. However when using implementations of CoinJoin (which itself is not a service that you can readily use but rather a concept of how you can anonymize bitcoin transactions), or similar tumblers make sure you research them beforehand. If for example one project is abandoned and has not received any updates recently, you should stay away from it since you may not get any benefits when using it or you even compromise your OpSec by doing so.

Cross-Cryptocurrency Tumbling

Cross-Cryptocurrency tumbling is a do-it-yourself tumbling method that involves exchanging cryptocurrencies into others to break the link. An example would be: you buy bitcoins and exchange them through shapeshift to another cryptocurrency. Then you could change that back to Bitcoin again (ideally using another exchange). Alternatively, if you exchanged your btc to Monero, you could also make a Bitcoin payment using xmr.to.

There are many ways to switch between several crpytocurrencies and achieve a somewhat tumbling-like process. The goal is to make tracing your money flow harder by using multiple cryptocurrencies.

While this sounds easy and secure, there are some things you need to pay attention to:

- The exchange rates can make it very costly and maybe not worth it.
- The process can take some time and the value of the cryptocurrencies you used probably changes in that period. To your advantage or to your disadvantage.
- Do not just use any cryptocurrency. Some offer significant benefits over others (like more privacy and anonymity) and some can even compromise your OpSec if you use them!

Setting up your wallet

Electrum 2FA

Do not use Electrum wallets with two-factor authentication (2FA). You may think that 2FA for markets is good (which it is) so it must be good for Electrum on Tails too. No. It requires you to bring your smartphone into DNM activities as well as installing google apps on it which is the last thing you want for an anonymous DNM wallet.
Plus your wallet will be secure enough if you keep your seed secure (e.g. written down on a piece of paper in a secret location and stored in a .txt file in your persistence directory, more on that later) and use KeePassX for your wallet password.

Please just create a normal wallet as described in the following steps.

Using Whonix?

If you are using Whonix, you need a couple of minutes to install Eelectrum first. Go to the electrum website and since you set NoScript to disable scripts globally, you should see a page without much content. To fix this, allow scripts temporarily for https://electrum.org by clicking on the NoScript-Symbol and clicking on the entry "Temporarily allow https://electrum.org"..

Now under the headline "Easy Installation", look for the line of the table that begins with "Linux". Copy the first command under the line "Install dependencies:", open the Konsole (using the shortcut on your desktop) and paste the command (right click -> paste) and press ENTER. It will ask you for your password, enter it and press ENTER again. Then some lines will appear in the Konsole window. After the bottom line of the Konsole begins with "user@host:~$" again, copy the second command under "Install Electrum:" and execute that too.

When the second command is also finished you can close the Konsole window and press the Home-button at the bottom left of your task bar. Enter "electrum" into the search field, right click on the appearing entry and select "Add to Desktop". Then go to your Desktop and start Electrum using the new shortcut.

Then you will get an install wizard that will ask you how you want to connect to a server. Select "Auto-Connect" and click next. In the next step you can rename your

wallet. It is recommended to just use the default name "default_wallet". After you clicked next, follow the steps under setting up Electrum.

Setting up Electrum

Fortunately Tails already comes with a wallet installed. So everything you have to do is to set it up. To do this click on "Applications" on the top task bar and select the category "Internet". Then click on the "Electrum Bitcoin Wallet" entry in the list on the right.

If you get the warning that "Persistence is disabled for Electrum" you either need to set it up first so you do not lose your bitcoins.

It should now start an installation wizard, in the following the questions it should ask you and what answers you will have to pick:

What kind of wallet do you want to create? Choose "Standard Wallet"
Do you want to create a new seed, or restore a wallet using an existing seed? Choose "Create a new seed"
You now get that new seed. As long as you remember that seed, you can **always** recover your bitcoins (even if you lose your password or your USB stick with Tails gets lost). So make damn sure that you either remember it or write it down somewhere where nobody else can find it.
Confirm Seed Now type in the seed you have remembered or written down.
Choose a password to encrypt your wallet keys Do **not** skip this step. Instead choose a strong password using KeePassX. In case you loose it, you can always restore your wallet with the seed and set a new password.

Almost done!

Now you just have to make a few change in the settings. Go to "Tools" -> "Preferences" and check the checkbox for "Use dynamic fees" and the one for "Enable Replace-By-Fee". Then switch to the "Transactions" tab in the new window and check the option "Use multiple change addresses". Then switch to the "Appearance" tab and switch the "Base unit" to BTC and change the "Online Block Explorer" to blockchainbdgpzk.onion.

After that you should also change the value of "Zeros after decimal point" to something like 5. Now close the dialog by clicking on "Close".

Last but not least, press CTRL + A so you get the "Addresses" tab displayed which shows all your Bitcoin addresses belonging to your wallet.

Do the same steps for your normal wallet (e.g. Electrum on windows, details here) too, but skip changing the "Online Block Explorer" value.
You also do **not** need to set up the normal electrum wallet to connect over the Tor network because it's goal is not to hide the identity of the owner, unlike the electrum wallet on Tails. So everybody can know that you withdrew the bitcoins from an exchange to your personal electrum wallet (the normal one) but then you send them to the anonymous one (electrum on Tails), as described in the next chapter.

Congratulations, you now have set up your Electrum wallet on Tails!

Important note

Electrum has a list of several servers which it will ask in order to get the balance of the addresses that belong to your wallet. Law enforcement could easily set up such a server to collect information about when what IP address asks for the balance of what Bitcoin addresses. So Electrum is **not** anonymous.

However if you use Electrum on Tails, law enforcement only knows which addresses belong to that wallet (because the IP address of a Tor exit node suddenly request the balance of for example 20 specific addresses) but not the true IP address of the owner because Tails routes it's entire internet traffic through the Tor network.

Because of this issue it is **very** important that you exactly follow the steps in the sending bitcoins chapter.

Electrum questions?

Check their FAQ, their documentation and google your question. If that does not help, you can post your question on /r/darknetmarketsnoobs

Electrum not starting any more?

First make sure you still have your seed for that wallet and can access it even if your Tails USB stick would break completely.

Then right click on desktop, open terminal, and type in

```
electrum
```

and press ENTER. See if it loads. If it does not do the following steps:

Make sure that "Bitcoin client" is checked in the list of data that will be preserved between reboots (go Applications -> System Tools -> Configure persistent volume to see the list).

One user also reported that doing a few reboots and in the end leaving it alone made the electrum window pop up eventually.

Several users also reported that the following helped: go Applications -> System Tools -> Configure persistent volume and uncheck the Electrum option. Then reboot and check the option again. To finish it, reboot again and test if electrum opens.

Reboot Tails and try deleting the "electrum" folder in the directory */live/persistence/TailsData_unlocked/* because it could be that the Electrum files are corrupted. Then restart Tails and see if you can open Electrum again, if yes you will have to restore your old wallet from your seed.

If that does not work go into your /home/amnesia/ directory and press CTRL + h. then rename the folder .electrum to .electrum.bak. After that restart and see if you can start Electum now.

Sending bitcoins

This chapter deals with sending your bitcoins from the source you got them (e.g. a Bitcoin exchange) to the final destination (a DNM). Unfortunately it is not as easy as sending them straight to your market deposit address because exchanges have banned and flagged accounts in the past that did that.

The path

Note: as described earlier, if you use Electrum an attacker can see what addresses belong to what wallet and which IP address regularly checks the balance of these addresses.
In general the path you should send your bitcoins is: **Bitcoin exchange -> normal wallet (e.g. Electrum on windows) -> Electrum on Tails -> DNM**.
Note: That normal wallet and the Electrum wallet on Tails have to be different wallets. So you have to do the setup process described previously twice: once for your normal wallet and once for your Electrum wallet on Tails.

Bought your BTC completely anonymously?

If you bought your BTC completely anonymously (e.g. on a BTC ATM which has no cameras and requires no phone number), you should go:

Source (e.g. BTC ATM) -> Electrum wallet on Tails -> Market.

Otherwise you would just unnecessarily reveal information with the 'normal wallet' in the default sending BTC path described above. If you want to be extra cautious you can go this path:

Source (e.g. BTC ATM) -> Electrum wallet #1 on Tails -> Electrum wallet #2 on Tails -> Market

---

To set up your normal wallet (in this case Electrum on windows) just go to the Electrum website, download it and follow the instructions in the previous chapter to set up a new wallet.

This process is to add plausible deniability: you can always say that you withdrew the coins from the exchange to your own wallet (the normal wallet). Then you sold them to an "anonymous stranger" (who owns the Electrum wallet on Tails) who then transferred

them to a market. That way you do not incriminate yourself and have some plausible deniability.

If you would go exchange -> Electrum on Tails -> DNM, it would be pretty obvious that you are the one who sent the bitcoins to the DNM (assuming that the DNM deposit address is known), because nobody would give the DNM deposit address to the Bitcoin seller when buying the bitcoins. That means: if you still claim that you sold the bitcoins to someone else after withdrawing them from the exchange to your Electrum wallet on Tails, that new buyer would have given you his DNM deposit address. This is extremely unlikely because you normally do not give out DNM deposit addresses out when buying bitcoins, but rather one that belongs to one of your wallets. Therefore nobody would believe you that you sold the bitcoins to a stranger. So your plausible deniability would be gone.

With the recommended path (marked in bold above) you can believably claim that someone else sent the bitcoins to a DNM and the exchange will most likely not ban your account because you did not sent them directly to a DNM.

Note: some markets have a minimum amount of bitcoins you have to send for a deposit. Make sure you meet that requirement or you could lose your money!

I did not sent my bitcoins that way before, am I fucked?

You will probably be fine, **BUT** make sure you go the path described above in the future for every DNM deposit. You do not have to delete your DNM account or Bitcoin exchange account, but step up your OpSec in the future.

Sending bitcoins with Electrum

The process

To send bitcoins from your Electrum wallet to an address just go to the "Send" tab and enter the destination Bitcoin address in the "Pay to". When sending the bitcoins make sure you use the transaction fee that is dynamically created by Electrum (by default it will get confirmed within 5 blocks). That means just let the slider under the amount field be in the middle. If you are sending the bitcoins from the normal wallet you have to get a receiving address from your Electrum wallet on Tails first. To do that go to the

"Addresses" tab in your Electrum wallet on Tails and write down the value of one of the Bitcoin addresses listed under "Receiving".

Note: you can double click on the space on the right of the address to change the label of that address. It is recommended to label it as "used <current date>" for example, so you know that you already used it and do not use it again.

After that boot your normal OS again and start Electrum again. Then you can go to the "Send" tab again and send the bitcoins to the address of your Electrum wallet on Tails. When you received the bitcoins on Electrum wallet on Tails you can repeat the same send-process but this time send them to the deposit address that your market gave you.

Setting the fee manually

You can also set the fee manually to ensure that your transaction (short: tx) does not take too long to confirm. Using the dynamic fee as described above is usually the best way though. If you do want to set the fee manually though, follow these steps:

1. Go to bitcoinfees.21.co, allow JavaScript for "https://bitcoinfees.21.co" and scroll down to the bottom of the graphs. There you see a sentence like "The fastest and cheapest transaction fee is currently 390 satoshis/byte".
2. Open Electrum and go Tools -> Preferences and uncheck the "Use dynamic fees" option. Then you can set the transaction fee per kilobyte (kb) in BTC/kB. If it shows mBTC/kB, switch to the "Appearance" tab and select "BTC" as the base unit from the dropdown menu.
3. Now change the value of the transaction fee per kb like this: If the recommended fee from the website is 390 satoshis/byte, set the fee to 0.0039 BTC/kB. That means, append three zeros to the satoshis/byte value as well as a point after the zero on the far left. If the website would have recommended 280 satoshis/byte instead, you should set the fee to 0.0028 BTC/kB instead in Electrum.
4. Done! Now click on the close button.

Transactions not getting confirmed

Transactions not getting confirmed

Bitcoin transactions become "confirmed" when miners accept to write them in the Bitcoin blockchain. In general, the speed of confirmation depends on the fee you attach to your transaction; miners prioritize transaction that pay the highest fees.

Another reason could be that the Bitcoin network is overloaded at the moment. Sometimes a lot of unconfirmed transaction rack up (tens of thousands) which you can spot here (onion link). these have to get processed, which will take a while. However for now you have to be patient and wait. It can take several hours or sometimes over a day for a transaction to get confirmed. Making posts about it on /r/DarknetMarketsNoobs is **not** confirming your transaction faster.

In the meantime you can check if the destination address of the transaction is correct, because if not you can wait forever for the coins to arrive.

Make sure that you use the transaction fee that is dynamically created by Electrum next time (by default it will get confirmed within 5 blocks). That means just let the slider under the amount field be in the middle in the "Send" tab.

There are however two ways which can speed up your transaction:

- Increase the transaction fee in Electrum. This is only possible for "replaceable" transactions. To create this type of transaction, you must have enabled "Replace by Fee" in your preferences, before sending the transaction. If it takes too long till this transaction gets confirmed you can right click on the transaction and then upgrade the fee to make it get confirmed faster (only works if you did not spend the full amount of bitcoins in your wallet).
- If you sent the bitcoins to an address you do not control (e.g. a market), the best you can do is try the ViaBTC Transaction Accelerator. It may or may not work.
- Create a "child pays for parent" transaction, with a generous fee. A CPFP is a new transaction, that compensates for the small fee of the parent transaction. It can be done by the recipient of the funds, or by the sender, if the transaction has a change output. Here is a step-by-step guide, however it is not that easy so you might just wait till your transaction gets confirmed eventually.

Can I cancel a transaction I made?

No, you will have to wait till it get confirmed eventually or rejected by the Bitcoin network.

Will I lose my bitcoins?

No, you will just have to wait some time till it gets confirmed or rejected.

PGP

General information

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

To get a general understanding of it's design please take a few minutes to read this.

When you create a PGP key, it gives you two unique keys. A public key, and a private key. You are to **not**, at any times, or for any reason, give anyone your private key. That is for your eyes only. Your public key, however, is able to be given out so others can encrypt messages with your public key, send them to you, and then only **YOU**can decrypt them with your private key.

This works exactly opposite when buying from vendors. You use their public key to encrypt all your shipping information, etc, then you send the encrypted message. Only the vendor is able to see it as only they possess the private key to decrypt, and read, your message.

Note: if you want to make sure that you can properly encrypt and decrypt messages with PGP please go to /r/GPGpractice

Sent a message without PGP?

Did you sent a message which contained sensitive data (e.g. your address) without encrypting it with PGP by yourself?

Then it is best to delete your market account and start a new one. And no, this is **not** overkill. When the Silk Road servers were seized, a lot of messages were not PGP encrypted and contained addresses in plaintext. In the following years the FBI gave those data to other law enforcement agencies around the world and they busted buyers that sent their addresses unencrypted. So if you would continue to order with that account, the evidence against you would just stack up even more.
Please make the cut now and create a new market account with which you will always PGP encrypt your address by yourself.

Do I need to encrypt all messages?

You only need to encrypt messages containing sensitive information such as packaging details (which should only ever be discussed between a vendor and a buyer) or addresses. Saying "Thanks!" doesn't need encryption.

Can I decrypt a PGP message I sent?

No, only the user whose public key you used to encrypt the message can decrypt it. However if you select the public keys of the users you want to send the message to **and** your own public key, then you will be able to decrypt the encrypted message (as long as your PGP key is not expired). You will learn later how to do that.

What is the difference between PGP and GPG?

It is explained here.

Creating a PGP key pair

Tails

Click on the clipboard icon on task bar at the top of your screen and select the option "Manage Keys". On the new window that appeared, click on "File" at the top and select the "New..." option. Then a list of items shows up that you can create, choose "PGP Key" and click "Continue".

Then you can enter your "Full Name". Obviously do not use your real one because everybody that has you public key later can see that name. It is best to choose the same username that you already have on a market because it will make it easier for your vendor.

The name has to be at least 5 characters long, if your name is shorter just add the market that you are using at the end of it or "DNM" for example.

After that you can enter your email address. It is not necessary and if you do not have one you can leave it blank. However if you want to create one please take a look at the Email chapter of the DNM bible. If you already have one that you want to enter in that field, please make sure that it fulfills the requirements mentioned in the Email chapter.

If one of the points is not fulfilled, please create a new one by following the steps in the email section or do not enter an email address for the PGP key creation.

Now click on "Advanced key options" and set the "Key strength (bits)" to 4096 and the "Expiration Date" to one or two years in the future.

Note: After a key pair expired it can not be used to send you encrypted messages any more (i.e. your public key can not be used) and you can not decrypt messages any more (i.e. your private key can not be used). It is a really useful feature that all DNM users should use because once the key expired nobody can read the messages any more, which means there will be no usable evidence against you. It is easy to set (just check the option during the creation of the key) and barely adds any extra work (i.e. creating a new PGP key once every year is not much work compared to the enormous OpSec boost you get).
However it is still *technically* possible to use your private key even after it expired, although not all tools let you do that. So in order to get that OpSec boost, you need to

delete your old, expired PGP key after you created your new one and updated your DNM account settings with the new key.
Confirm the data by clicking on "Create". You now get asked to set a password which is, in combination with your private key, necessary to decrypt messages that were encrypted with your public key. Please choose a strong password by using KeePassX.

After you clicked on "OK" you will have to wait a bit (usually not longer than a few minutes) and you will see your key in the list of GnuPG keys (click on "GnuPG keys" on the left sidebar).

Congratulations, you now created your own PGP key pair!

One last thing: if you want to copy your public key, just select your key in the "GnuPG keys" list and press CTRL + C. Now you have your public key copied and can paste it anywhere.

Your public key should look like this:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFhNDOsBEACzwJJVsMo7sIiLhvCsLx2n+DVHzw1trM/C8Yao8EmWdDYe3ei9
mXRqSudbD6S4KvJfm+ZeOlEQ6gGoG2q3aFYASRgcK7WDhs+jwG42EA+j2oIpU/EO
8EQXTmTn8T+LQT84JZ5KkiZZp2CqLU8RVszfkKEj1oX/sO5watxNQur4fbk9FiCA
1MjHMYir1g==
=TV04
-----END PGP PUBLIC KEY BLOCK-----
```

The gibberish part in the middle will be a bit longer though. The "Version" line may also be different or not exist at all. It is just additional information and not necessary, in fact it only gives away information about the software that you are using, so feel free to remove that line before entering your public key in the DNM account settings.

Whonix

Do all of the following steps on the Whonix Workstation. Open KGpg by double clicking on the shortcut on the Desktop. On the top bar go Keys -> Generate Key Pair.

Then you can enter your Name. Obviously do not use your real one because everybody that has you public key later can see that name. It is best to choose the same

username that you already have on a market because it will make it easier for your vendor.

The name has to be at least 5 characters long, if your name is shorter just add the market that you are using at the end of it or "DNM" for example.

After that you can enter your email address. It is not necessary and if you do not have one you can leave it blank. However if you want to create one please take a look at the Email chapter of the DNM bible. If you already have one that you want to enter in that field, please make sure that it fulfills the requirements mentioned in the Email chapter.

If one of the points is not fulfilled, please create a new one by following the steps in the email section or do not enter an email address for the PGP key creation.

Leave the Comment field empty. Set the key size to 4096 (bit) and the Expiration to one or two years in the future.

Note: After a key pair expired it can not be used to send you encrypted messages any more (i.e. your public key can not be used) and you can not decrypt messages any more (i.e. your private key can not be used). It is a really useful feature that all DNM users should use because once the key expired nobody can read the messages any more, which means there will be no usable evidence against you. It is easy to set (just check the option during the creation of the key) and barely adds any extra work (i.e. creating a new PGP key once every year is not much work compared to the enormous OpSec boost you get).
However it is still *technically* possible to use your private key even after it expired, although not all tools let you do that. So in order to get that OpSec boost, you need to delete your old, expired PGP key after you created your new one and updated your DNM account settings with the new key.
You now get asked to set a password which is, in combination with your private key, necessary to decrypt messages that were encrypted with your public key. Use KeePassX to generate and store a strong password.

After you clicked on "OK" you will have to wait a short time (usually not longer than a minute) and you will get a window that says that your new key pair was created. Check the box to the left of "Save as" in the box titled "Revocation Certificate" and click on OK to close the window.

Congratulations, you now created your own PGP key pair!

One last thing: if you want to copy your public key, just right click on your key in the "Key Management" window 8the one you see after opening KGpg through the shortcut from the Desktop), select "Export Public Key" and check the options "Clipboard" and "Clean Key" on the newly appeared window. Now you have your public key copied and can paste it anywhere, like in your market profile which you should definitely do.

Your public key should look like this:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFhNDOsBEACzwJJVsMo7sIiLhvCsLx2n+DVHzw1trM/C8Yao8EmWdDYe3ei9
mXRqSudbD6S4KvJfm+ZeOlEQ6gGoG2q3aFYASRgcK7WDhs+jwG42EA+j2oIpU/EO
8EQXTmTn8T+LQT84JZ5KkiZZp2CqLU8RVszfkKEj1oX/sO5watxNQur4fbk9FiCA
1MjHMYir1g==
=TV04
-----END PGP PUBLIC KEY BLOCK-----
```

The gibberish part in the middle will be a bit longer though.

Importing a public key

Tails

To be able to send someone an encrypted message (e.g. your address to a vendor), you need their public key. In order to get a vendor's public key you have to visit his profile and look out for a link that is named like "PGP key" or "Vendor public key". Sometimes it is also featured directly on the vendor's profile page.

When you found it, it should look like this:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFhNDOsBEACzwJJVsMo7sIiLhvCsLx2n+DVHzw1trM/C8Yao8EmWdDYe3ei9
mXRqSudbD6S4KvJfm+ZeOlEQ6gGoG2q3aFYASRgcK7WDhs+jwG42EA+j2oIpU/EO
8EQXTmTn8T+LQT84JZ5KkiZZp2CqLU8RVszfkKEj1oX/sO5watxNQur4fbk9FiCA
1MjHMYir1g==
=TV04
-----END PGP PUBLIC KEY BLOCK-----
```

The gibberish part in the middle will be a bit longer though. The "Version" line may also be different or not exist at all. It is just additional information and not necessary, in fact it only gives away information about the software that you are using, so feel free to remove that line.

Now copy that public key and go to your "GnuPG keys" list. Then press CTRL + V and you should see your vendor's public key in that list.

If you get a pop up with the following error:

```
Could not display 'Clipboard text'
Reason: Unrecognized or unsupported data.
```

there was a formatting problem with the key you copied into the clipboard. Make sure that you are copying all of the key including the five dashes at the beginning and end of the key and the BEGIN and END statements. PGP is very picky about formatting errors.

Whonix

To be able to send someone an encrypted message (e.g. your address to a vendor), you need their public key. In order to get a vendor's public key you have to visit his profile and look out for a link that is named like "PGP key" or "Vendor public key".

When you found it, it should look like this:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFhNDOsBEACzwJJVsMo7sIiLhvCsLx2n+DVHzw1trM/C8Yao8EmWdDYe3ei9
mXRqSudbD6S4KvJfm+ZeOlEQ6gGoG2q3aFYASRgcK7WDhs+jwG42EA+j2oIpU/EO
8EQXTmTn8T+LQT84JZ5KkiZZp2CqLU8RVszfkKEj1oX/sO5watxNQur4fbk9FiCA
1MjHMYir1g==
=TV04
-----END PGP PUBLIC KEY BLOCK-----
```

The gibberish part in the middle will be a bit longer though. The "Version" line may also be different or not exist at all. It is just additional information and not necessary, in fact it only gives away information about the software that you are using, so feel free to remove that line.

Now copy that public key and open the KGpg window. At the top you see a few buttons, one of which is named "Import Key". Click it and select "Clipboard" on the window that appeared. Confirm by clicking "OK".

If all went well, you should get a message like "1 key processed. One key imported: One RSA key imported.". Close the window by clicking on "OK" and check the list of PGP keys to see if it contains the PGP key you just imported. When you find it, right-click on it and select "Key Properties". Then select "Ultimately" from the drop-down menu for the field "Owner trust" and confirm by clicking "OK". This will make it easier for you to quickly encrypt messages with that PGP key (i.e. send encrypted messages to that vendor).

If you get an error like "Key importing failed. Please see the detailed log for more information.", there was probably a formatting problem with the key you copied into the clipboard. Make sure that you are copying all of the key including the five dashes at the beginning and end of the key and the BEGIN and END statements. PGP is very picky about formatting errors

Encrypt a message with PGP

Tails

Note: you first need to import the public key of the user (e.g. a vendor) that you want to message, so you can encrypt messages that you want to send to him.

To encrypt messages with PGP you first have to type that message in a text editor (e.g. gedit). Then press CTRL + A and CTRL + C to copy it. After that click on the clipboard icon and select "Sign/Encrypt Clipboard with Public Keys".

On the new window select the public key of the user you want to encrypt the message for (e.g. your vendor) by checking the checkbox in front of the list entry. Then select your key on the drop down list on the right of "Sign message as:" and make sure that the "Hide recipients" option is unchecked.

When that is done, click on "OK" and you should get asked if you trust these keys. Click on "Yes" and enter your password for your private key. To confirm that it encrypted your message properly go back to your text editor and press CTRL + V. If you see something that looks like this

```
-----BEGIN PGP MESSAGE-----

hQIMA8Pzj/CHV15DAQ/+JOWXCC6vDIxNge3xRqHsKCSEToFkx02qXd9PwWRFESgc
QZGwh6yz0DVlB7yKJZvzRK1O0tS2wLpKKMBNv8dPv/u6B609yXzP6ns3066C7ymO
PAFA1MgvKvu7mUg5wxFRPKgFfYxBNbCleS5MzPp8bPJq6xQaVeOOogPtFWerN/vM
iIcCod+JyWoBgy3iBw==
=alkJ
-----END PGP MESSAGE-----
```

it is encrypted properly. The gibberish in the middle (the actual encrypted message) will be a little bit longer for you.

Note: after you encrypted your message you will **not** be able to decrypt it any more. Only the person with the corresponding private key and the password will be able to do it (in this case the vendor). If you need to backup the message content, store the plaintext of it somewhere in a file before encrypting the message. However as long as you still have your own private key and remember your password you set for it, you

can always decrypt the messages that you got in the past (i.e. that were encrypted with your public key). This is assuming that your key has also not expired yet.
Note: there should also be a line that starts with "Version:" between the "-----BEGIN PGP MESSAGE-----" and the beginning of the gibberish part. Please remove it, so the encrypted message looks like above since the version line only gives unnecessary information to an attacker.

Now all you have to do is going to the market or email website, paste the clipboard content into the relevant text field and send the message or email.

After you did this please close the text editor and if it asks you if the changes should be saved, select "Close without saving".

Whonix

Note: you first need to import the public key of the user (e.g. a vendor) that you want to message, so you can encrypt messages that you want to send to him.

Open the KGpg window and select File -> Open Editor. Then type in the message that you want to encrypt in the new editor window. To encrypt it, click on the "Encrypt" button at the bottom and then select the according PGP key from the list that appeared in the new window (i.e. the PGP key of the vendor that you want to send the encrypted message to).

Then the text in the editor will change to something like this:

```
-----BEGIN PGP MESSAGE-----

hQIMA8Pzj/CHV15DAQ/+JOWXCC6vDIxNge3xRqHsKCSEToFkx02qXd9PwWRFESgc
QZGwh6yz0DVlB7yKJZvzRK1O0tS2wLpKKMBNv8dPv/u6B609yXzP6ns3066C7ymO
PAFA1MgvKvu7mUg5wxFRPKgFfYxBNbCleS5MzPp8bPJq6xQaVeOOogPtFWerN/vM
iIcCod+JyWoBgy3iBw==
=alkJ
-----END PGP MESSAGE-----
```

if it is encrypted properly. The gibberish in the middle (the actual encrypted message) will be a little bit longer for you.

Note: after you encrypted your message you will **not** be able to decrypt it any more. Only the person with the corresponding private key and the password will be able to do

it (in this case the vendor). If you need to backup the message content, store the plaintext of it somewhere in a file before pressing the Encrypt-button.

Now all you have to do is going to the market or email website, paste the clipboard content into the relevant text field and send the message or email.

After you did this please close the editor window and click the "Discard" button when it asks you if you want to save the document.

Signing and verifying a message with PGP

Tails

Signing

If you just want to sign a message, everybody will see that content of it and if they have your public key they also know that you signed it. It is usually not necessary to sign messages as a normal DNM buyer but if you need to do it, here is how.

This is not for encrypting your address or other private messages. Everybody can read a signed message (that's not encrypted).

Type that message in a text editor (e.g. gedit). Then press CTRL + A and CTRL + C to copy it. After that click on the clipboard icon and select "Sign/Encrypt Clipboard with Public Keys". On the new window do not check any keys in the recipient list but select your key on the drop down list on the right of "Sign message as:". Also make sure that the "Hide recipients" option is unchecked.

When that is done, click on "OK" and enter your password for your private key. To confirm that it signed your message properly go back to your text editor and press CTRL + V. If you see something that looks like this

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

signed message text
-----BEGIN PGP SIGNATURE-----

iQIcBAEBAgAGBQJYg5AQAAoJEMPzj/CHV15DTbkP/iweuHOlCH9fxa2CqBoxUn2D
BZiW94/PMitNAG1hP/Nucc+rAbRgvmtrQ/GfPkcgtUmsLJy0+duMk7PBg1Q3imkz
icqHhI6eN7F4aHSlM1kVKIXhNSwE0AVaf5n45Yrqtkt+O3BQ7aH/v5vcFbTTzIcf
XJGfhh/OAig8+w6LQvJL
=QsWE
-----END PGP SIGNATURE-----
```

it is signed properly. The gibberish in the middle will be a little bit longer for you. Now all you have to do is going to the market or email website, paste the clipboard content into the relevant text field and send the message or email.

After you did this please close the text editor and if it asks you if the changes should be saved, select "Close without saving".

Verifying

Before you can verify the PGP signed message, you need to import the public key of the user that signed the message. So see where it is listed (e.g. on the vendor's profile on the market) and then import it

After that you can copy the PGP signed message which should look something like this:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Text of the PGP signed message.
-----BEGIN PGP SIGNATURE-----

iQIcBAEBAgAGBQJYsU1SAAoJEMPzj/CHV15DkfgP/RcJw9EtFiv/+4LIV5rrgqcF
+FHEZiYb5jQhsqHrR7jS69rAwxzMD/rttQxMMw4cXBDh/dQaelwOVWbcy4DUwHaj
c3gFOzt/42VK40LcQlEs
=ON6z
-----END PGP SIGNATURE-----
```

After you have copied it, click on the clipboard icon at the top taskbar and select "Decrypt/Verify Clipboard". The a new window should pop up which contains "Good signature from <name of the key pair that signed the text>" at the bottom, if the signature was correct.

Whonix

Signing

Open the KGpg window and select File -> Open Editor. Then type in the message that you want to sign in the new editor window and click on the button "Sign/Verify". Select your PGP key from the newly appeared list and clic on "OK". It will then prompt you for the password of your PGP key, enter it and confirm again by clicking on "OK".

Now the content of the editor should look like this:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

signed message text
-----BEGIN PGP SIGNATURE-----

iQIcBAEBAgAGBQJYg5AQAAoJEMPzj/CHV15DTbkP/iweuHOlCH9fxa2CqBoxUn2D
BZiW94/PMitNAG1hP/Nucc+rAbRgvmtrQ/GfPkcgtUmsLJy0+duMk7PBg1Q3imkz
icqHhI6eN7F4aHSlM1kVKIXhNSwE0AVaf5n45Yrqtkt+O3BQ7aH/v5vcFbTTzIcf
XJGfhh/OAig8+w6LQvJL
=QsWE
-----END PGP SIGNATURE-----
```

if it is signed properly. The gibberish in the middle will be a little bit longer for you. Now all you have to do is going to the market or email website, paste the copied content of the editor into the relevant text field and send the message or email.

After you did this please close the editor window and click the "Discard" button when it asks you if you want to save the document.

Verifying

Before you can verify the PGP signed message, you need to import the public key of the user that signed the message. So see where it is listed (e.g. on the vendor's profile on the market) and then import it

After that you can copy the PGP signed message which should look something like this:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Text of the PGP signed message.
-----BEGIN PGP SIGNATURE-----

iQIcBAEBAgAGBQJYsU1SAAoJEMPzj/CHV15DkfgP/RcJw9EtFiv/+4LIV5rrgqcF
+FHEZiYb5jQhsqHrR7jS69rAwxzMD/rttQxMMw4cXBDh/dQaelwOVWbcy4DUwHaj
c3gFOzt/42VK40LcQlEs
=ON6z
```

```
-----END PGP SIGNATURE-----
```

After you have copied it, open a new editor window, paste the signed message into it and click on the "Sign/Verify" button. The a new window should pop up which contains "Good signature from <name of the key pair that signed the text>", if the signature was correct.

Decrypting an encrypted message

Tails

To decrypt PGP encrypted messages just follow the guide on the Tails website.

Whonix

Open the KGpg window and select File -> Open Editor. Paste the message that you want to decrypt in the new editor window. To decrypt it, click on the "Decrypt" button at the bottom. It will then prompt you for the password of your PGP key, enter it and confirm again by clicking on "OK".

If all went well, you will see the decrypted message in the editor window. To reply you can open a new editor window and type in the response (and check the first editor window with the decrypted message during that process if you need to re-read parts of the decrypted message again).

To encrypt your reply, follow the steps from the Encrypting a message chapter.

Formatting PGP texts for reddit

Note: when publishing signed messages, you have to press enter after you wrote a handful of words in one line because otherwise the users will have to scroll sideways and it will look like this:

```
This is a very long sentence which will be included in a PGP signed message and if you do not press ENTER once in a while the user will have to scroll sideways.
```

instead of this (which is much easier to read):

```
This is a very long sentence which will be included in a PGP signed message but
since you pressed pressed ENTER once in a while it is much easier to read because
the users do not have to scroll sideways.
```

To get it right when you have to press enter, just try to make your lines as long as in the example above and then post it on reddit. If the lines are still a bit too long just re-format the text that you signed (by making the line breaks earlier) and sign that new message again. Then edit your post or comment which includes the old signed message and replace it with the newly signed message (keep in mind you must follow the steps below too).

The line breaking is only necessary when writing the text for signed messages. If you just want to send or post encrypted messages or keys you only have to do the following :

Linux:

1. Open a text editor (gedit if you are on Tails or KWrite if you are on Whonix) and paste your PGP encrypted message, signed message or key into it.
2. Mark the whole text by pressing CTRL + A and press TAB once if you are on Tails or twice if you are on Whonix.
3. Mark the whole text again by pressing CTRL + A and copy it with CTRL + C.
4. Done, you now can paste it into a reddit comment or post.

Windows, OS X, others:

1. Go to the website https://html-online.com/editor/ and tell NoScript to allow scripts from https://html-online.com
2. Scroll down to the second textarea and paste your PGP encrypted message, signed message or key into it.
3. Mark the whole text by pressing CTRL + A and press TAB twice.
4. While the text is still marked, copy it with CTRL + C.
5. Done, you now can paste it into a reddit comment or post. Please close the tab of the html-online.com site now.

Shipping

Postal Systems

Getting a letter or parcel from Point A to Point B is the goal. Nearly every country worldwide has a system to achieve this. Interchanging mail between each countries is called "international" mail. If the mail piece is delivered in the same country it was sent from, it is called "domestic" mail.

Although countries vary in system design, similar things like mail sorting facilities and Customs inspection facilities are found in most. International mail goes through two customs inspection facilities, one from the country of origin, and the other in the country of it's destination. International mail is subject to far more eyes and inspection (including unwarranted opening and x-raying, varying on a country's laws and common practices) than is domestic mail which merely goes through sorting facilities. In the USA, all domestic First-Class mail is protected by law against unwarranted search and seizure.

International mail is also more expensive, and has higher loss rates than domestic mail. Certain countries are known for having particularly strict Customs inspections on incoming mail, including Singapore, Australia, New Zealand, Israel, Norway, Sweden, Finland, and many Middle Eastern and Asian countries. Ordering contraband via international mail to and from these countries is up to the buyer, but generally discouraged because of the elevated risk of detection and arrest.

Accepting packages

This is a very useful resource that you should really read before continuing with the other chapters.

How long do I have to wait between two orders?

It is **strongly** recommended to not order more than one package at a time, and if the package arrived successfully and without trouble you can make your next order. That way in the worst case (your package gets intercepted) law enforcement seizes only *one* package with illegal goods and your address on it. If they discover more than

one package of contraband, it will be harder for you and your lawyer to deny your knowledge about it in court.

Do I need to change my shipping address?

No, if you follow the steps in the DNM Bible and do not order more than one package at a time, you can reuse your address.

My package is damaged.

Sometimes packages get a bit damaged while not being completely opened. Remember that those boxes get thrown around a lot. It is for example possible that it was tossed onto the ground, bent, manhandled by workers or torn by sorting machines.

It is a federal offense to open someone else's mail. Nevertheless if someone could see the illicit content of your mail through the holes you should not order for a while. If the contraband could not be seen, because of a visual barrier and/or a decoy the vendor used, you will most likely be fine even if your mail was delivered damaged.

Can I order to a university or a dorm?

Yes, but make sure you haven't signed away any of your rights to your school giving them permission to search your mail. Remember that your university can search your dorm without your knowledge and without cause.

Can I order to my workplace?

No. Do you want to get fired AND arrested at the same time! Keep all DNM activities separate from your work.

Should I check tracking?

Do not check tracking at all, unless a substantial or abnormal amount of time has passed without delivery. You will only leave traces when doing so but will not make it arrive faster. For more details visit the non arriving packages chapter. If you absolutely have to check it (which should never be the case), do **not** use Tor to do it. It will be a huge red flag and law enforcement already knows about DNM users checking their packages over Tor. Instead use a third party website if possible, so not the one of your mail carrier but a website which checks the tracking for you. Examples

are TrackingEx and PackageMapping. Also do not use your own WiFi for checking the tracking number. Use one that is not tied to your identity (e.g. a cafe) or use a VPN and choose a server that is in the same country as you (to not raise any red flags).

What should I do if I receive a double order, additional items, or something I didn't order at all?

Contact the vendor. If you can reasonably make use of the product, you should offer to pay for it. If you can only really partially use or you will use it but didn't really want it, you might consider paying shipping + 50% of the item's price. If you just don't want it or can't use it at all, please at least let them know. Try to be good to good vendors. There's a better chance they'll be good to you.

How to dispose of the packaging

When you extracted the goods from your package, you will have some left over packaging material. It is best to not throw it in your own trash to not incriminate yourself too much. It is recommended to either burn it or throw it away in a trash can somewhere away from any location associated with you. A very common practice in drug investigations is to collect and look through a suspect's trash for evidence of drug law violations.

Origin Countries

The first rule is: stick to **domestic** whenever possible. Mail that does not cross any country border will get far less checked than all other mail. This reduces the risk of you not getting your package or even getting in legal trouble.

However one disadvantage is that the prices can be a bit higher compared to other listings from vendors that ship not from your country. You have to decide for yourself if you want to take the higher risk and pay a bit less or if you want to play it safe and pay a bit more.

If you buy for the first time or for one of the first times, it is best to stick to domestic even if you have to pay a bit more. Many new users worry too much during their first orders (e.g. get paranoid) or even make mistakes. In order to get yourself some peace of mind you should stick to domestic because it generally means a higher success chance.

"Hot" Origin Countries

If you order international, it is strongly **discouraged** to order from the following "hot countries" because mail coming from these countries will usually get checked extensively.

- The Netherlands (NL) - notorious origin country for all drugs
- Colombia (CO) - notorious cocaine and heroin origin country
- Peru (PE) - notorious cocaine origin country
- Bolivia (BO) - notorious cocaine origin country
- Venezuela (VE) - significant but marginal cocaine origin country with possibly rising market share
- Ecuador (EC) - significant but marginal cocaine origin country
- Canada (CA) is on Israel's drug origin country watch list, and, specifically, XpressPost (express mail) from Canada is often opened by US Customs indiscriminately. Note: Mail that is **not** XpressPost from Canada is usually not cause for extra concern.
- Spain (ES) is on Israel's drug origin country watch list. This affects imports into Israel.
- France (FR) is on Israel's drug origin country watch list. This affects imports into Israel.
  Though their list may differ somewhat from global customs agencies including US Customs, the US State Department gives a decent idea about which countries they consider to be major sources of drugs. In their yearly International Narcotics Control Strategy Report, they give details about the following countries which they consider to

be "Major Illicit Drug Producing, Drug-Transit, Significant Source, Precursor Chemical" countries. As of INCSR 2018 Volume 1, those are:

Major Illicit Drug Producing, Drug-Transit, and Significant Source Countries

Major Illicit Drug Producing and Major Drug-Transit Countries

A major illicit drug producing country is one in which:

A. 1,000 hectares or more of illicit opium poppy is cultivated or harvested during a year; B. 1,000 hectares or more of illicit coca is cultivated or harvested during a year; or C. 5,000 hectares or more of illicit cannabis is cultivated or harvested during a year, unless the President determines that such illicit cannabis production does not significantly affect the United States. [FAA § 481(e)(2)]

A major drug-transit country is one:

A. that is a significant direct source of illicit narcotic or psychotropic drugs or other controlled substances significantly affecting the United States; or B. through which are transported such drugs or substances. [FAA § 481(e)(5)]

The following major illicit drug producing and/or drug-transit countries were identified and notified to Congress by the President on September 13, 2017, consistent with section 706(1) of the Foreign Relations Authorization Act, Fiscal Year 2003 (Public Law 107-228):

Afghanistan, The Bahamas, Belize, Bolivia, Burma, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, India, Jamaica, Laos, Mexico, Nicaragua, Pakistan, Panama, Peru, and Venezuela.

Major Precursor Chemical Source Countries

The following countries and jurisdictions have been identified to be major sources of precursor or essential chemicals used in the production of illicit narcotics:

Afghanistan, Argentina, Bangladesh, Belgium, Bolivia, Brazil, Burma, Canada, Chile, China, Colombia, Costa Rica, Dominican Republic, Ecuador, Egypt, El Salvador, Germany, Guatemala, Honduras, India, Indonesia, Mexico, the Netherlands, Nigeria, Pakistan, Peru, Republic of Korea, Singapore, South Africa, Switzerland, Taiwan, Thailand, the United Kingdom, and Venezuela.

Countries known for strict customs enforcement on inbound international mail

Certain countries are known for having particularly strict customs inspections on incoming mail. Ordering contraband via international mail to and from these countries is up to the buyer, but generally discouraged because of the elevated risk of detection and arrest. Notable countries:

- Australia (AU)
- New Zealand (NZ)
- Israel (IL) - don't order drugs to Israel from Canada, Spain, France or the Netherlands
- Norway (NO)
- Sweden (SE)
- Finland (FI)
- Singapore (SG) and many other Asian countries
- Most Middle Eastern countries

Also inform yourself if your country is part of some kind of organization or has trade deals with other countries that allows mail to get send more easily and gets less checked.

Stealth

Stealth is important to get your ordered product to your front door. It is mainly a vendor topic (because they have to package the order) but you have to pay attention to it too, in order to avoid getting into legal trouble because you chose a vendor who is known for his bad stealth.

The important difference between stealth and decoy is that stealth is used to make the pack appear as normal as possible and also conceal the smell of the drugs. The decoy is an item that is used to hide the drugs inside the pack in an attempt to mitigate the possibility that the drugs in your pack will be found. Therefore decoys are essential in international orders because these packages get inspected two times by customs (in the origin country and in the destination country). They are not that important for domestic order though because they do not cross borders.

So if you order internationally you should look closely on the reviews for the vendor (as described in the choosing a vendor chapter) and check if they uses decoys and adequate stealth.

Non arriving packages

General

Keep in mind that some vendors mark your order shipped before they actually ship it (for security reasons and/or because they are lazy). So do not expect that they actually shipped your order out when it got marked shipped.

There can also be a lot of other reasons why your package is late (e.g. weather, postal strike, . . .), so please be patient.

Testing if your mail gets intercepted

To test if your mail gets intercepted you can mail yourself something (preferably from a post office as far away from you as possible).

- Package it carefully yourself. Remember exactly how you placed things. Take pics if it'll help.
- Get creative. Use colorful tape, make shapes over the openings of the package with it. Use a specific number of packaging peanuts that you counted out. Wrap the object you mail in some thin holiday wrapping paper. Tape that too. Go crazy! It doesn't matter if it looks sketch, shucks, might be better for it. Hell, maybe even hand write the info on the pack.
- The item you send doesn't matter so long as it's legal (I'd send one of those motion sensor cameras that hunters use to capture night time wildlife). Remember, we're trying to find out if our mails being tampered with.
- Conduct this experiment as many times as necessary.

And some more ideas how to check if the package got intercepted.

Got "Undeliverable as Addressed"?

This means that the receiver address on the package doesn't "exist", or couldn't be read by the post man/woman. This could be for a number of reasons, the most common being, you forgot to include your apartment/unit number that you live in. Other possible reasons: you spelt something wrong, you gave a fake name (don't do this). Even more possible causes: mail man/woman is dumb/blind and can't interpret

your address, the shipping address got smeared/smudged along the way, or the vendor you purchased your lab supplies from forgot to include your apartment number although you sent it to the vendor.

Scenario:

You're patiently waiting for your order to come. You think it's supposed to be here today so you check the tracking number to see it's status which says "Undeliverable as Addressed - package will be shipped back to sender if sender address is valid". You panic for a bit and then come to you're senses, but you still don't exactly know what to do. But lucky for you, you have this guide and you keep on reading ahead.

What to do if it's been **LESS** than a day since you're package was marked "Undeliverable as Addressed" (i.e. it's 12pm and the tracking number indicates your package was marked "Undeliverable" at 7:30am):

Call the post office that your tracking information says it's sitting at. If they answer (unlikely), politely explain your situation and give them your name and the correct shipping address. They may ask you to just come in and pick it up though, don't be scared cause you didn't do anything wrong. In my experiences local post office phone numbers lead to no where, or the workers just don't pick up the phone, but maybe it'll work for you.

If calling your post office doesn't work, then go to the post office that your tracking information says it's sitting at. Make sure you have your ID (or proof of residency at the package's shipping address), having the package's tracking number is not necessary but it will help a lot, so bring it. Politely (use sir/ma'am & please/thank-you) tell them that you're experiencing issues with getting a package delivered, and were told to come down to this post office to pick it up because it's sitting at this post office. If they ask what the issue is, say it was supposedly marked "Undeliverable". They'll ask for your ID, give it to them, and also give them the tracking number.

They should be able to find it, if it's there. If they don't find it, or if the cranky USPS worker essentially tells you to fuck off, then don't panic. Call the toll-free 800 USPS customer service phone number (google it), be prepared to stay on hold for 30 to 90 minutes, but stay on, because it'll be worth it. Once the hold music stops and you're able to talk to a customer service agent tell them the scenario, give them your name and full/correct address.

They'll say something like "ok we should hopefully be able to get this sent to you". Be prepared to wait another 5 to 10 days before you receive it though (that's if they were able to get the package and update the label, sometimes they aren't able to update the label if it's been too long -- keep reading if you find that happens to you).

What to do if it's been **OVER** a day since you're package was marked "Undeliverable as Addressed" (i.e. it's Jan 15th and the tracking number indicates your package was marked "Undeliverable" on Jan 13th):

Call the toll-free 800 USPS customer service phone number (google it), be prepared to stay on hold for 30 to 90 minutes, but stay on, because it'll be worth it. Once the hold music stops and you're able to talk to a customer service agent tell them the scenario, give them your name and full/correct address.

They'll say something like "ok we should hopefully be able to get this sent to you". Be prepared to wait another 5 to 10 days before you receive it though (that's if they were able to get the package and update the label, sometimes they aren't able to do that). So you watched the tracking number for a week, saw it come to your city, it looks like it's gonna get delivered, then all of a sudden you see the dreaded "Undeliverable as Addressed" error.

This is because you initially tried to fix the "Undeliverable" package issue a little too late and they were unable to update the shipping address fully and could only try and send it back to your city. This is not a problem, hopefully you caught it soon enough this time, all you need to do are the steps above with the title "What to do if it's been LESS than a day since you're package was marked "Undeliverable as Addressed". Then bam! You should have your package and be happy!

Drop

Regardless of where you choose to get your order delivered to, always have a "clean" house when you are expecting a package. That means do not have any illegal or suspicious things (like a bong) in your house or any other locations tied to your identity. That is because if something goes wrong, your properties will get searched. If law enforcement then finds illegal things, it is much harder to argue in front of the court that you are a perfectly law abiding citizen who knows nothing about the drugs that someone sent to his address.

Should I use my real name if ordering to my home address?

Yes. From the beginning, this has been one of the most debated topics for buyers. The conclusion has always been: Use your real name. No, your idea is not original. No, you are not exempt from this rule. Using your real name does not automatically make you more guilty. The point of using your real name is to blend it in with the other packages you receive. USPS keeps track of names delivered to addresses. A fake name sticks out like a sore thumb to your local postman, and the USPS computers.

If a package is discovered, it doesn't matter whose name is on it. It matters that they can prove that you ordered it, which will not be the case if you followed all the steps in the DNM bible. Using your real name increases the chance of a smooth delivery.

Living with your parents?

If you are living with your parents do **NOT** order to their house. It does not matter if they do not check your mail or know that you are doing drugs. If only a tiny mistakes happens (e.g. the vendor does not seal the product he sends properly) you parent's house could get raided by law enforcement. Needless to say that they will be *very* pissed and will know that you ordered the package. They took care for you for well over a decade and you want to show your appreciation by ordering drugs to their house?
Do not do it. Instead get a P.O. box and get your packages delivered there. Are you not old enough to open one? Then close this tab and any DNM related sites too. Seriously, DNMs are for **adults** (therefore the subs are set to 18+) not for kids who want to test out the "secret deepp dank webz and order lots of drugz".

On a funnier side, this might also be a reason for you to not order to your parents house.

Should I sign for the package/mail if asked to?

Depends on your jurisdiction. Some require it as a prerequisite to police action, others don't.

Yet, if a CD (controlled delivery) is in place to happen, you're going to get arrested. Maybe not at that point in time if you refuse to sign, but it will happen. If they have made the decision to CD you, they aren't gonna let you off the hook if you refuse to sign. Not signing will suspicious too.
Also, *signing for a package doesn't make you guilty*. Its the courts job to prove that you asked for the package, and signing for a package does not prove this.

The only reason postal services have you sign is to say that you received the package, and that they have done their job. It's a standard practice, especially for international mail and deliveries.

So why are there so many people on the "don't Sign" boat? Not signing make you feel like you have a say in the most dangerous part of the darknet process. People are paranoid and anxious, and want a say in what's happening around them. Once the package is out however, there is little any person can do against any LEO (Law Enforcement Officer) intervention.

Using a drop

Definition of a drop: a place where you are not connected to, but retrieve questionable mail from.

If you still want to use a drop, although it is **strongly** discouraged, in the following are some tips.
Note: a PO box does not fall under the drops section.

There are many right ways to do one, and your best weapon is your own imagination. Every situation is going to be different and adapting to each is part of the deal. These are not easy, but can be very worth it.

From /u/VIadThePutin posted here:

A drop address needs to be created, cultivated even. A quick run through on how I pick some of my drops:

- I pick a house with no one living in it (but not bank owned)
- Make it look lived in, including mow the lawn, weed the garden, maybe throw a kids toy out there.
- Stop by every day or two for at least a week, preferably two or three. You want the neighbors to have a vague notion of someone living there without being able to pick out your face.
- Get the mail man used to mail coming here, send junk mail to this address (This is where you pick the delivery name) cheap packages, whatever. Be mindful that Amazon mails through UPS and the USPS man won't know if you've had packages delivered. I stop by every day and put the mail on the counter inside the house, waiting a few days before opening just

  Now I run a property management business, so I have access to a rotating group of empty houses; not everyone is going to have this situation. Opening a PO box in someone else's name is a good option. I've opened boxes in my name in other states for friends before, I just give them the keys and have no idea what they do with it. I purchased for short term and my friend just keeps renewing every time the little slip says time is up. No fake ID needed, plausible deniability for me and a mailing address for them.

  Please, do not take this as all encompassing instructions for how to cultivate a drop address, this are just quick main points off the top of my head. There are lots of little things that also need doing, but depend on the situation specific to the drop you're working on.

Can I use my PO box right after I created it?

It is not necessary to wait some time **but** it is recommended. Some people order small legal items first to check if everything is working correctly. Several users reported issues with the first usage of their PO box, e.g. the employees forgot to activate the box. It would be a shame if you run into issues with a package that contains illicit items, wouldn't it? It is way better to send a test package made by you to your PO box or an amazon/ebay/. . . order first. Furthermore, consider looking into /r/freebies to make sure that you don't only have drugs coming to it though.

LE actions and how to counter them

Law enforcement makes use of several tactics to prosecute buyers. Some of them are described in the following chapters and also how you can protect yourself against them.

Controlled Delivery (CD)

What is a Controlled Delivery?

This is an attempt to accept a package containing drugs to obtain a solid reason for a search of your home to be conducted. They get you to accept the package and they believe that this is reasonable cause to believe you ordered the package and knew it was coming. **Just because a package requires a signature does not mean it is in anyway a CD**

How do people get CD'ed?

This can happen in many ways. They may order a bulk amount of product from abroad. LE may have noticed an influx of packages from the same person and inspect one and profile you for a while. You are more likely to get CD'ed when ordering **large amounts** from **another country**. Domestic packages of a smaller quantity are very unlikely to get caught, and if its a personal amount, you will more likely get a love letter and that will be the end of it. They may start monitoring your mail.

What happens in a CD?

LE will try and deliver a package containing drugs to you as you would normally receive them. Nothing will look out of the ordinary if done correctly. A common misconception is a SWAT team will come bursting through your doors shooting at everything that moves. **This is not true**. They will get you to accept the package, and they will come out of hiding and announce their presence and give you instructions on what they want you to do. That is normally step out of the house.

How much of _____(product) will they do a CD for?

This question has such a varying answers by where you live, what your past is, how old you are, how much extra time and money LEO/your local police force has, and other factors, that it cannot be answered to a global audience. Use your head. If you are ordering lots of stuff, use a drop. There is no strait definition of "Bulk". Use your damn head, and make smart choices.

What do they do after you accept the package?

They search your house trying to find other drugs you have ordered. They will look for empty letter and packages with return address on them. It is not 100% true that they always take your computer. The chances are that if you don't tell them anything, they wont know that they came from a DNM. **Do not talk to the police, only through your lawyer that you researched beforehand.**

How can I protect myself from a potential CD?

A few things can hint at a possible CD. A very long time for postage. A seizure letter from a big order or if the vendor is busted and they seize his outgoing mail.

How do you protect yourself? First thing first is basic OpSec, that means read and follow this guide step for step. Unless you know what you are doing, do not use a drop. Believe it or not, your address is one of the safest places to order to. Always use your real name and address if you can, as it's less suspicious. If you are going to get CD'ed, you will regardless if you are ordering to a vacant house or a PO box, they will catch you out if they want to. You also put the vendor at risk, so my best advice is to order to your house using your **real name**.
One of the most important things to do if you suspect a CD is to **clean your house**. It does not hurt to get rid off all illegal items and ideally suspicious items too (e.g. a bong). Because if they do not find anything in the search, its hard to convict you of any crime as you could be a completely innocent person who got drugs randomly delivered to their door. Furthermore since you used Tails there is no evidence of your current order or your previous ones. A CD does not mean you are going to get any sort of punishment, they have to find solid evidence that you ordered the package.

Is my address burned if I get a CD?

Most likely, yes. They will watch your mail for sure. If you get a CD, you can do two things. You can stop ordering from the DNMs or you can order to a friend's address. I would not recommend a drop as if they find you to be ordering drugs to another place after getting away with one CD, they will definitely bust you. If you order to a friends house using their name, if they get a CD it wont be related to you in any way, if your friend does not squeal.

Monitored Delivery

What is a Monitored Delivery?

Unlike a controlled delivery, a monitored delivery is a much rarer practice and occurs when law enforcement knowingly delivers drugs to you and then puts you under surveillance to gain evidence to further their investigation of your illegal activities in order to build a bigger case against you. This can continue over several months. That way law enforcement is able to build strong cases against suspects even if their OpSec is tight.

- Example #1
  PSA / Article: Friend of a friend got busted submitted by T00N

  Someone that goes to my buddy's school just got busted today by DEA. He'd been reselling mostly xans and coke. Turns out they intercepted a package 7 months ago but kept delivering them in order to build evidence. RIP be careful out there :(
- Example #2
  This happens all the time with large quantity imported packages. It happened to a friend of mine importing MDMA in the SR1 days. A customs agent followed him from his drop to his home and then watched him drop packs in the mail. He got off pretty light for all the shit they caught him with (6+ kg MDMA, 1-2g LSD, oodles of ketamine). And that's just the shit they charged him for. He had EVERYTHING you can imagine in bulk + some shit you can't imagine.The feds totally missed the half kilo of DMT he had heat sealed up in a big whey protein bottle and some other things that were just hidden under his bed. He'll be out of prison in 2019.

How can I protect myself from a monitored delivery?

Unfortunately you do not have many options to protect yourself against a monitored delivery, especially since you usually do not know what law enforcement is doing. It is generally expected to only see these tactics used against drug distributors and not for users ordering personal amounts.

You can use these tricks to check if you mail may be examined, although it does not guarantee success. Oftentimes the package will not appear tampered with. Furthermore it is a good idea to order as infrequently as possible to make law enforcement think that there will no be future packages.

Depending on the legal situation in your country, LE may be restricted from conducting monitored deliveries. In the USA, it does happen.

Love letter

A "love letter" is a playful name for a letter from the postal services which basically states:

We seized your goodies, but don't have the time/money to build up a case against you; and/or you didn't order enough for us to be too concerned. You lucked out bastard. Don't do it again, we are watching your address. Sincerely, LEO/Post Office/Postal Inspector

International Seizure Letters

Customs agencies around the world, including US Customs, frequently send "love letter" seizure notices to recipients of international mail with small amounts of suspected illegal drugs inside. These seizure letters are usually real.

Examples of real love letters from US Customs:

- Received Seizure Letter From US Customs for Anabolic steroids
- Love Letter & Burned Address from US Customs for Steroids
- Love letter from US Customs for importing cat meds from Thailand
- Seizure Notice from US Customs at SFO described
- Description of international package opened by US Customs - There will be **green tape** on it with black lettering that says "INSPECTED BY US CUSTOMS" and the Homeland Security logo.
  Once you get one of these love letters, consider that address burnt. Do not use it again as a delivery address for contraband. See PSA: US Customs keeps a record of all seized packages that were going to your address.
  It is possible to receive a **fake** international seizure letter. Example:
- Fake US Customs seizure letter sent from a (scamming) Netherlands vendor - LETTER IMAGE

Domestic Seizure Letters

It is very, very uncommon to get a **domestic** seizure notice for seized items sent from **inside** a country for delivery to the same country. The usual protocol when illegal drugs are found in domestic mail is to conduct a controlled delivery and arrest the intended recipient. Normally any seizure notices of this kind are simply clever scams by unscrupulous vendors. This applies especially in the USA where, 99% of the time, any

seizure letter you receive for a **domestic (US to US)** drug order is totally fake. The only time US Postal Inspectors send seizure letters for domestic items is when they have seized **cash**.

Examples of (US-domestic) **fake love letters**:

- Warning: Got [fake] domestic love letter after order with vendor - LETTER IMAGE
- Siezed Package Potentially fake? - LETTER IMAGE
- Comments on "Domestic Love Letters"
- How to tell if love letter is legitimate?

Darknetmarkets

A darknet market is a commercial website that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, unlicensed pharmaceuticals, steroids and similar stuff.

Different payment methods

Escrow

In standard escrow the market holds the money during the purchase. If you received your order you tell the market to finalize your order and give the vendor your money. Be careful: the orders finalize after some time automatically, in case you forgot to do it manually and so that the vendor has not to wait ages for his money.

If you have not received your order or have issues with it (it was less than the amount you bought or the product was not as advertised), you can dispute it. That prevents the order from auto-finalizing and you can resolve that matter along with a market staff member and the vendor in a discussion. The market staff member then decides after the discussion what actions to take (e.g. who gets the money from the order or if one of your violated the market rules). Remember to message the vendor first if you have problems with your order, instead of disputing it right away.

The big risk is that the market can always run away with that money. It happened a lot in the past, some examples are sheep market, evolution, abraxas, nucleus, middle earth marketplace, . . .

So using standard escrow is discouraged and you should use alternative payment methods.

Multisignature (multisig)

Multisignature is a form of technology used to add additional security and for bitcoin transactions. Multisignature addresses require another user or users sign a transaction before it can be broadcast onto the block chain. The required number of signatures is agreed at the start once people agree to create the address

Multisignature allows the creation of 2-of-3 escrow services. For example: when Buyer (you, the buyer) wants to pay Vendor (the vendor), you send a transaction to a multisignature address, which requires at least two signatures from the group "Buyer,

Vendor and the DNM" to redeem the money. If the buyer and the vendor disagree on who should get the money (the buyer wants a refund, whilst the vendor believes he fulfilled his obligations and demands the payment), they can appeal to the DNM. The DNM grants his signature to the buyer or the vendor, so one of them can redeem the funds. So who gets the bitcoins in a dispute is decided by the market staff.

As you can see, nobody can simply run off with your money. There always have to work two parties together to release the money (the buyer and the vendor, the DNM and the buyer or the DNM and the vendor).

So if you have the choice, please choose that payment method.

To use multisig with specific DNM please look at their help section or wiki where you should find how to do it.

Finalizing Early (FE)

If you finalize early you basically give all your money to the vendor you make your order with. So as soon as you give up your order the vendor receives the money for it. It is like giving your street dealer your money and letting him run around the block to get the stuff.

As you can see this is extremely risky because it is easy to scammed. Especially if you have a buyer account with little history (few orders). Few people would believe you, and if you do get scammed using FE, you **never** get your money back. Sometimes vendors offer a lower price for the same item if you FE for it (because it is more convenient if they get their money instantly), but it is usually not worth the risk. It is also strongly discouraged to FE for new vendors since the risk that they scam you is even higher.

When it is okay to FE:

- When you are okay with possibly never seeing your money or product again. Example: I see a new vendor who is offering an eighth of medical bud for $15 as an introductory offer. I have extra money left in my account, I'm not gonna be in a bind if the vendor doesn't come through, so I FE per his requirements. Whether the product comes or not, the worst thing is that I lose $15.
- When you are confident, absolutely positive that the vendor will still ship the product. I have to put an asterisk beside this one because even upstanding, well-known vendors have made FE a requirement and then split with the money. Anyone remember LucyDrop from SR? Most popular LSD vendor in his time. Required FE. Three months

went by without a single complaint. Then BOOM! The vendor stopped shipping and walked away with over a million in BTC. Point is that even if a vendor is "trusted", there's still a chance that they will steal your BTC; but 99% of the time, trusted vendors will be honest and send your product.

When it is not okay to FE:

- When you cannot afford to lose the money. This seems so common sense to me, but I continue to be amazed at the number of people who FE, get scammed, and lose money that either wasn't theirs to begin with or money that they just couldn't afford to lose. Example: If you're a dealer and you borrow money from either customers or someone higher in the chain to make a purchase on a QP of some dank, you should NOT FE. If the vendor doesn't send your product, you now owe money to many people. It doesn't matter how good the deal looks or how reputable the vendor is, DO NOT FE.
- When the vendor is shady or there are reports of scamming. Someone posted a couple of days ago, angry that the vendor RCI had not sent his product. He had FE'd on one of the markets and therefore could do nothing about it except get upset and post here. Why FE in this situation? His order was placed after there were bad reviews coming in for RCI. Another example is the vendor Heisenberg. He's a known selective scammer who loves when you go ahead and FE for him. You're already taking a chance by ordering from him anyway, why increase that chance by FE'ing?

FAQ

What if I am only buying legal items off a market? I'm not breaking any laws then, am I?

Unfortunately, yes, you still are. You are technically aiding a criminal organization (by paying the market fee) as well as bypassing country tax laws. Luckily it doesn't seem as though LE is very concerned at all about this and you most likely will never face any kind of legal trouble for ordering legal items off a market.

Is <market name> down?

If you cannot access a site, there is most likely a site-wide outage; you are not the only one having difficulties. Check /r/DarkNetMarkets to see if anyone else is having a problem. If you consistently cannot connect for several hours, try checking the forums and seeing if there are any postings regarding the status of the site. Do this BEFORE posting the question here!

Can I just browse DNMs, without buying anything without Tails?

No. Do not do it. If you get caught, or law enforcement for whatever reason searches your house, they will know that you browsed DNMs. Then good luck trying to explain the judge that you are a perfectly law abiding citizen. Your plausible deniability will vanish into thin air. So take the 2 minutes to boot tails and do not be the low hanging fruit.

I lost access to my DNM account, can I get it back?

It depends on the market and what information you can provide to the support. In general you best shot is to make a new account on the market and message the support. Provide as much information as possible to prove that you are the real owner of that account (like what messages you sent, what orders you made, when you created the account, . . .) and then hope for the best.

Why is <drug> so expensive?

Supply and demand dictate prices. Your street prices may be lower than the market price. The market is not beating street prices for cocaine in Columbia, MDMA in The Netherlands, or cannabis in California.

Why is the shipping so expensive?

Read this post for some insight on shipping prices.

A vendor wants to be paid in Paypal/Western Union/cash in the mail. Is this legit?

NO! This is the easiest way to get scammed. If a vendor asks you to circumvent the escrow system, immediately report the vendor to the sites's administration.

I deposited bitcoins to my account, but blockchain.info shows them being sent to a different address!

Some sites have a built-in bitcoin "tumbler" to disguise the destination of deposited coins. Once this process is complete, your account balance should reflect the deposit. Note: the market system is not a tumbler since it just deals with dirty bitcoins (the

ones from drug buyers and vendors) and dos not use clean bitcoins as a real tumbler would.

Are prices adjusted for fluctuations in the BTC exchange rate?

Most sites peg their prices in USD so prices are automatically readjusted according to bitcoin fluctuations and generally show the same USD value irrespective of the BTC exchange rate.

What are the chances of me getting caught?

There is no specific number, but it is relatively low if you follow all steps in the DNM bible.

I found this link on the hidden wiki. . .

It is very likely that this link is a scam. **Only** use links that are on the superlist and follow the instructions on there to cross check these links.

Is it possible that LE creates a new vendor account to catch buyers?

It depends on the legal situation in your country, but in general: yes. However it is rather unlikely that this will happen, because the past showed that LE prefers to bust a vendor and then take over his accounts if possible (and try to get customer addresses). So be careful if the vendor starts acting weird and in doubt ask him to sign a message that confirms that he is well with his PGP key (how to verify a signed message).
If a vendor suddenly changes his PGP key without signing it with his old one, **stay away** from him until he does so!

What are the safest items to buy/ship?

Some products are easier to conceal and ship (e.g. LSD) than others (e.g. weed) but it does not matter which is safer, but what you actually want to order. If you follow all the tips in the DNM bible (especially the "How to choose a good vendor" chapter), you will most likely be fine and can minimize the risk of your order not arriving.

I visited a market without disabling JavaScript/setting the security slider to high, am I fucked?

You will probably be fine. **But** make sure this does not happen in the future, so set the security slider to high **every time** you start the Tor browser in the future as described here.

Important tips for using markets

Tips

- **NEVER** let the market encrypt sensitive data (such as your address) for you. **Always** encrypt it yourself. The market can always store the plaintext version of your message, and send an encrypted one to the vendor. That way you both think it was encrypted while the market still has the original and unencrypted message. Also if the market gets taken over by law enforcement, they will store the plaintext versions of the messages that the users sent using the 'PGP encrypt' checkbox to harvest addresses. But they will still send the encrypted ones to the vendor to not make anyone suspicious.
- Use 2 Factor Authentication (**2FA**). It means you will have to decrypt a PGP message that was encrypted with your public key every time you log in, in addition to your username and password. Using 2 FA will greatly improve your chances of success when contacting the support of the market because you lost some funds for example (since 2FA makes it much harder for unauthorized persons to break into your account they will not just say that you got phished and close your ticket). To set up 2FA, go to your DNM account settings and look for an option to enable 2FA. Upload your public PGP key first in the settings first if you have not done it already. Here is how to create a secure PGP key.
- **Never** leave more bitcoins on a market than necessary. Ideally you should only transfer the necessary amount to the market if you also ready to make the purchase right after they have arrived in your market wallet. Leaving funds in your market wallet is too risky since the market can steal them at any given time.
- **Make sure to never tell anybody about your DNM activities.** This can not be emphasized enough.
- **Never** use the same username, password, PIN or PGP key-pair on more than one market. If an attacker or even rogue market staff gains access to your account on one market, he could easily break into the other ones as well and do even more damage (like stealing your coins or deleting your account).
- Do **not** use identifying usernames. That means your username should give no clue about who you really are, e.g. do not include your birth year in your username.
- **Never** use privnote or similar services that claim to offer self-destructing messages. Absolutely nothing prevents such services from storing your message even after it was 'officially' destroyed. On top of that they also require Javascript, which is a huge no-go. Just encrypt your messages with PGP like every other market user and send them using

the internal market messaging system. Also avoid vendors that use privnote or similar services.

- Do not check tracking at all, unless a substantial or abnormal amount of time has passed without delivery. You will only leave traces when doing so but will not make it arrive faster. For more details visit the non arriving packages chapter. If you absolutely have to check it (which should never be the case), do **not** use Tor to do it. It will be a huge red flag and law enforcement already knows about DNM users checking their packages over Tor. Instead use a third party website if possible, so not the one of your mail carrier but a website which checks the tracking for you. Examples are TrackingEx and PackageMapping. Also do not use your own WiFi for checking the tracking number. Use one that is not tied to your identity (e.g. a cafe) or use a VPN and choose a server that is in the same country as you (to not raise any red flags).
- Do not just order from the biggest vendor(s) on the market simply because of the size of their operation or because they pay for ads on a DNM or other site. Often there are smaller vendors with who offer a better product with a better customer service.
- Do you not know if it is a lower case L or upper case i in a captcha? It is almost always a lower case L.
- If a vendor suddenly changes his PGP key without signing it with his old one, **stay away** from him until he does so!
- When sending messages (no matter if on reddit or a DNM) try to write all you have to say in **one** message. Nobody likes getting hit with a high notification counter when logging in just to realize that you wrote half of the new messages. It is also easier to answer for your chat partner if you sent only one message.
- When you make an order, the status of it will be unaccepted (or similarly called) at first. When the vendor confirms/accepts your order it will be market as accepted or processing. Again the exact words vary from each DNM. The next step would be market as shipped or in transit. The last step of the order is finalized or completed.
- It is not necessary to encrypt every message you send on a DNM. You **absolutely** have to encrypt all sensitive data such as addresses or tracking numbers. However mundane questions about the product for example do not need to be encrypted, since the vendor would need much more time to decrypt all messages.
- Do not use SWIM or a variation of it. It stands for "Somebody who is not me" and is absolutely useless. No law enforcement agent will stop his work when he sees that you used SWIM. It only makes you look like a complete noob. Instead step up your OpSec which is far more helpful. Please also read the wiki section about using reddit with Tor.

- Remove the version string from your PGP public key (which is the line that begins with "Version:" and is directly under the "-----BEGIN PGP PUBLIC KEY BLOCK-----" line). It is not necessary and just gives away information about the software that you are using.
- Found a link on the hidden wiki or similar sites? It is very likely that they are a scam. **Only** use links that are on the superlist and follow the instructions on there to cross check these links.
- Are you not getting past the captcha although you always entered it correctly? Restart your Tor browser and visit the market address again to register (try another onion address if the market provides more than one). If that still does not work please go to your privacy preferences by entering about:preferences#privacy in your address bar or by going to Edit -> Preferences and selecting "Privacy" on the sidebar. Then click on the button 'Exceptions...' next to the checkbox labeled "Accept cookies from sites' (which should be unchecked). Then paste the site address (the onion link of the market that you are using) into the input field. Click on "Allow for Session" and then on "Save Changes". If you do not want to do it every time, check the checkbox "Accept cookies from sites" (it is the default setting anyway).
- **NEVER** use Tor gateways. By using them you send your login credentials and all other data in plaintext through the whole internet till it reaches the Tor gateway. So not only your ISP knows that you are buying drugs online but also the gateway can simply steal your bitcoins. Just follow the steps in the DNM bible as every other sane user.
- Get a scale. Seriously.
- **NO** market staff will message you on reddit. If you get a PM from someone claiming to be market staff, please report it to the mods of /r/DarkNetMarket immediately.
- Use KeePassX to generate and store your market, Electrum and PGP passwords.
- Unsure when to use "Bitcoin" and "bitcoin"? Bitcoin - with capitalization, is used when describing the concept of Bitcoin, or the entire network itself. e.g. "I was learning about the Bitcoin protocol today." bitcoin - without capitalization, is used to describe bitcoins as a unit of account. e.g. "I sent ten bitcoins today."; it is also often abbreviated BTC or XBT. (From bitcoin.org)

About other goods you might find on DNMs

Credit Cards: Nobody is going to sell you a physical cloned CC that you can use at a store or stick in an ATM and get money out. If they are selling them for less than the balance of the card they are basically giving you money as they could cash the cards out just as easily as you could.

Paypal accounts/transfers: People sell paypal accounts/transfers because they can't figure out how to beat paypals anti-fraud systems to cash it out. If you think you can do that better than career fraudsters go ahead. Even on the highest rated vendors for them on Evolution there were still plenty of bad reviews about accounts being locked down minutes after receiving them.

Electronics: All onion electronics stores are scams. There is already a market where you can sell electronics you have carded or stolen from stores, it's called Ebay. The reason thieves target electronics is because they can be flipped for close to face value. Why would they setup a hidden service to sell stuff as stolen for half price when they could get 75% of it's value on Ebay with much less hassle?

Darknet non-escrow "stores" in general: Unless it is being run by a vendor that started on a DNM (there should be a matching PGP key, don't trust any other proof) they are all scams. They are primarily advertised on various "hidden wiki" sites where there is no place to leave feedback. Without escrow or feedback opportunities they have **zero** incentive to ever deliver a product to you.

Counterfeit Money: It is never a good idea to order and use it. Not only is law enforcement really going hard after such people (e.g. in the US the secret service is investigating counterfeit money cases), but it is also very hard to actually use the fake money. For example the quality has to be very good, it takes very long to get rid of the fake notes and get real money back because you can not use them all at once but have to go to different places and can only carry one fake note at a time, . . . So counterfeit money is definitely not worth the risk.

Choosing a DNM

To get the legit links you should cross check your desired link with these three resources:

- the reddit superlist
- the sidebar of deepdotweb (onion link): click on the list entry of the market you are searching for and you get the link.
- dnstats.net (onion link)

All are well established sites/resources and would have much credibility to loose if they started serving phishing links. To reduce the risk of getting phished even more, you need to check that the link you got is the same on all of these three resources.

When you got the right link, **BOOKMARK THEM** and only use the bookmark in the future.
General rule: any market that jacks other markets names should be avoided at all costs.
Important: check the warnings and notes of the markets that you use on the superlist regularly! Some markets do not tell their users if security problems happen. It is therefore necessary to stay up to date about the possible dangers of using a market.

Choosing a DNM

To get the legit links you should cross check your desired link with these three resources:

- the reddit superlist
- the sidebar of deepdotweb (onion link): click on the list entry of the market you are searching for and you get the link.
- dnstats.net (onion link)

All are well established sites/resources and would have much credibility to loose if they started serving phishing links. To reduce the risk of getting phished even more, you need to check that the link you got is the same on all of these three resources.

When you got the right link, **BOOKMARK THEM** and only use the bookmark in the future.
General rule: any market that jacks other markets names should be avoided at all costs.
Important: check the warnings and notes of the markets that you use on the superlist regularly! Some markets do not tell their users if security problems happen. It is therefore necessary to stay up to date about the possible dangers of using a market.

Choosing a vendor

Choosing a vendor to buy your desired product from is an important step and you should take your time for that to avoid trouble later. It can mean the difference between you not getting the product and loosing your money and a successful and flawless purchase.

Tips

When you are a new buyer it is best to stick to already established ones because this usually means that you are less likely to run into issues and the vendor knows what he is doing. In the following a few characteristics that you should look out for when searching for a new vendor:

- Is the product description and his vendor profile informative and more than just a few sentences with bad grammar?
- How is the overall feedback of the vendor? Try choosing one that has at least about 50 positive reviews and not more than 3 negative ones.
- How is the feedback of the specific product that you want to buy? If it has significantly more negative reviews than the other products that the vendor offers you should avoid buying it.
- Does the vendor encourage bad OpSec measures (e.g. wants you to not encrypt your address with PGP)? If yes **avoid** him.
- Did you read his profile, listing description and agree with the stated terms (e.g. no refunds for new buyers)?
- Did the vendor just copy and paste texts about his product from other websites?
- Can the vendor answer questions to the products he is offering, how he is shipping, . . .?
- Are the photos that the vendor uses meaningful? Do they show the actual product with his name tag or are they just stock photos? If they contain potential OpSec compromising details, like a hand that hold the product or other things in the background, **avoid** that vendor.

- When were the latest reviews written? Are they all pretty old or a big influx of negative ones recently? If yes, avoid that vendor because he could be in the middle of an exit scam.
- Is he on other markets and how does his feedback look over there? If he has a bunch of orders, ~5 star feedback and you can not find literally anything about them anywhere else, he is most likely a scam.
- Search /r/DarknetMarkets for reviews of this vendor by using the search function on the top of the right sidebar.
- Check for manipulated feedback. If he has a bunch of feedback from the same days and the same bitcoin amount each time the he is probably padding his feedback. Also, if the bitcoin amount is lower than any of their actual orders. Often the scammers are stupid and do like 40+ feedback score the same day along with it being like $10 orders.
- Is he "over-advertising" his products? If he claims that he has the "absolute best coke in the entire galaxy" it is often not true and shows that the vendor is not honest.
- How many different products does the vendor sell? This can be a red flag because vendors who sell a large selection of very different products can be greedy and care less about their OpSec. That means they rather have a couple of thousands dollars more in exchange for a higher risk and harsher penalty.
- Is the vendor saying that you can not leave neutral or negative feedback or dispute? Buyers should contact the vendor before leaving negative feedback or disputing, to give the vendor a chance to resolve the issue. If they do not manage to do it, then the customer can leave a honest review which reflects his experience with the vendor and the product. If a vendor does not want to "allow" you to leave negative feedback or to dispute, it is a red flag since if you run into trouble with him you will have a hard time even if you are right. Stay away from such vendors.
- How many views and sales does his product listings have and for low long are they up? If they are for example up since 4 days, have a couple of dozen views but a bunch of sales, it is suspicious. Especially if the listing is a rather expensive one. It could indicate that the vendor is manipulating the feedback, be careful and stay away when in doubt.
- Check his products and his prices. Many scammers post bulk products for pretty cheap. Cheaper than normal.
- Does the vendor post on the weekly 'DarkNet Deals' thread on /r/DarknetMarkets? If yes check if he uses appropriate image hosters. A no-go would be imgur.com: they do

not allow Tor users to upload images and require you to enable JavaScript. So if the vendor used it, he has bad OpSec and you should **avoid** him. To check if an image hoster is appropriate, visit that site and try to upload an image that you grabbed from /r/pics. If it is possible while using Tor and without enabling Javascript, then the image hoster is okay.

If a vendor does not choose you

Sometimes vendors decline orders without giving you a reason. Possible causes could include:

- Out of stock. If the vendor did not edit the "items left in stock" option or the market does not even have one, they could cancel the order.
- Bitcoin fluctuations. If the Bitcoin price drops drastically and you already sent the money into escrow it would mean that the vendor gets less money in Bitcoin than he initially charged for the product after the transactions is done. If a vendor does this you might consider not buying from him again because they will always accept your orders when the Bitcoin price rises so that they get more money than they initially charged for the product.
- Lack of feedback on your account. Some vendor prefer to only deal with buyers that already have some feedback and history on their accounts, because the chance that the transaction will go flawlessly is higher and the risk that you are an undercover LEO is lower (because they would need to make several purchases before being able to order from that vendor).

Types of scams

Here an example of a vendor scam broken down to the details.

Scammer	Scam Field	Scam Description	How To Spot It	How To Prevent/Fix It
Vendor	Feedback	Vendor pays users to purchase items, never delivers them but users leave positive feedback to make it look like they were legit sales (to prevent the feedback manipulation being tracked back to the vendor).	Multiple feedback that have similar qualities & spelling.	Check the forums, reddit, and any vendor review threads for the vendor.
Vendor	Feedback	Vendor uses an alt/puppet account and vote on their own product.	Multiple feedback that have similar qualities & spelling similar to vendor profile.	Check the forums, reddit, and any vendor review threads for the vendor.
Vendor	Feedback	Vendors blackmail clients to leave positive feedback.	Multiple feedback that have short, hostile, or confusing reviews. Reported on forums.	Check the forums, reddit, and any vendor review threads for the vendor.

Scammer	Scam Field	Scam Description	How To Spot It	How To Prevent/Fix It
Vendor	Escrow	Send empty box to the customer as tracking also indicates it arrives. Photo evidence is not supported as buyer could remove item and take photo.	Feedback indicating package never arrived, vendor reviews	Verify the vendor is legitimate and feedback supports all claims. Ask for tracking.
Vendor	Escrow	Not send any item and receive 50% to 100%, of which all is profit.	Feedback indicating nothing was sent. False/Non-responsive tracking numbers issued.	Verify the vendor is legitimate and feedback supports all claims. Ask for tracking.
Vendor	Finalize Early	Not send any item and receive 100%, of which all is profit.	Feedback indicating nothing was sent. False/Non-responsive tracking numbers issued.	Verify the vendor is legitimate and feedback supports all claims. Ask for tracking.
Vendor	Feedback	Sends a fake love letter instead of the product	You get a love letter that does not look like it	Check if it is known how a real love letter looks like, show the

Scammer	Scam Field	Scam Description	How To Spot It	How To Prevent/Fix It
			comes from an official source.	support the alleged love letter.
Buyer	Feedback	Extort vendor for more items/refund on terms of feedback manipulation.	Hostile buyer, demanding products	Make sure you know your buyers before you sell to them, and limit firs time sales to small items.
Buyer	Feedback	Leave negative/bad feedback even when order was successful	Buyer messages that seem confused, or buyers that seem unaware of how to fully use the market.	Make sure your buyer is intelligent enough and understands that markets native language of the market. Start with small orders.
Buyer	Finalize Early	Finalizes Early	Buyer makes assertions that they will FE, or that FE will be done as a complement.	Simply inform buyers that FE is not required, and state it on your profile several times.
Buyer	Escrow	Finalizes Early	Buyer makes assertions that they will FE, or that FE will be done as a complement.	Simply inform buyers that FE is not required, and state it on your profile several times.

Scammer	Scam Field	Scam Description	How To Spot It	How To Prevent/Fix It
Buyer	Escrow	Buyer claims item did not arrive when tracking indicates it did.	Resolution or PM indicating the order did not arrive.	Send the tracking number. If it is valid, it can be used to obtain 100% resolution.
Buyer	Escrow	Buyer claims item did not arrive, no tracking avaiable.	Resolution or PM indicating the order did not arrive.	Bring it to resolution, and use tracking in the future.
Buyer	Direct Message	Buyer makes threats over order instead of sending it to resolution	Hostile or otherwise self-centered buyer messages.	Do not respond in anything less than a professional manner, do not antagonize the or over explain things, and report them immediately to the admins.

How to be a good buyer

Being a good customer is just as important as selecting a good vendor. So here are some tips that will help along a smooth transaction.

- Always order sober. You will make mistakes if logging into a market while being high.
- Always read a vendors page completely before ordering. They may have special requirements to be met. Most questions for them can usually be answered this way.
- Be polite (to the vendor **and** market staff). This usually will take you further than expected.
- Do not wait for the last second or hour to dispute. Sometimes the market clock counts differently that you expect, so make sure to dispute at least half a day before the Auto-Finalize timer runs down. Also do not forget to contact the vendor first if you have issues with your order instead of disputing right away. Often they are interested in solving the problem without a dispute.
- If you are in a dispute: be calm and respectful. Explain your situation using just the facts available to you, no assumptions or accusations. Provide a desired outcome to your problem. Express willingness to compromise in situations where it is appropriate.
- When sending messages, use proper grammar and well structured sentences. Always encrypt your address properly yourself.
- After you make a purchase, log in within a day or two afterwards to make sure the vendor doesn't have a question or issue with your order. Keep checking until it says shipped.
- When you receive your package, finalize the order so the vendor gets their money. But **wait to give feedback until you have tested the product**. There is much feedback like "I'll update once tried" or something along the lines of that. You often can not update feedback once it is placed.
- Keep any chatter to a minimum and keep it short and sweet. Most vendors time are valuable to them.
- Be patient. Remember that this is not Amazon. Most vendors have a special way of getting packs out. A good rule for domestic orders is 7 days Tor-to-door. This is a very reasonable amount of time.
- **Never** ask for tracking unless a substantial amount of time has passed. And before asking for those tracking numbers, ask the vendor if they could give a heads up on the pack first.
- Don't double encrypt. That means encrypt your address using Tails and then paste that address into the message field on the market. Leave any checkbox that offers PGP encryption unchecked, otherwise the message would get encrypted twice which adds no

necessary security boost and only annoys the vendor. To read why you should never let the market encrypt sensitive data for you please go to the important tips for using markets chapter.

- You do not need to include your public PGP key in the messages you send to the vendor since you already have it entered in your market account settings (if you have not done it yet, please do so **immediately**). If you still want to, you can include it at the bottom of your first message to that vendor (like "Here is my public key: <public key here>") so he does not have to go to your profile to get your public key.
- Leave honest feedback and finalize the minute you get your pack and have assessed it's contents.
- Keep your PGP keys current on the market. That means if you key expired after a year, you should immediately replace it with the newly generated one in your settings on the market.
- Do not message a vendor before making an order and claim that you "usually move 10k pills a week but you are only ordering 150 from him to test them out to make sure they are legit" in hopes of getting some sort of deal or preferential treatment. Vendors get these messages all the time. They know that you are not some big player moving massive bulk, you are just someone hoping to get a discount by making a vendor want to land a "big fish" like you. Vendors get tons of messages every day and they notice buyers who are simple to work with. Eventually after a few seamless and easy orders, you can send them a PM telling them you like their service and ask them if they can get bulk orders bigger than what they list and what the prices they would be. Then they may start offering you better deals.
- The vendor does not need to know that you will be placing an order in a few days.
- If you agreed upon a special request, specific artwork, different stealth, modified shipping, etc with a vendor, put that same info in with your address. That way when the vendor is working on your order, it is right there in front of him again.
- Did you get too much or another product? Contact the vendor and tell him the situation. You will not be forced to send the product back or send the vendor some money, but the vendor knows that he made a mistake while packaging. Then he also does not have to wonder why the other customer is not receiving his order.

Getting a lawyer

If you get in legal trouble

Note: this mainly applies to americans. In other countries, such as the UK it can be different and for example remaining silent could be used against you. So make sure you research the legal situation in your country on your own too.
If you ever encounter law enforcement due to serious issues (e.g. a controlled delivery) say nothing. Shut the fuck up. You could have the best lawyer on speed dial but still get a decade in jail because you talked to the police and incriminated yourself (willingly or unwillingly). Here a good video about how to talk to law enforcement. Here another resource from a lawyer who sometimes posts to reddit too (/u/kenpopehat).

Do not even deny anything. If you haven't been arrested yet (even if they 'detain' you), the only two things which should come out of your mouth are: "Am I free to go?" and some version of "Me. Lawyer. Now." plus that you invoke your right to remain silent.

To add to this, you should avoid making any statements because anything that ends up not being true can add another crime to your list. They'll likely come at you with all kinds of scare tactics and/or promises/deals. Let them work that out with the lawyer you demanded.

Getting / Researching a lawyer

This is a crucial and important step. You **have** to do the steps in this chapter before making your first order, because if you later get in trouble you will not have time to research a lawyer properly.

As soon as you get in legal trouble law enforcement will try to get you to talk and admit as much crimes as possible. They often use different tactics to achieve that and a good counter measure is searching for a lawyer beforehand. If you later get in legal trouble you just have to tell them that you only speak with your lawyer and can avoid any incriminating discussions with law enforcement officers.

It is best to search for **two** different law firms who have much experience with drug cases and are also successful at their job. If you found two good results write their numbers and locations down on **several pieces of paper** (because your electronic devices might get seized during a search). Store them for example in your wallet, desk and phone case.

If you ever get in legal trouble you now can just call a number from the note and if the first one is unavailable you can try the second one. Also remember to keep a bit money on the side to pay your lawyer if you have to hire one.

Moreover do not forget to **look up the laws that you are breaking**. You can easily avoid harsher sentences by avoiding pitfalls if you know about them. An example would be not using/having guns when also violating drug laws, because that will increase your penalty drastically in many countries.
IF LAW ENFORCEMENT IS QUESTIONING YOU, TELL THEM YOU ONLY SPEAK TO YOUR LAWYER. Do not get intimidated by their scare tactics. No person ever said "Fortunately I talked to the police first and told them everything before contacting my lawyer".

Making a purchase

Do you have PGP, Electrum and your market account set up? Good, now go **back up that data** so you do not loose access to your accounts and money.

Tips

Making a purchase is one of the better parts of all of this. Before you do there are some things that should be considered.

- First timers and noobs should stick with domestic orders to get a feel for how his works.
- Make sure you have performed proper market and vendor research.
- Be safe and be sure you have researched the product you intend to buy. (This is very important. Respect these substances and your body. Erowid has reliable dose charts, first hand experience reports, substance laws and many other treasure troves of knowledge about many products found on the DNMs).
- Knowing exactly how much to send to the market (cost of product, shipping and commission fees) and having that coin ready is another good practice.
- Sometimes it takes a while to transfer BTC into a market wallet. BTC is volatile and the price can rise or drop very suddenly, so it is also a good idea to send a little more than expected. You can always withdraw any left over coin to a personal wallet once the order is placed (and you should always do so).
- **Double** and triple check that you wrote your address correctly: either according to the vendors preference which is detailed in his profile description or to the recommended standard for your country. If you fuck it up you could get in legal trouble and the vendor will not be happy either. Once you have made your first order, store your written address in a .txt file in your persistence directory (home/Persistence) and copy it form there for every future order. Also do not forget to check if the vendor wants another format as the one you copy from your .txt file.
- Include your **PGP encrypted** address in the order. Most markets have some kind of order/buyer notes in which you have to put it.
- If you, by any chance, make a mistake when providing your address in the order information, let the vendor know as soon as possible.
- Remaining in escrow or using Multi-Sig is a good way to keep from vendor exit scams.

- If you have already entered your public PGP key in your profile settings (which you should **absolutely** do), it is not necessary to include it in your messages to the vendor.
- If it looks too good to be true, it probably is.
- Overnight shipping: overnight is highly unlikely from any vendor. It is misleading because it is not true overnight shipping in the vast majority of cases since the order arrives almost always later.

Giving Feedback

Tips

Giving feedback and rating a vendor is just as important as escrow or multi-sig. It is your voice to the vendor and any future patrons of that vendors business. Rating a vendor and leaving feedback should be taken seriously. It's truly the only means of regulating how business is conducted and it's what maintains the purity of products you find on the markets. The combined feedback and ratings left by customers is paramount when choosing a vendor. Here are the main factors to consider when rating a vendor.

- Communication: Although this should be kept to a minimum and sometimes not needed at all, speed of responses and professional interactions are important.
- Efficiency: The speed at which the order is accepted and marked shipped. (The arrival speed is out of the vendors hands and falls on the delivery service. 7 days Tor-to-door domestic is a fair margin, also consider holidays and poor weather.)
- Packaging: Vac-seal is an absolute necessity. Adequate stealth should be considered also, but not every vendor goes overkill. Your purchase should be scent and weather proof with some visible barrier in case the package is damaged in transit.
- Weight: You should receive what you pay for. Heavy packs are common and should be praised, but light packs are just as common and should be just as known.
- Purity: Again, you should get what you pay for. The purchase should come as advertised and should be known to the user before leaving any rating or feedback.

Ratings are very important to a vendors business, but the feedback is very important to the rest of the community. Your feedback will exist as long as the vendor shop is open (other users will not know who wrote what) Here are a few tips that will ensure your feedback benefits others.

- Feedback should only be left after you have received the pack and have assessed it's contents. This should be the same time that you finalize the order.
- It should be honest so other people will know what to expect.

- Remember that this is the DarkNet and not Amazon, and anything less than a perfect rating can really harm a vendors business, so be reasonable when considering how you rate them.
- Before leaving bad feedback or anything less than a perfect rating, contact the vendor to see if they could make things right first. Be courteous and you might end up leaving a perfect feedback after all.

  If you want to post a review on /r/DarkNetMarkets too make sure that you follow the steps in the using reddit and Tor chapter and use one of the vendor review templates. To include images in your review, make sure you read and followed the uploading images securely chapter.
  And here some more tips for making a useful review.

Getting threatened/blackmailed by a vendor

Sometimes vendors go full-retard and threaten you. Sometimes they even want to dox you (releasing your personal information like your address) or report you to law enforcement.

If that happens to you, you first of all need to **stay calm**. Follow the steps here and you will have little to worry about. Furthermore you should report him immediately to the market staff and tell them the situation in a normal tone and without any insulting, bad grammar or panic. That way you will have the best chances to win the argument in your favor and get the vendor banned.
If you followed the tips on how to be a good byuer you already have an advantage, because all your messages were written in a polite, clam and respectful way. So the market staff will clearly see that you stayed down-to-earth and the vendor is probably the one going crazy.

Threats like sending law enforcement to your address are rarely followed though by those who write them because they would have to compromise their own OpSec (e.g. by calling the police) and it would be a lot of hassle any way for them just to fuck with one buyer. So these threats are often just to scare you into giving in and handing your money over to the vendor.

However also clean your house so that there is nothing illegal or suspicious (e.g. a bong) in it for the worst case. That way you will be innocent even if law enforcement visits you. That the vendor personally visits you (or sends someone) is highly unlikely because he is just a pussy who wants to win the dispute by threatening you while

hiding behind a computer screen. It is probably also a good idea to not make new orders for some time, at least till that matter is resolved.

You can also make a post on /r/DarknetMarkets naming and shaming the vendor as long as you also publish the proof for it.

Uploading images securely

Images can tell the world a lot of information and can even reveal your true identity although you have followed all other steps in the DNM bible. So it is important to read and follow this chapter too because it can literally mean the difference between freedom and jail.

Just do give you an example of what basic forensic video/photo software is capable of doing. Now imagine what forensic software on steroids law enforcement can buy with all their money.

Making a photo

Even if you follow all the tips in this chapter it is still possible to identify the camera that you used because of other camera specific data that is much harder to obfuscate. Therefore it is highly recommended to either use a throwaway camera or one that you never used to make pictures that you uploaded online somewhere.

To get the image for your camera or mobile phone onto Tails, simply stick the SD card into your computer or connect your mobile phone with a USB cord to your computer when you booted Tails.

Removing traces

To remove at least some of the traces of the images that you want to upload, do the following steps. Keep in mind that this is not 100% protection against all the forensic methods out there.

Right click on the image, hover over "Open With" and select "GNU Image Manipulation Program" from the context menu.

Note: you can enable the Single-Window Mode by clicking on "Window" (at the top of the middle window which shows your image) and then selecting "Single-Window Mode". This may make GIMP a bit easier to work with.

Then crop the image to remove any background details that could identify you using the "Crop Tool" in the toolbox (on the left side, click on the icon knife icon which says "Crop Tool: Remove edge areas from image or layers"). After you selected the area that you want to keep in the image, press Enter.

Now apply some noise to the image using "Filters" (at the top of the middle window) > "Noise" > "HSV Noise". The default values should be enough to remove any unique differences in the sensor in the camera that may be used to identify you. However if you are paranoid, play around with the settings to find something that is still relatively clear but applies more noise.

Save the image by going "File" > "Export As..." and store them in your Persistence folder. Uncheck all the options that you get (the list that contains entries like "Save resolution").

Repeat the above steps for each image you want to upload.

Note: this process also remove the EXIF data. It is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Almost all new digital cameras use the EXIF annotation, storing information on the image. That information can be used to de-anonymize you, e.g. because your smartphone put the GPS coordinates where the photo was made automatically in the EXIF data. But you do not need to worry about that any more as that data is already removed.

Optional: To verify it you can right click in the file browser and select "Open in Terminal". Then enter the command (assuming your image is named image.jpg):

```
exiftool image.jpg
```

That will return a short table of information which does not contain any unnecessary information that could de-anoymize you. To see the difference you can execute that command before you clean the metadata.

Copy the now clean images to Home > Persistent > Tor Browser. This is important because the Tor Browser can only access that part of your file system.

Note: even the filenames may be used to identify you. So change them to remove any information that might be useful to LE (including date/time).
If you don't want to keep the images, securely delete them from your persistent volume using right click > "Wipe". You should also **wipe the images from your phone or camera** using a secure deletion tool if possible. If not, please remember that simply deleting the images will leave the data on your camera until it is written over with other images.

Uploading it

To choose an image hoster to upload your image please use the superlist. Make sure that you choose one that allows Tor users to upload images (which is the case with every listed hoster on the superlist). Ideally it should also not require JavaScript for uploading nor viewing images and, if it is a clearnet site, provide a secure connection (https instead of http).

Alternative communication methods

Usually it is not necessary for buyers to use the following alternative communication methods since the internal market message system should be sufficient. However it can become necessary to use them if for example the market the vendor uses goes down and you want to stay in touch with him. Therefore the following chapters will be dedicated to using alternative communication methods without compromising your OpSec.

Email

Note: Email providers, especially those run by anonymous people (as most .onion email providers are), can go offline at any time. This happened a lot in the past and will happen in the future too. So make sure you always back up the emails you want to keep and do not have important accounts tied to these email addresses (e.g. 2FA for a valuable Bitcoin trading account).

In order to use email securely to communicate you have to pay attention to the following points:

- Choose an email provider from the DNMSuperlist or a similar one that allows Tor users and is known for not being very responsive to government requests.
- The email provider should be completely usable **without** having to enable Javascript.
- **Always** use PGP to encrypt the emails you send and make sure that your communication partner does the same too.
- **Never** give away information in the subject field. Although the content of your message is encrypted with PGP you can still give away information with the unencrypted subject field. For example do not use "about the $4k drug deal we made" as a subject but rather something like "subject".
- Research the name of the email provider on /r/DarknetMarkets using the search function, and check if there are any notes or warnings on the DNMSuperlist entry if it is listed on the Superlist.
- Do not forget to check out /r/emailprivacy too. There are a lot of useful tips, guides and links on there.

Jabber / XMPP

General Information

XMPP is a communications protocol which enables the near-real-time chats between any two or more network entities. That means it's like a skype or facebook chat between two or more users. It was originally named Jabber, a name which sometimes still gets used for it.

Following this guide you will be able to send end-to-end encrypted messages in real time for free.

How to configure Pidgin and OTR Plugin

Pidgin (formerly named Gaim) is a free and open-source multi-platform instant messaging client. It has support for many instant messaging protocols, allowing the user to simultaneously log into various services from one application. That means you could chat with your facebook / google talk / AIM friends using only Pidgin and not visiting the website itself (e.g. facebook.com).

Pidgin is widely used for its Off-the-Record Messaging (OTR) plugin, which offers end-to-end encryption. For this reason both (Pidgin and the OTR plugin) are included Tails and you just have to set it up correctly. However your chat partners have to have the OTR plugin too (Pidgin is not necessary, they could use a similar tool) in order to be able to chat with you this way.

The OTR plugin ensures the messages cannot be recovered by a third party because it uses Perfect Forward Secrecy. However as always your other chat partner could always keep logs of your conversation without you knowing or be compromised.

First open Pidgin by going to Applications (at the top left of your screen) -> Internet -> Pidgin Internet Messenger. Then two separate windows should open. On the one called "Buddy List" go Tools -> Plugins and scroll down the alphabetically sorted list till you see an entry called "Off-the-Record Messaging". Make sure the checkbox on the left of it is checked, then select the entry and click on "Configure Plugin".

Ensure that the following options are selected:

- "Enable private messaging"

- "Don't log OTR conversations"
- "Automatically initiate private messaging"

Now close the configuration window and the plugin overview window.

Getting an XMPP account

To be able to chat with someone you still need to register an account. You can do so for free on the XMPP servers listed on the superlist. Some XMPP servers do not log connecting IPs or greatly limit what they log. Policies are decided entirely by each individual XMPP server administrator. The ones listed on the superlist however are rather privacy friendly and you are using Tor (by using Tails or Whonix) any way. Some may require registering your account through their website and cannot be registered through Pidgin. The registration is usually quick and easy in any event.

In the "Buddy List" window go Accounts -> Manage Accounts which should switch you to your second window (the "Accounts" window). Click on the "Add" button and select the following options:

- Protocol: **XMPP**
- Username: **YourDesiredName**
- Domain: **jabber.calyxinstitute.org** (or whatever jabber server you want to use, see the linked list above)
- Resource: Leave blank. It indicates which device you are using, not important.
- Password: **(make your password strong and unique)**
- Check the checkbox called "Create this new account on the server" at the bottom

To finish click on the "Add" button and wait a short time. Then you should get automatically presented a window to enter your username and password which you previously set in the configuration. Enter them and click "OK". Then you should get the message that the registration of your account was successful.

After that go to the account window and check the checkbox on the left of your new account to enable it. This should ask you again for your password and after a short time the status at the bottom of the "Buddy List" window will change to "Available" with a green circle on the left of it.

For the XMPP server used in this example you also get a welcome message telling you their twitter account and that you should donate if you find the service useful (which you should do if you have some leftover money or donate them here).

Chatting with someone

After doing the above steps you can now add other XMPP users to your buddy list by going to: Buddies > Add Buddy (close and re-open all the Pidgin windows if the "Add Buddy" selection is disabled).

Now enter the username the the other person gave you. I could for example be *username99@jabber.calyxinstitute.org*. Optionally you can also set an alias for him in the line below which gets shown in the chat window when you chat with that person (instead of the long username which you previously entered). To confirm click the button "Add".

The user you want to add will receive a notification when he comes online again where he gets asked to authorize you (he sees your username). He has to click the "Authorize" button and confirm the new dialog window where he can also set a local alias for your username.

When he did that and he is currently online, you will see him in your "Buddies" list. You will also see the small authorization notification at the bottom of your "Buddy List" window where the other user wants to add you to their buddy list. Click on authorize.

That's it! Now double-click on his name in the buddy list, click on the red "Not private" at the bottom right and select "Start private conversation". Then the chat window will print some messages like "Attempting to start a private conversation with <other user's username here>" and something about authentication. Another window will also open and tell you something about creating a private key. When the text in it has "Done" at the end you can close the window by clicking "OK".

Your chat partner will see a new message window too with the authenticated-messages and the generated private key notification too.

Now you both can chat securely!

Authenticating your buddy

About the authentication messages: while you have established a secure chat with some other user, it may be the wrong user. That means you could chat the whole time with a wrong person who might be malicious. In most cases the other person (your are now chatting on XMPP with) gave you his XMPP username through an encrypted message or a similar channel.

So if you are sure that the message (where he told you his XMPP username) that the other user sent you could not be manipulated, then you can skip the authentication / verification. If however you received the username through for example a clear text message on a DNM, this message may have been tampered with by LE who might have taken over the market. So to be sure that you are chatting with the right user, do the following.

Click on the "Unverified" at the bottom right and select "Authenticate Buddy". Now you can enter a question and a secret answer. It is sufficient if you choose for example "check your email account" as a question and a random string like "Af!J}m" as the secret answer. Before you click on the "Authenticate" button, send the other user that secret answer through a secure channel first. For example using his PGP key you have saved and sending an encrypted email to his email address that he usually uses. The content can be like "The answer to my authentication question is <secret answer here>".

Now click the "Authentication" button and you should get a window waiting for the authentication to be completed. The other user now gets prompted to enter the answer for your authentication question and if he does it successfully then you will see the content of your authentication progress window change to "Authentication successful". You can close it by clicking "OK".

Now you have confirmed that you not only established a secure chat with some user, but also with the correct user. The other user can also decide to ask you such a authentication question so you are marked as authenticated on his side too.

Closing Words

Have you read **all** chapters of the DNM bible? Good! Now you know how to greatly minimize the risk of ordering drugs using DNMs. You will never completely erase the risk of getting caught, but you can make it damn hard for law enforcement to catch and prosecute you by simply doing what is written in the DNM Bible.
If you want to show your appreciation for this guide, you can donate to the projects below and/or be a helpful and friendly users on /r/DarknetMarketsNoobs where you may help other new users to be safe while ordering on DNMs.

Do you ever look at the many DNM drug listings on your computer screen and feel like a small kid in the candy store? Well this is possible due to the relentless work of many people who donate their free time. So it is only fair if you show your appreciation by donating to them once in a while. If you have money for drugs, you can also spare a few bucks for donating:

- Tor Project
- GnuPG
- Whonix
- Tails

And do not forget our fallen heroes. Ross Ulbricht, the man who played a significant role in creation of the DNM scene, has to pay a hefty price for implementing his revolutionary ideas.

/r/DarkNetMarkets will rise again.