Welcome to the DNM Buyer's Bible

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 /d/ DarknetMarketsNoobs already has that issue covered. If not feel free to make a post on this subdread 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 However these are just as additional information because software often changes and these gifs can quickly become outdated.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.

Happy reading and stay safe.

Any requests or changes feel free to send me a message on Dread Shakybeats

Version 2

Author: /u/Shakybeats

Co-Authors: /u/Thotbot /u/WilliamGibson

Speial thanks to the entire Dread community that worked on this in so many different ways
/u/Edgar_allen_Poe /u/HumanPie /u/DrHorrible /u/SamWhiskey /u/Blonger /u/BadMedicine the dread team, and anyone else I am forgetting! All of these people pitched in with everything from ideas, writing, and edits. Half the information wouldn't be available without this group.

Version 1

Author: /u/wombat2combat (from reddit and Dread)

Co-Authors: /u/Seraphim_X (reddit)

Special thanks to these reddit users: /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

---

Before you start□

So you are about to read how to commit felonies and reduce the risk of getting caught. It is strongly recommended that anything that could be considered Darknet related you don't do on your normal operating system, or default browser. Keep your darknet activity as far away from your real identity as possible. 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
- 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 /d/DarknetMarketsNoobs .□

Operating Systems□

Using a secure operating system is one of the most important parts of using the darknet. The main operating system we will be focusing on in the guide is called **Tails** we will also be mentioning using **Whonix or Qubes.**

NOTE: You will see this note come up a few times as you read on, but it cannot be said enough. DO NOT USE WINDOWS OR OSX.

Tails□

If you’re a new user or someone not very tech savvy you should stick with using tails. Most of this guide will be written around using tails, and it’s pretty easy to use!

Why tails?Tails is secure live operating system that will work out of the box. Most software we will use will be included right in tails.

Whonix/Qubes□

Using a Whonix/Qubes setup is one of the most secure setups. This setup is very advance, if you do not configure everything correctly you can potentially hurt your opsec or put yourself at risk. If you do not know what you are doing just stick with using Tails.

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?

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).

- 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)

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).

Installing Tails□

Tails has very detailed guides that will walk you through the entire installation process.
Click here to install from windows

Click here to install from MacOS

Click here to install from Linux

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 /d/DarkNetMarketsNoobs about it.

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.

Tip If you're having problems getting your computer to boot to the bios/boot menu. You can hold down shift while click restart. From there select USB device or go to advance options and select UEFI options.

Important settings and tips□

- **Every time you start the Tor browser, you have to set the security slider to safest**. 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

- **If a DNM site ever asks you to enable JavaScript, leave *immediately*.**Ideally warn the community on /d/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.**

- **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.

- **Can I run tails on a virtual machine?**
  No tails is desgined to be a live OS and will not function properly in a virtual machine.Read about it here

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.

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 coins with it.

Backing up will only take a few minutes over your time be sure you do it regularly!

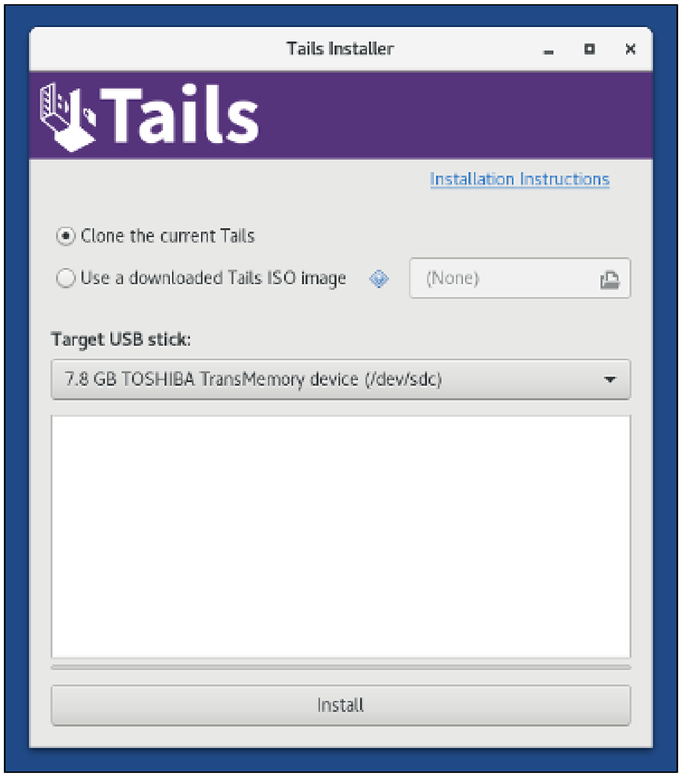
To start you will need another USB that you wish to back your system up onto.

Cloning Tails□

Note: First thing we need to do is clone your current tails drive. If you already have Tails cloned you can jump down to the backing up Persistent Storage section below

Note 2: This part will NOT backup your persistent! You must clone tails before you can backup

- First login to the tails USB you want to backup. Once you are logged in to Tails plug in your USB stick that will serve as your backup.
- Now go to Applications-> Tails -> Tails Installer (or you can find it on the sidebar)
- A window like this will open



● Clone the current Tails
○ Use a downloaded Tails ISO image (None)
Target USB stick: 7.8 GB TOSHIBA TransMemory device (/dev/sdc)

- Select Clone the current Tails, and select the USB that will be your backup on the Target USB stick Drop down menu.
- Click Install
- Read the warning message in the confirmation dialog. Click Yes to confirm.Depending on your computer will vary how long the installation will take. The progress bar usually freezes for some time while synchronizing.
- Finally it should say Installation Complete!

You now have cloned tails!

Backing up your Persistent Storage□

Note: If this is your first time backing up to this USB you need boot into your backup USB first enable persistent volume and everything else you want enabled. (Electrum, GNUPG, DOT files)

- Once everything is enabled on your backup drive, boot back into your main Tails drive that you will be backing up.

On the Welcome Screen, enable the Administration Password. You can make it whatever you want it will reset after you shutdown tails. (Click the + in the bottom left)#Insert welcome screen image

- Once you have booted up tails with the Administration Password enabled go to, Applications-> Accessories-> Files to open the Files browser
- Plug in your backup USB stick.
- You should see a encrypted volume in the sidebar of the Files browser. Click on it and enter the Persistent storage password for your BACKUP tails.
- It should now appear as TailsData volume on the sidebar.
- Open up root terminal. You can either go up top and type terminal and click root terminal or go Applications-> System Tools -> Root Terminal enter the Administration Password that you made.
- In Terminal run the following command:

```
rsync -PaSHAXv --del /live/persistence/TailsData_unlocked/ /media/amnesia/TailsData/
```

When the command finishes running you should see something like this displayed:

```
sent 32.32M bytes received 1.69K bytes 21.55M bytes/sec
total size is 32.30M speedup is 1.00
```

Congrats you have successfully backed up your entire tails drive!Going forward you do not need to clone your drive again. You can just boot up with administrator password enabled, unlock your backup, and run that command. It will update the backup for you.

This only takes 5 minutes to do! Remember to take regular backups so you don't lose your shit!!

Optional: Install Debian Packages on Boot□

This is an **optional** part if the DNM bible. Please only follow the instructions here when you actually need to install further packages. It is not necessary to install additional software because Tails already has everything you need installed. Any additional software is a security risk. Tails has a facility for automatically installing Debian packages on boot up.

Boot Tails.
Enable persistence and assign an administration password.To use this system, you should enable the following two persistence items by clicking on them so that they have a green check mark in the Tails persistence wizard. (Applications ->

Tails -> Configure persistent volume):

APT Packages
APT Lists

If those items were not checked, then reboot so that the settings can take effect.If you needed to reboot, enable persistence and assign an administration password again.Start a root terminal (Applications -> System Tools -> Root Terminal)Type the following commands:

```
apt-get update
```

(this will take awhile, probably 5 to 10 minutes)In this example, we are going to install the following package:gpa (The GNU Privacy Assistant - a familiar PGP client)Type the following commands:

```
apt-get install gpa
```

(enter y to confirm installation of the package)

```
cd /live/persistence/TailsData_unlocked

gedit live-additional-software.conf
```

Add the following line to the empty file:

```
gpa
```

Save the file and exit gedit.
(You will get some warnings from gedit. They are safe to ignore.)Normally when you install software on Tails using apt-get, it is erased when you shutdown and you have to re-install it next time you boot. Using the above apt persistence settings, the downloaded software is saved locally. By listing items in the “live-additional-software.conf” file, the system will automatically unpack and install them on boot.The packages are unpacked by a separate process, so that the boot up time is not extended too much.A status message will pop-up when the system is done installing the software reading “Your additional software / The upgrade was successful”.
To start the PGP client GPA, Select Applications -> Accessories -> GNU Privacy Assistant.

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 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 .
- 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 /d/DarknetMarketsNoobs subdread to search for solutions for your problem. If that does not help you can make a post on /d/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”).

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 /d/DarkNetMarketsNoobs or /d/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:

- /d/Whonix
- /d/VirtualBox

What is Whonix?

It's basically like a sandboxed and torrify'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.

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.

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.

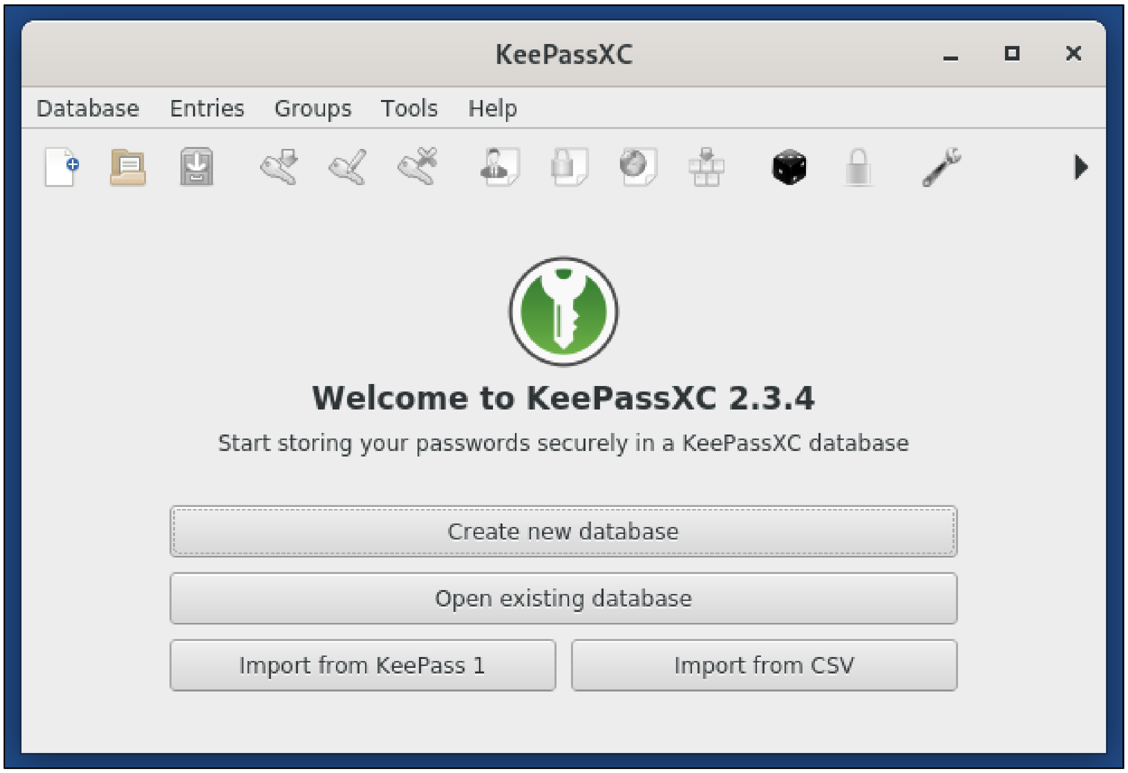
Storing secrets with KeePassXC□

KeePassXC is a password manager that helps you store usernames, passwords and other secrets so that you don’t have to remember them. It comes with a built-in password generator that allows you to use strong and unique passwords for all your accounts, leading to a lower risk of your accounts getting compromised (by hackers or law enforcement). Your secrets are stored in an encrypted database file that can only be unlocked with a master password, this way you can access all your accounts by remembering a single password.

You should use KeePassXC to store:

- Login details to market accounts and forums
- Cryptocurrency seeds and wallet passwords
- Passwords for your PGP keys

To start the tool on Tails, go to “Applications” -> “Accessories” -> “KeePassXC”.



Welcome to KeePassXC 2.3.4

Start storing your passwords securely in a KeePassXC database

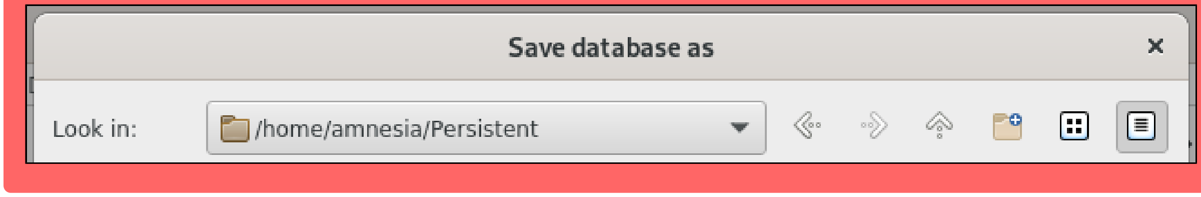
Creating a KeePassXC database□

Tails

Before creating a new database make sure that you have set up and unlocked the persistent volume .

On the welcome screen, click on ‘Create new database’. Alternatively, click on “Database” in the menu bar -> “New database”.

Make sure you save the database on the persistent volume. If you fail to do this your database will be gone when you restart Tails.



Look in: /home/amnesia/Persistent

You will now enter your master password. This is the only password you will need to remember since it will be used to keep all your stored secrets safe. It must not be easy to bruteforce or guessable by an attacker, anyone that can guess your master password has access to ALL secrets in the database.

The best way to create a password that is both strong and memorable is to create a mnemonic . A mnemonic of at least 5 words or more is recommended.

You can use the built-in passphrase generator for inspiration. Click on the 🎲 button in the toolbar. Under the passw field select “Passphrase”. Adjust the word count to the desired length. Then keep pressing “Generate” until you come across one you like. Press “Copy” to copy the passphrase to the clipboard and close the password generation window by pressing the 🎲 button once more.

Think of a story that incorporates all the words in the phrase, this will help you to remember your mnemonic. If you fear you might forget your password you can write it down on a piece of paper and store it in an inconspicous location until you know it by heart.

After entering your password, click “OK”.

You should now restart Tails to make sure that your database is on the persistent volume and that you can still open it.

Whonix

Opening a KeePassXC database□

Tails

If the program isn’t already opened go to “Applications” -> “Accessories” -> “KeePassXC” to start KeePassXC.

Click on “Open existing database”. Then navigate to the directory where you stored your database, and double click on the `.kdbx` file.

Now enter you master password and click “Ok”.

Whonix

Accessing secrets□

Right click on the entry you want to use (e.g. the one named after the market on which you want to login). This will open up a context menu and allow you to copy the username or password to the clipboard.

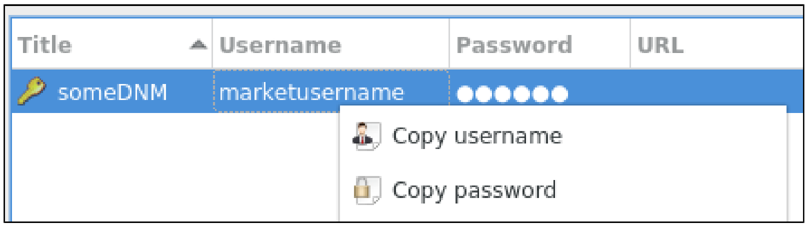
Now all you have to do is go to the market site (e.g. registration page or login page) and paste that password there. Your clipboard will automatically clear after 10 seconds, so be quick.

To access other information stored in the entry, right click on it and then move the cursor over “Copy attribute to clipboard”.

You can also double click on an entry to bring up the editor, but be careful that you don’t accidentally overwrite any important information.

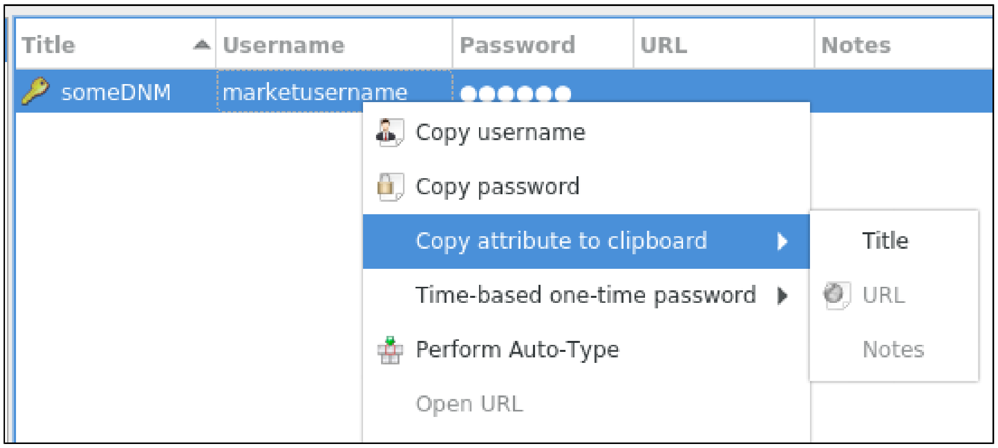
Accessing secrets□

Right click on the entry you want to use (e.g. the one named after the market on which you want to login). This will open up a context menu and allow you to copy the username or password to the clipboard.



Now all you have to do is go to the market site (e.g. registration page or login page) and paste that password there. Your clipboard will automatically clear after 10 seconds, so be quick.

To access other information stored in the entry, right click on it and then move the cursor over “Copy attribute to clipboard”.



> You can also double click on an entry to bring up the editor, but be careful that you don’t accidentally overwrite any important information.

Cryptocurrencies□

Your cryptocoins will be used to pay for your products or services. This part will cover a few different ones that can be used, and the correct paths for using them so that they can not be tied to your identity. When possible you should stick with Monero. Always at the very least convert your bitcoin to monero

> Before we begin it is important that you remember **EVERYTHING** with bitcoin is public on the blockchain. If possible you should ALWAYS start with Monero. If you need to pay your vendor in Bitcoin, or for some reason you started with bitcoin, you can use the converting chapter to keep you safe.

> **Note:** This also cannot be stressed enough. If you start with Bitcoin, or Monero NEVER send your coins directly from an exchange to a vendor or market!!

F.A.Q.□

Is it really necessary to convert my coins to XMR? I don’t want to spend that much in fees.□

YES IT IS NECESSARY! You wouldn’t pay a dealer in front of LE in person. Don’t do it here! Any other form of asking if you need to use XMR will be responded with the same. Yes it is necessary.

If the price of bitcoin/monero 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/monero drops, the item will still be $20, but the bitcoin/monreo equivalent will change. the vendor will only loose money after someone has made a purchase and the price of bitcoin drops.

Do both 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.

Monero (XMR)□

Monero (XMR) is a decentralized cryptocurrency, meaning it is secure digital cash operated by a network of miners operated by users. Transactions are confirmed by distributed consensus and then immutably recorded on the blockchain. Third-parties do not need to be trusted to keep your Monero safe. These coins are much more difficult to trace. This article talks about how eurpol has admitted they cannot be traced.

How to Buy Monero□

Peer-to-peer

Service	Notes
Local Monero	similar to localbitcoins. cash in mail, bank transfer, SEPA, revolut, others
Bisq	decentralized exchange, BTC/XMR pair
OpenBazaar	

Exchanges

Website	KYC	Fiat gateway	Trading pairs	Notes
Kraken	Yes	Yes: USD, EUR	BTC, EUR, USD	SEPA deposits are free
Binance	Yes	Yes*	BTC, ETH, BUSD, USDT	*Binance offers a wide range of fiat deposit options, but does not offer XMR directly for fiat. Purchase one of the available trading pairs with fiat then exchange for XMR.
Tradeogre.com	No	No	BTC	low volume
Anycoindirect	Yes	Yes:EUR		Buy XMR directly with SEPA, creditcard, others

Bitfinex	Yes	Yes: USD	BTC, USD
Bittrex	Yes	No	BTC, ETH, USDT
KuCoin	Yes	No	BTC, ETH, USDT
Poloniex	Yes	No	BTC, USDT

Installing Monero□

Because of the constant changes and updates, we reccomend following our sister Monero Guide which is always kept up to date.

You can find it here: http://xmrguide42y34onq.onion/

It will walk you through everything from different wallets you can install, to how to use them!

Creating Monero Wallets□

Because of the constant changes and updates, we reccomend following our sister Monero Guide which is always kept up to date.

You can find it here: http://xmrguide42y34onq.onion/

It will walk you through everything from different wallets you can install, to how to use them!

Bitcoin (BTC)□

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

Remember if you start with Bitcoin it can easily be traced back to your real identity. If you can’t buy Monero to start you 100% need to convert your coins.

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 bitcoins for your order and the shipping costs. A little extra left over is ok.

How to buy bitcoins□

The best method to buy btc is to not reveal your identity. Unfortunately most major btc exchanges require ID, or ones that will keep you anonymous have very high fees. If you have to use your ID, or are just buying with a card that is attached to your real identity it is okay. We will be covering how to break the chain of custody to your identity by converting to Monero later on.

The best method to buy btc is to not reveal your identity. Unfortunately most major btc exchanges require ID, or ones that will keep you anonymous have very high fees. If you have to use your ID, or are just buying with a card that is attached to your real identity it is okay. We will be covering how to break the chain of custody to your identity by converting to Monero later on.It is your choice to pick the 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 on converting later on.

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 for creating an account at 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. 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. Some of the most often used and more anonymous payment methods are:

- 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. Be aware of the risks of sending large amounts of cash through the mail.

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.

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:

```
• 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. 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 ” 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

Tumbling is a service that has worked well in the past. With the rise of the darknet, tumbling has become more of an outdated service. Many tumblers risk your opsec, or just scam you of your coins. Tumbling your coins is still better than not tumbling them but we will cover better methods later.

Setting up your wallet (BTC)□

Note: 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 Electrum 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?[/] “Standard Wallet”[i]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 loose your password or when 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 /d/darknetmarketsnoobsElectrum not starting any more?First make sure you still have your seed for that wallet and that you can still access it even if your Tails USB stick would break completely.Then right click on desktop, open terminal, and type in electrumand press ENTER. See if it loads. If it does not load 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).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 can happen 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 Bitcoin□

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.

The general the path you should send your bitcoins is: Bitcoin exchange ->BTC Wallet1-> convert to XMR->XMR Wallet -> DNM IF your vendor does not accept XMR you can convert back to Bitcoin. More on that later in the converting section.

Note: That normal wallet and the Electrum wallet on Tails have to be different wallets. So you need to do the setup process described previously twice: once for your normal wallet and once for your Electrum wallet on Tails.

This process is to break the chain of custody to you, and add plausible deniablity. Once converted to XMR it cannot be traced anymore. If you were to be questioned about converting you can just say you sent them for consulting, or simply say you no longer have access to the wallet.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 send 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 ” 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

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) 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 /d/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.

FAQ□

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.

Converting□

Converting in an important step you should always use to help keep coins from coming back to your real identity. As stated before you should always try to stick with XMR when possible. However some vendors or services do not accept XMR, in the case you can safely convert back to bitcoin and be on your way. For some it is just easier to buy bitcoin from an exchange with your real identity. We can break the chain so that these coins are no longer linked to your identity.

In this guide we are going to talk about using Elude, and morphscript. A list of other Exchangers is below.

If this is your first time converting, or you are not very comfortable changing coins in terminal you should stick to using Elude. Elude is a darknet service that is very active on dread. If you have any issues or questions you can easily get in touch with them on their subdread /d/Elude

After you convert a few times you may want to try out using morphscript. Morphscript uses Morphtoken API. Supports conversion between BTC, ETH, BCH, LTC, DASH and XMR. Meaning you can do it all in one place, you can also check the current fees to find which is the cheapest option for you.

Changers□

Here is a list of some other changers you can try out!

Website	JS Required?	Hidden service?	Support	Notes
XMR.to	No	No	support@xmr.to	only XMR -> BTC, instant conversion up to 0.1 BTC
Morphtoken	Yes*	No	contact@morphtoken.com	*can be used without JS with morphscript. Supports BTC, ETH, BCH, LTC, DASH and XMR

Godex	Yes*	No	support@godex.io	*can be used without JS with godex.py
Elude	No	Yes	contact@elude.in or /u/Elude	not a caution: not a registered business
Xchange	No	Yes	support@xchange.me	
Kilos	No	Yes	ugu@firemail.cc , read this	XMR/BTC exchange. caution: not a registered business
Uplink	No	Yes	see this	XMR/BTC exchange. caution: not a registered business
flyp	Yes	No	support@flyp.me	

Bitcoin to Monero

Everything with Bitcoin can be viewed on the blockchain. If you started with Bitcoin that could be tied to your identity, or you want to convert your Bitcoin to Monero (recommended) start here.

How you bought your coins does not matter when you follow this path to break the chain to your identity:For our example here we are going to use Elude. A list of of other exchanges can be found on /d/Monero Once you have done converting a few times you might want to try using Morphscript. More info on Morphscript can be found on /d/Monero

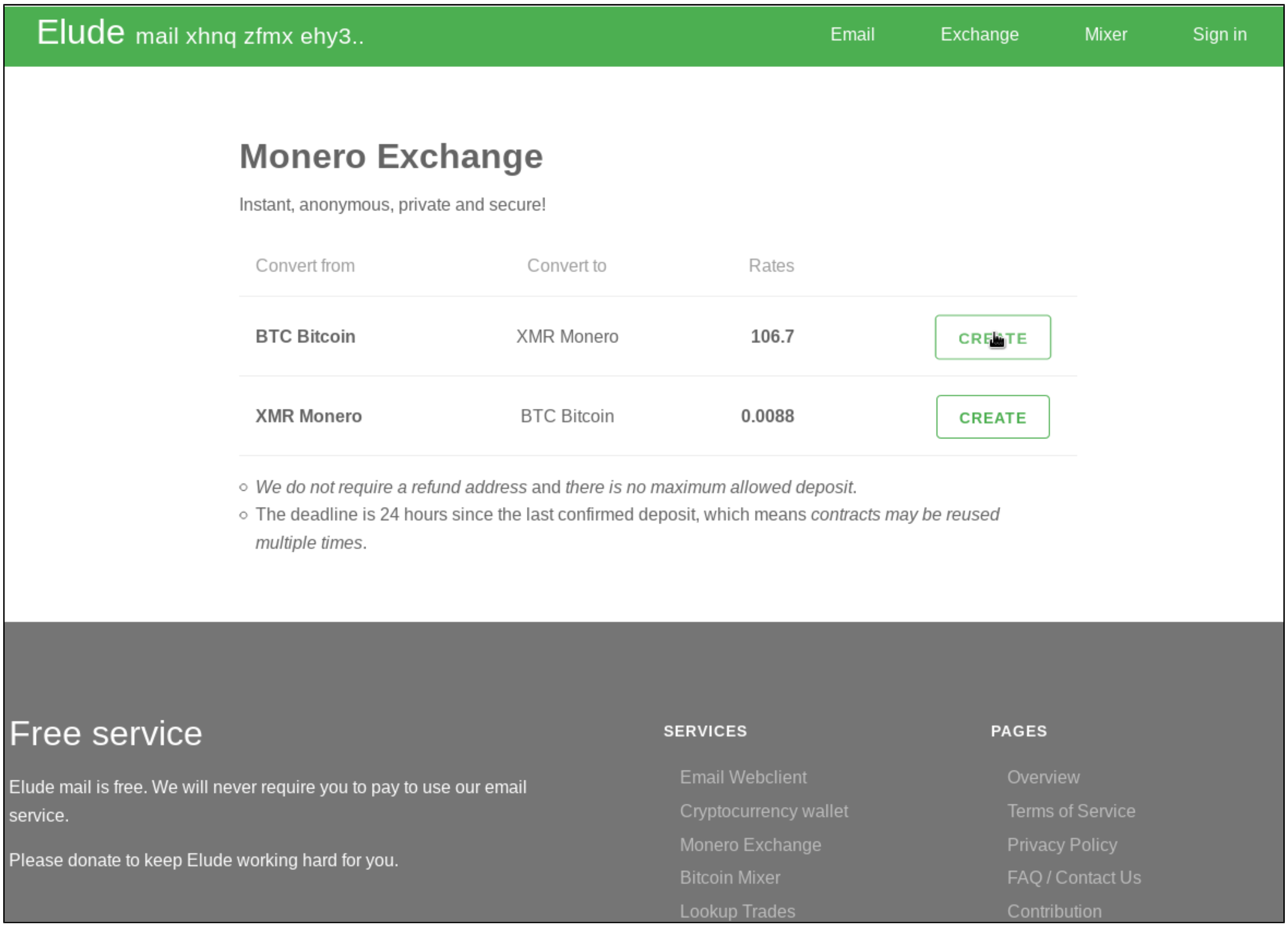
Elude

Elude

- Send your coins from your exchange to your private wallet.

NOTE: Always keep “clean” coins in this wallet. This wallet should NEVER send coins directly to a market as it could be linked to you.

- Go to http://eludemaillhqfkh5.onion/exchange
- Click Exchange bitcoin to XMR.



Monero Exchange

Instant, anonymous, private and secure!

Convert from	Convert to	Rates	
BTC Bitcoin	XMR Monero	**106.7**	CREATE
XMR Monero	BTC Bitcoin	**0.0088**	CREATE

- *We do not require a refund address* and *there is no maximum allowed deposit*.
- The deadline is 24 hours since the last confirmed deposit, which means *contracts may be reused multiple times*.

Free service

Elude mail is free. We will never require you to pay to use our email service.

Please donate to keep Elude working hard for you.

- Enter the address that you would like your XMR coins to be sent to.
- Send your bitcoin to the address shown.
- Click check status of transfers, and make a note of the exchange status key.
- Wait for your XMR to arrive.This is the path your coins just took: Exchange-> BTCWallet1-> Elude-> XMR wallet.

Morphscript

Monero to Bitcoin□

Some vendors, or services do not accept Monero.If this is the case you will need to convert your coins to Bitcoin. Again once you have converted a few times you might want to try Morphscript to convert. More about Morphscript can be found on /d/Monero .□

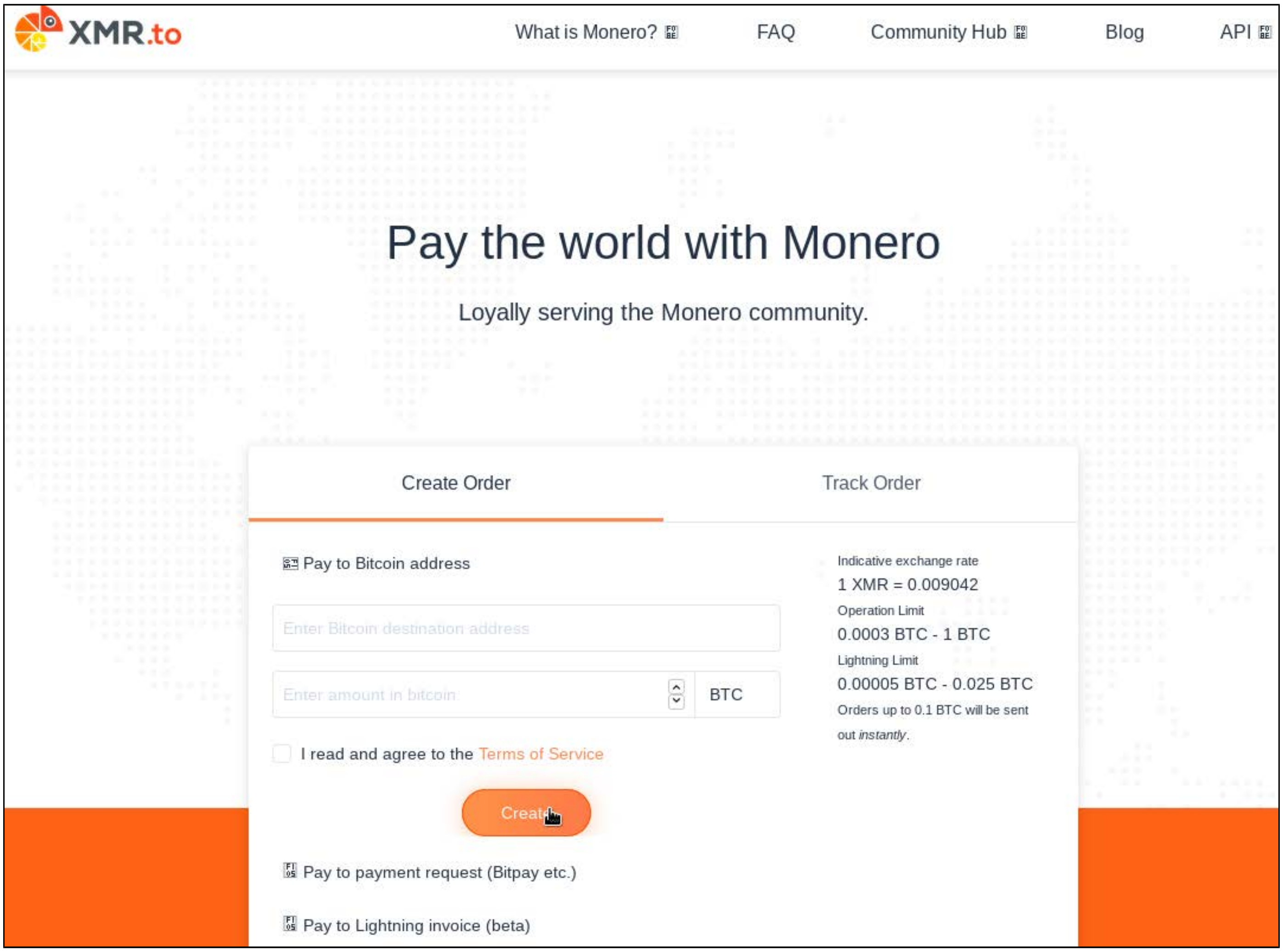
You can use other services, but the most common one used is XMR.to

XMR.TO

- Go to XMR.to on Tor. If you get a message saying this is service is not available in your country, click the menu button in your Tor Browser, then establish new Tor circuit to this site.
- Enter the address you want to receive your bitcoin at.

NOTE: Make sure this wallet is not your normal wallet that can be linked to you. This wallet will be used to send bitcoin to a market making it labeled “hot”

- Enter in the amount you want to receive.
- Click Create order



Pay the world with Monero

Loyally serving the Monero community.

☐ I read and agree to the Terms of Service

Indicative exchange rate
1 XMR = 0.009042
Operation Limit
0.0003 BTC - 1 BTC
Lightning Limit
0.00005 BTC - 0.025 BTC
Orders up to 0.1 BTC will be sent out *instantly*.

- You should now see a page with the total amount you must send to receive your bitcoin. Make a note of the secret key. This will allow you to check your order if you have any issues.
- Send the required amount of XMR to the address they provided.
- Wait for your bitcoin to arrive. Most of the time it should arrive fairly quickly.
- Use your bitcoin to pay for your goods.

Morphscript

Crypto Closing Words□

In short this is the path you will follow. XMR Wallet->XMR.to->Bitcoin wallet->Market

Note: After you convert make sure you use a new wallet that has not ever been tied to your identity. Wallets that send coins to markets can be labeled as “hot” you don’t want the two wallets to ever interact.

If you started with Bitcoin, and need to pay in bitcoin here is an example of the path you follow: BTC Exchange-> BTC Wallet 1 -> Convert to XMR -> XMR Wallet-> Pay for your goods. OR-> convert back to BTC-> BTC Wallet 2-> pay for your goods.

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 and files and to increase the security of email communications.

A typical darknet user will use PGP to:

Encrypt messages□

- To encrypt the shipping address and other sensitive information so only the vendor can read it.

Decrypt messages□

- Vendors will encrypt sensitive shipping information for you (e.g. tracking codes).
- Decrypting a message is sometimes required to login to a market.

Verify messages□

- To verify that a market link is legit and not a phishing site.

Learning how to use PGP is very important. You don’t ever want your personal details to fall into the hands of law enforcement. Please carefully read through all sections in this chapter. If you want to make sure that you can properly encrypt and decrypt messages with PGP please go to /d/PGPPractice .□

FAQ□

What if I sent a message without PGP?□

Did you sent a message that 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.

Can I use the market’s built in encryption?□

No. The server processes the message in plain text, if the market is compromised attackers will be able to see the contents. Always encrypt sensitive information 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. 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□

When you create a PGP key pair, it gives you two unique keys: a public key, and a private key. You are to not, at any times, or for any reason, to 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.

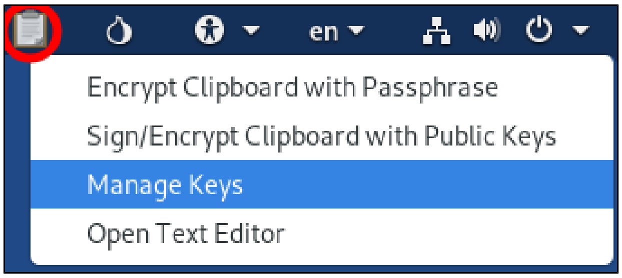
When you sign up to a market you may be asked to enter a public key. To prevent your market accounts from being linked together, **you should always generate a new key pair for every account you make**. Never upload the same public key to multiple accounts.

By uploading your public key you allow your vendor to securely send you sensitive information about your shipment (e.g. tracking codes). It can also serve as a two factor authentication mechanism to login to a market: every time you login you are required to decrypt a message containing a special code. Entering this special code proves that you own the account, because only you would be able to decrypt the message.

You should not keep private keys around that are no longer in use. If you make a new account on a market, delete the old key. If a markets gets busted or exit scams delete all keys for the accounts you created on that market. In the event that your private keys are compromised you want an attacker to be able to decrypt as little sensitive information as possible.

Tails

Click on the clipboard icon on task bar at the top of your screen and select the option “Manage Keys”.


en
Encrypt Clipboard with Passphrase
Sign/Encrypt Clipboard with Public Keys
Manage Keys
Open Text Editor

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 name because everybody that has your public key later can see that name. Never use a name that can be linked to your real identity.

If you’re making a new key to sign up to a market it is best to fill in your market username, this will make it easier for your vendor to encrypt messages for you.

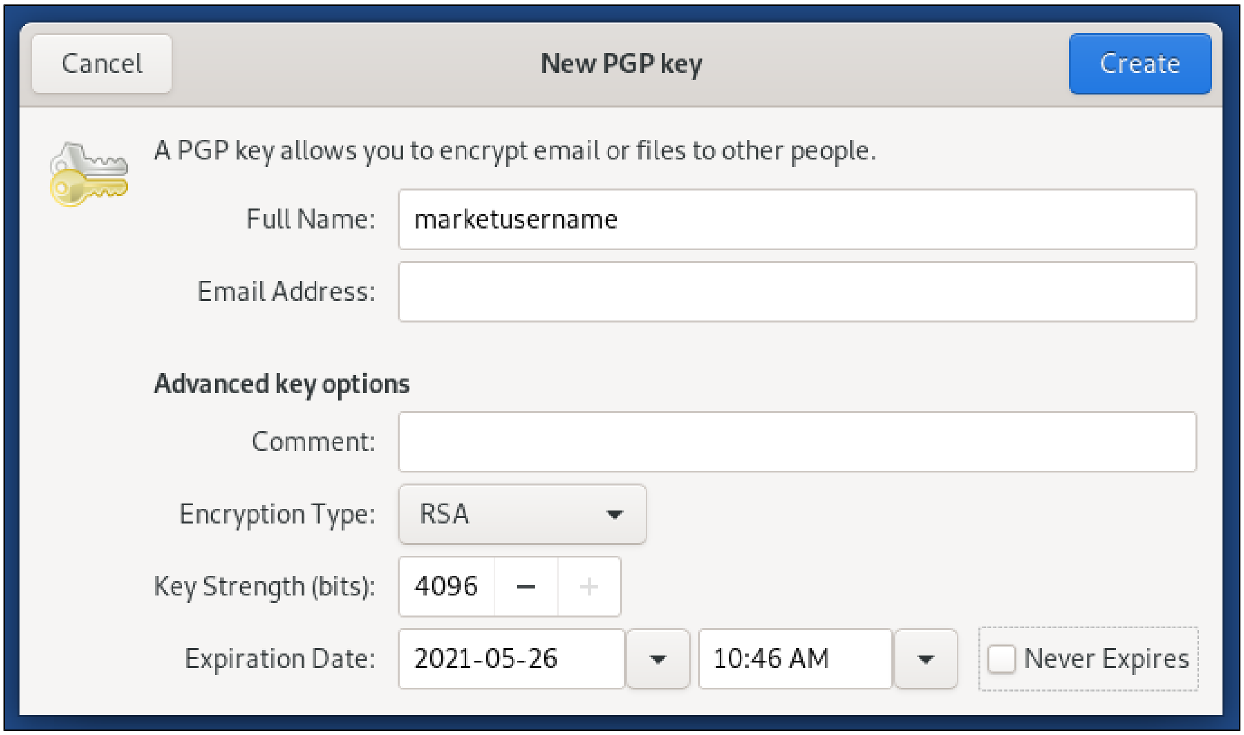
It is recommended to leave the email field blank. If you want to be contacted via email you can add one, but please make sure that it fulfills the recommendations mentioned in the email chapter .

Under “Advanced key options”, set the “Key Strength (bits)” to 4096 and the “Expiration Date” to one or two years in the future.

> **Note**: Setting an expiration date does not prevent messages that were encrypted with the associated public key from being decrypted in the future. In other words, if your private key is ever compromised an attacker can still decrypt messages after the key is expired.
>
> The expiration date only serves as a reminder to periodically rotate your key pair, to limit the amount of sensitive

information that can be decrypted with a single private key. When you do this be sure to let others know you are changing your key by signing your new public key with your old key.

Rotating a key only applies to keys that were created for off-market use. For example, a public key that you add to your profile on Dread. Keys created for market accounts are generally short-lived and should not be kept around for long.



A PGP key allows you to encrypt email or files to other people.

Full Name: marketusername

Email Address:

Advanced key options

Comment:

Encryption Type: RSA

Key Strength (bits): 4096

Expiration Date: 2021-05-26 10:46 AM

□ Never Expires

Confirm the data by clicking on “Create”. You will 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 KeePassXC.

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 have 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-----

mQINBFhNDOsBEACzwJJVsMo7sIiLhvCsLx2n+DVHzw1trM/C8Yao8EmWdDYe3ei9
mXRqSudbD6S4KvJfm+ZeOlEQ6gGoG2q3aFYASRgcK7WDhs+jwG42Ey+j2oIpU/EO
8EQXTmTn8T+LQT84JZ5KkiZZp2CqLU8RVszfkKEj1oX/sO5watxNQur4fbk9FiCA
1MjHMYir1g==
=TV04
-----END PGP PUBLIC KEY BLOCK-----
```

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

Whonix

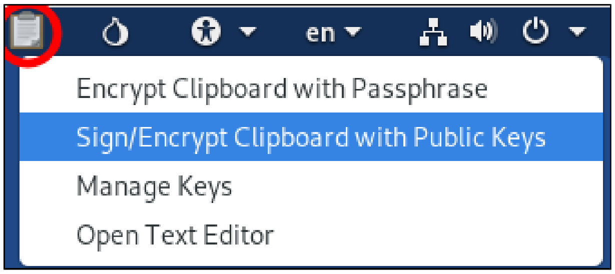
Encrypting a message with PGP□

You must always encrypt sensitive information yourself. Never trust a market to do it for you.

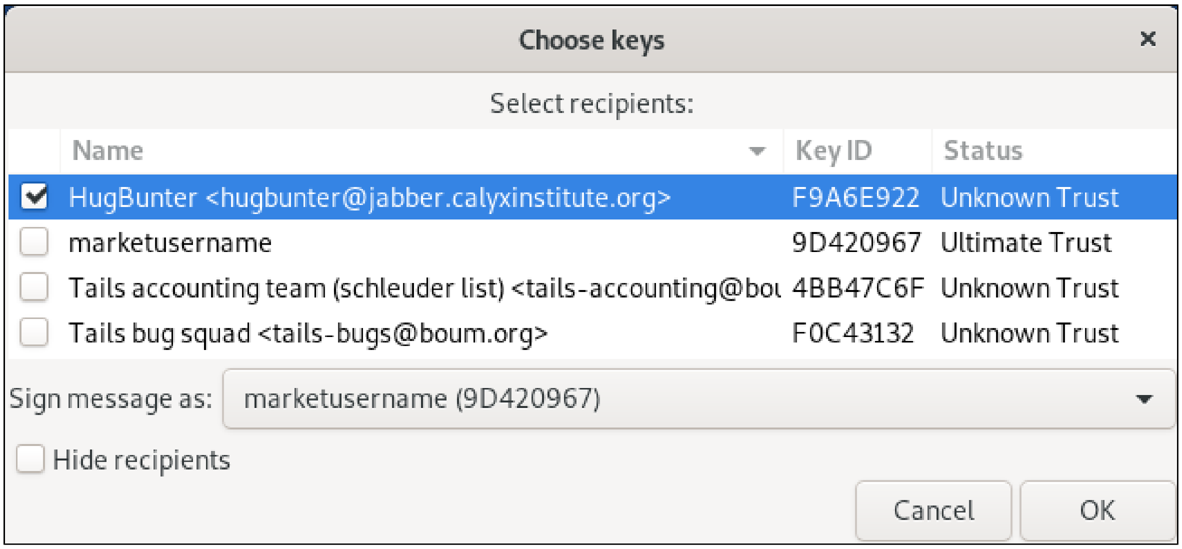
Tails

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 the text editor. 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”.


en
Encrypt Clipboard with Passphrase
Sign/Encrypt Clipboard with Public Keys
Manage Keys
Open Text Editor

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.



Select recipients:

	Name	Key ID	Status
☑	HugBunter <hugbunter@jabber.calyxinstitute.org>	F9A6E922	Unknown Trust
□	marketusername	9D420967	Ultimate Trust
□	Tails accounting team (schleuder list) <tails-accounting@bou	4BB47C6F	Unknown Trust
□	Tails bug squad <tails-bugs@boum.org>	F0C43132	Unknown Trust

Sign message as: marketusername (9D420967)

□ Hide recipients

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, it is encrypted properly.

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

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

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

Note: After your message is encrypted you will not be able to decrypt it. Only the selected recipient will be able to do it. It is possible to select multiple recipients, so if you want to be able to decrypt your message you must also select your own key.

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

Verifying a message with PGP□

Verifying messages is commonly used to check the authenticity of market links. Markets publish signed messages containing links to their market. If you have the market's public key you can use it to verify that the message was created by the market and that the links are legimate.

Markets, vendors and moderators will sometimes sign announcements or warnings. You can also use this to verify those.

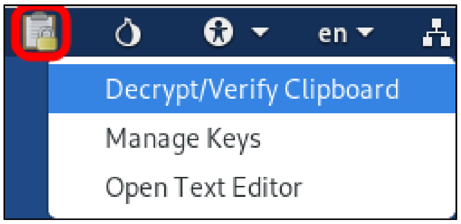
Tails

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, or on the market's subdread) and then import it.

Copy the PGP signed message, it looks something like this:

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

Here are our onion links:

ar3a3uxsmdjvlv3o.onion
effma5umlll2bxmd.onion
xw7w4apecxzw4t7h.onion

- SomeDarknetMarket

-----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".



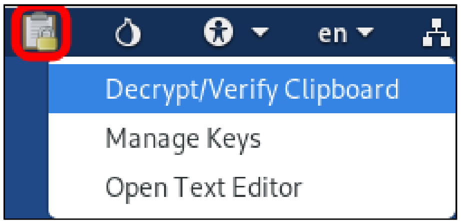
A new window should pop up which contains “Good signature from ” at the bottom, if the signature was correct.

Whonix

Decrypting a message□

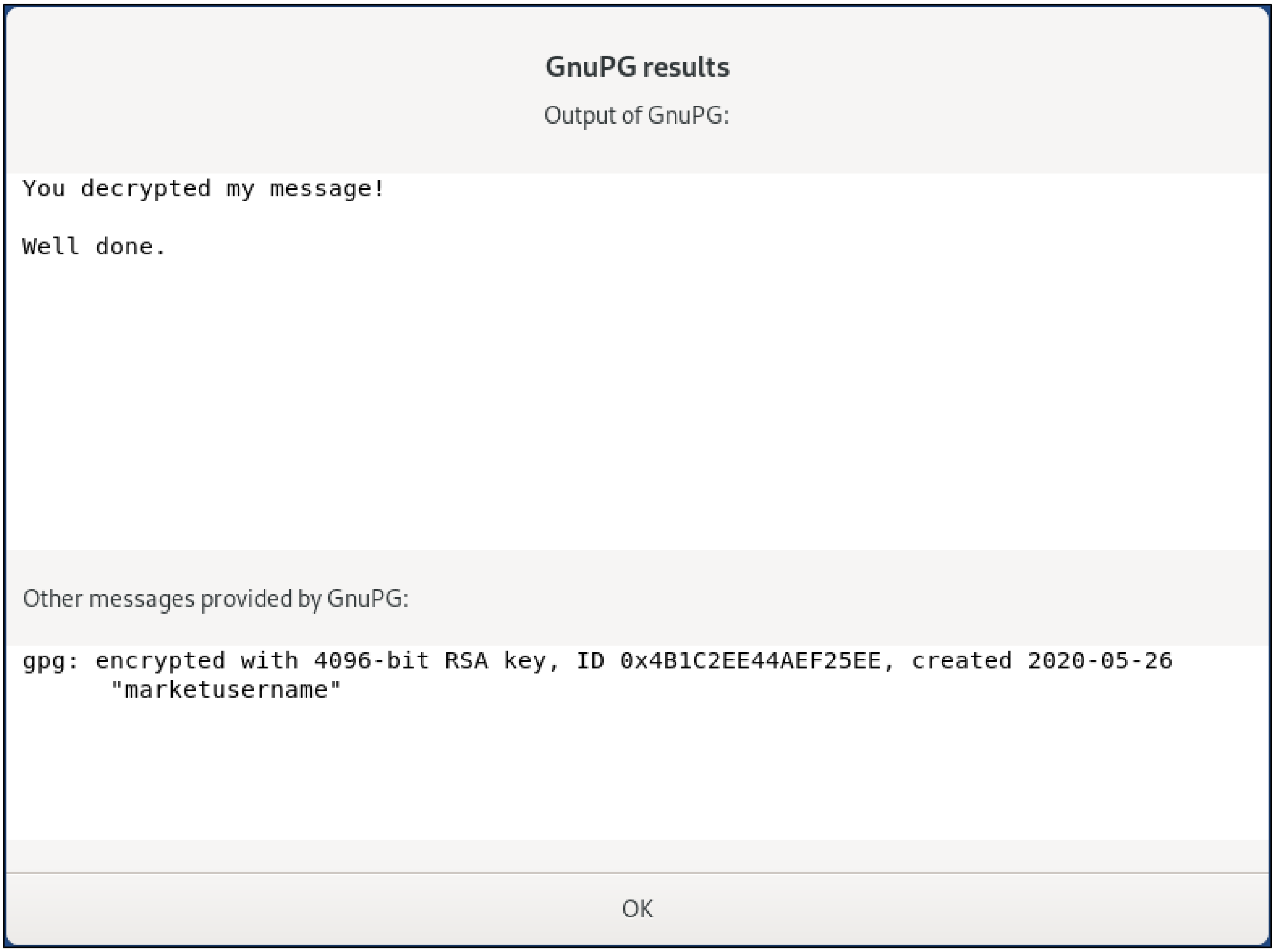
Tails

First copy the encrypted message. Then click on the clipboard icon and select “Decrypt/Verify Clipboard”.



Enter the password for your key if requested.

A window will show up the decrypted message:



```
You decrypted my message!

Well done.
```

```
gpg: encrypted with 4096-bit RSA key, ID 0x4B1C2EE44AEF25EE, created 2020-05-26
      "marketusername"
```

Whonix

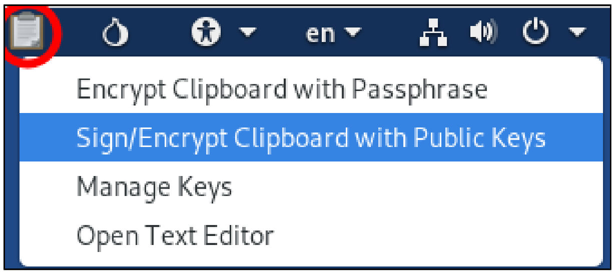
Signing a message with PGP

This is not for encrypting your address or other private messages.

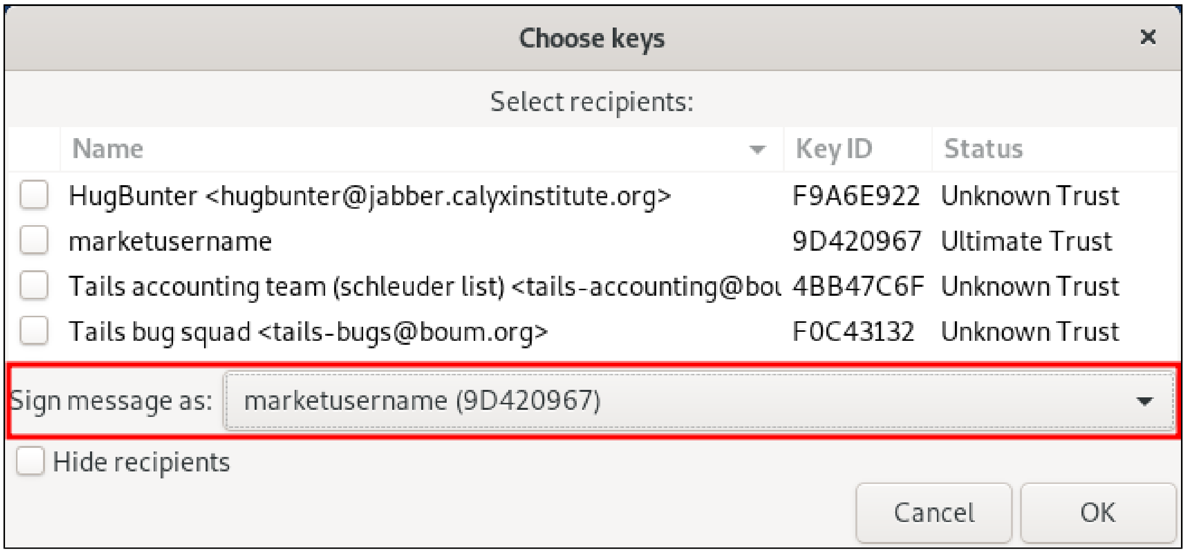
You can sign a message to prove that you created it. Anyone that has your public key can verify that you signed it. It is usually not necessary to sign messages as a normal DNM buyer but if you need to do it, here is how.

Tails

Type the message in the text editor. 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”.


en
Encrypt Clipboard with Passphrase
Sign/Encrypt Clipboard with Public Keys
Manage Keys
Open Text Editor

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.



Select recipients:

	Name	Key ID	Status
□	HugBunter <hugbunter@jabber.calyxinstitute.org>	F9A6E922	Unknown Trust
□	marketusername	9D420967	Ultimate Trust
□	Tails accounting team (schleuder list) <tails-accounting@bou	4BB47C6F	Unknown Trust
□	Tails bug squad <tails-bugs@boum.org>	F0C43132	Unknown Trust

Sign message as: marketusername (9D420967)

□ Hide recipients

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, it is signed properly.

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

This is my signed message.

Anyone with my public key can verify that I signed it.
-----BEGIN PGP SIGNATURE-----

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

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”.

Whonix

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.

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?

If you are in the US you can sign up for informed delivery. You can check that for all packages coming to you but you don't need to have the tracking number. You still retain plausible deniability because it is a service the USPS wants you to use and they give you the information without you ever asking for it.

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.

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”.

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.

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 (Yes on reddit) to make sure that you don’t only have drugs coming to it though.

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 T00NSomeone 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.

Once you get one of these love letters, consider that address burnt. Do not use it again as a delivery address for contraband. 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.

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.

Resources□

Take some time to read though some of these resources. You can learn about just about any drug, the science behind them, get questions from real experts. Or if you just need someone to help you through a bad trip. All of it can be found on here.

Doses and recovery position□

If this is your first time trying a new drug, or if you don’t have a tolerance anymore. Take some time to read about correct doses from Erowind , and PsychonautWiki .

Also take some time to make sure you are familiar with the “Recovery Position” this could help save a life in the future. It will only take you a minute to look over. Here

PsychonautWiki

http://psychonaut3z5aoz.onion/

PsychonautWiki is a community-driven online encyclopedia that aims to document the emerging field of psychonautics in a comprehensive, scientifically-grounded manner. Our primary motivations include:

- documenting all aspects of psychonautic theory and practice (including meditation, lucid dreaming, psychoactive substance use, sensory deprivation, ritual, etc.) from an evidence-based, academic perspective

- providing accessible education, encouraging safe practices, and reforming cultural taboos around the responsible use of psychoactive substances, using both expert and crowd-sourcing methods
- promoting a culture of free thought and personal autonomy by safeguarding the information needed to make informed decisions over altering one's body and consciousness

Erowid

https://www.erowid.org

Erowid is a member-supported organization providing access to reliable, non-judgmental information about psychoactive plants, chemicals, and related issues. We work with academic, medical, and experiential experts to develop and publish new resources, as well as to improve and increase access to already existing resources. We also strive to ensure that these resources are maintained and preserved as a historical record for the future.

National Harm Reduction Coalition

https://harmreduction.org/

Our work is to uplift the voices and experiences of people who use drugs and bring harm reduction strategies to scale. For more than 25 years, we've worked with communities to create, sustain, and expand evidence-based harm reduction programs and policies.

They help make sure people can stay safe by finding sterile syringes, Naloxone distribution, and fentanyl testing. Check them out!

DNM Avengers

http://avengersdutyk3xf.onion

DNMAvengers is a substance oriented forum dedicated to harm reduction via discussion & the testing of substances bought on Crypto-Markets

Tripsit

https://tripsit.me/

Our mission is to provide open discussion of harm reduction techniques and positive support. We promote the use of harm reduction tools such as test kits, and offer guidance and support with regards to harm reduction when using drugs. We encourage discussion of scientific, medical, philosophical understandings, and many of us can provide advice based on life experiences, an invaluable asset for someone who may be experiencing a similar issue. We are eager, willing, and prepared to guide or 'tripsit' users who may be having a hard time while under the influence of drugs.Our network is comprised of an IRC chat team dedicated to 24/7 live support from quick information to a friendly guide through difficult experience. We also offer a drug-information wiki for those seeking quick information and a live radio service for those seeking musical company.

DanceSafe

https://www.dancesafe.org/

DanceSafe is a 501(c)(3) public health organization promoting health and safety within the nightlife and electronic music community. Founded in the San Francisco Bay Area in 1998 by Emanuel Sferios, DanceSafe quickly grew into a national organization with chapters in cities across North America.Our Initiatives and Services

- Provide safe spaces to engage in conversations about health, drug use, and personal safety;
- Provide free water and electrolytes to prevent dehydration and heatstroke;
- Provide free safe sex tools to avoid unwanted pregnancies and the spread of STIs;
- Provide free ear plugs to prevent hearing loss;
- Provide honest, fact-based, unbiased information on drug effects and potential harms to empower users to make informed decisions;
- Offer a nonjudgmental first-point of contact to risky or challenging situations;
- Offer drug checking services to prevent overdose and death; and
- Work with promoters and local stakeholders to advocate for safety first approaches.

Drugs and Me

https://drugsand.me/en/

Drugs and Me provides accessible, objective and comprehensive educational material to help reduce the short and long term harms of drugs.We are a group of scientists, educators and analysts with extensive experience in drug education. We wanted to do something to stop the increasing number of accidents and deaths that occur in the world due to lack of drug education.

DrugWise

https://www.drugwise.org.uk/

As well as updating our drug information and writing new reports, we provide a full range of DrugScope archival materials and all Druglink articles back to 1986.

DrugWise also has an international dimension which is not restricted to drugs, but includes alcohol and tobacco where the advent of e-cigarettes is causing as much controversy as that surrounding the conflicting views on drug policy and practice.

There are many robust international and internationally-relevant national reports and reviews in all these areas. The problem is that they are not all in one place. So we have created I-Know, the international knowledge hub which will build up a library of information, policy and practice material stored on our server so that they will always be available.

Resources□

Take some time to read though some of these resources. You can learn about just about any drug, the science behind them, get questions from real experts. Or if you just need someone to help you through a bad trip. All of it can be found on here.

Doses and recovery position□

If this is your first time trying a new drug, or if you don’t have a tolerance anymore. Take some time to read about correct doses from Erowind , and PsychonautWiki .

Also take some time to make sure you are familiar with the “Recovery Position” this could help save a life in the future. It will only take you a minute to look over. Here

PsychonautWiki

http://psychonaut3z5aoz.onion/

PsychonautWiki is a community-driven online encyclopedia that aims to document the emerging field of psychonautics in a comprehensive, scientifically-grounded manner. Our primary motivations include:

- documenting all aspects of psychonautic theory and practice (including meditation, lucid dreaming, psychoactive substance use, sensory deprivation, ritual, etc.) from an evidence-based, academic perspective
- providing accessible education, encouraging safe practices, and reforming cultural taboos around the responsible use of psychoactive substances, using both expert and crowd-sourcing methods
- promoting a culture of free thought and personal autonomy by safeguarding the information needed to make informed decisions over altering one’s body and consciousness

Erowid

https://www.erowid.org

Erowid is a member-supported organization providing access to reliable, non-judgmental information about psychoactive plants, chemicals, and related issues. We work with academic, medical, and experiential experts to develop and publish new resources, as well as to improve and increase access to already existing resources. We also strive to ensure that these resources are maintained and preserved as a historical record for the future.

National Harm Reduction Coalition

https://harmreduction.org/

Our work is to uplift the voices and experiences of people who use drugs and bring harm reduction strategies to scale. For more than 25 years, we’ve worked with communities to create, sustain, and expand evidence-based harm reduction programs and policies.

They help make sure people can stay safe by finding sterile syringes, Naloxone distribution, and fentanyl testing. Check them out!

DNM Avengers

http://avengersdutyk3xf.onion

DNMAvengers is a substance oriented forum dedicated to harm reduction via discussion & the testing of substances bought on Crypto-Markets

Tripsit

https://tripsit.me/

Our mission is to provide open discussion of harm reduction techniques and positive support. We promote the use of harm reduction tools such as test kits, and offer guidance and support with regards to harm reduction when using drugs. We encourage discussion of scientific, medical, philosophical understandings, and many of us can provide advice based on life experiences, an invaluable asset for someone who may be experiencing a similar issue. We are eager, willing, and prepared to guide or 'tripsit' users who may be having a hard time while under the influence of drugs.Our network is comprised of an IRC chat team dedicated to 24/7 live support from quick information to a friendly guide through difficult experience. We also offer a drug-information wiki for those seeking quick information and a live radio service for those seeking musical company.

DanceSafe

https://www.dancesafe.org/

DanceSafe is a 501(c)(3) public health organization promoting health and safety within the nightlife and electronic music community. Founded in the San Francisco Bay Area in 1998 by Emanuel Sferios, DanceSafe quickly grew into a national organization with chapters in cities across North America.Our Initiatives and Services

- Provide safe spaces to engage in conversations about health, drug use, and personal safety;
- Provide free water and electrolytes to prevent dehydration and heatstroke;
- Provide free safe sex tools to avoid unwanted pregnancies and the spread of STIs;
- Provide free ear plugs to prevent hearing loss;
- Provide honest, fact-based, unbiased information on drug effects and potential harms to empower users to make informed decisions;
- Offer a nonjudgmental first-point of contact to risky or challenging situations;
- Offer drug checking services to prevent overdose and death; and
- Work with promoters and local stakeholders to advocate for safety first approaches.

Drugs and Me

https://drugsand.me/en/

Drugs and Me provides accessible, objective and comprehensive educational material to help reduce the short and long term harms of drugs.We are a group of scientists, educators and analysts with extensive experience in drug education. We wanted to do something to stop the increasing number of accidents and deaths that occur in the world due to lack of drug education.

DrugWise

https://www.drugwise.org.uk/

As well as updating our drug information and writing new reports, we provide a full range of DrugScope archival materials and all Druglink articles back to 1986.

DrugWise also has an international dimension which is not restricted to drugs, but includes alcohol and tobacco where the advent of e-cigarettes is causing as much controversy as that surrounding the conflicting views on drug policy and practice.

There are many robust international and internationally-relevant national reports and reviews in all these areas. The problem is that they are not all in one place. So we have created I-Know, the international knowledge hub which will build up a library of information, policy and practice material stored on our server so that they will always be available.

Labs□

On this page you can find some labs and drug test results. Want to know the exact breakdown of what's in your goodies? Then this is the resource for you.

If you're buying bulk, or planning to resell please especially take the time to get a lab test done so you don't go accidentally killing someone!

Energy Control International

https://energycontrol-international.org/

We are a group of like minded people regardless of whether we are drug users or not, concerned about the problems related to drug use in recreational settings and in society. We develop Harm Reduction strategies, offer information, personal advice and education regarding drugs in order to diminish risk and harm related to their use.

We offer a Drug Checking Service in order to inform the users about the composition of the drugs and therefore are in a position to advise them on less risky taking of said substance. We also offer customized, non-moralistic, and scientific drug information directed at drug users. The Drug Checking Service started operating in Spain from 1999 and since 2014 it is also offered as an International Drug Testing Service.

You can find reports from our International Drug Testing Service and links to our most relevant peer-reviewed scientific articles, interventions in international congresses and other scientific forums, and conference posters.

DrugData

https://www.drugsdata.org/

DrugsData (formerly EcstasyData) is the independent anonymous laboratory drug testing program of Erowid Center. Its purpose is to collect, review, manage, and publish laboratory testing results from our lab and republished from other analysis projects worldwide.

Wedinos https://wedinos.org/

Information from a range of sources in the UK and Europe indicate that some users of new psychoactive substances (NPS) are at risk of a number of serious adverse effects. Principally these include the direct or acute physical, psychological and behavioural effects following use, as well as the potential for increased engagement with criminal justice services. Longer term, or chronic effects are, in the main, poorly evidenced. This project is designed to inform both.

Get Your Drugs Tested

https://getyourdrugstested.com/ (Canada)

We will test your street drugs and tell you what's in them!GET YOUR DRUGS TESTED is the world's largest repository of street drug analysis results. We are a community service offered entirely funded and operated by the Medicinal Cannabis Dispensary. We are certified by Vancouver Coastal Health as an Overdose Prevention Site but we receive no government funding and are independently run.

HOW THE TESTING WORKS

We have a special machine called an "FTIR Spectrometer" which can identify drug samples and tell us what they are.

The test takes less than five minutes and does not destroy the sample. The machine shines an infrared laser onto the sample, then analyzes the reflected light spectrum to identify the substances in the sample.

We also have test strips available, more specifically to test for even trace amounts of fentanyl or benzodiazepines.

We are currently offering drug testing nationwide through the mail, and in Vancouver samples can be dropped off for testing at 880 East Hastings during operating hours.

Vancouver Coastal Health

http://www.vch.ca/ (Canada)

We provide a wide variety of free and confidential harm reduction services to our clients. Harm reduction services provide supplies for safer drug injection (needles), safer smoking (mouthpieces, push sticks) and safer sex (condoms). VCH harm reduction services are a part of a comprehensive public health and addictions program that includes both prevention and treatment. The goal of harm reduction programs is to keep individuals and communities safe and healthy by preventing infections, illness and injury related to drug use and sexual practices.What harm reduction services are offered?

- Education on safer drug use and safer sex, as well as referrals to health services, addictions services and other supports
- Education and access to testing and treatment for communicable diseases as well as referrals to counseling services
- Needle exchange services to promote safe recovery and disposal of used needles
- Supervised consumption sites
- Overdose prevention and response services
- Cannabis (marijuana)
- Referrals for clients seeking drug detox, treatment or counseling

Drug Foundation https://www.drugfoundation.org.nz/ (New Zealand)

We offer tools and advice for people who use drugs, their whānau and people who care about them, and for communities impacted by alcohol and other drug use. Let’s work together to eliminate all drug harm in Aotearoa New Zealand.

Our current harm reduction services include Did You Know for parents; Living Sober; PotHelp; DrugHelp; Drugs in Bars; expanding access to free drug checking; an Acute Drug Harm Community of Practice for services and professionals; working with agencies to establish a drugs early warning system; helping employers reduce workplace impairment risks which includes projects with the NZ Defence Force and Maritime NZ; partnering with ready-for-work programmes; and improving how schools respond to drug use issues.

Suicide Hotlines□

We all have shitty times in our lives. If you are in need of real help, or just need someone to talk to, please try calling one of these numbers.

This list is from https://www.reddit.com/r/SuicideWatch/wiki/hotlines

Argentina□

Centro de Asistencia al Suicida: https://www.casbuenosaires.com.ar/ayuda 135 (CABA & GBA), (011)5275-1135 (Todo El País/Nationwide)

Australia□

13 11 14□https://www.lifeline.org.au/crisis-chat/

Austria□

142, Youth 147 Online: http://www.onlineberatung-telefonseelsorge.at

Belgium□

Dutch: 1813 https://www.zelfmoord1813.be/ French: 0800 32 123 http://www.preventionsuicide.be/fr/lesuicide.html

Brasil□

141Chat, Skype and Email also available at: https://www.cvv.org.br/

Canada□

National Crisis Line from Crisis Services Canada (Pilot Project, phone only at present): 1.833.456.4566Other Crisis Lines by Region Alternatively, 211 works in most of Canada, and they can advise regarding local resources.Nationwide Kids Help Phone (Up to age 18): 1.800.668.6868 or text HOME to 686868

Deutschland□

http://www.telefonseelsorge.de/ Tel: 0800-1110111 oder 0800-1110222Chat: https://chat.telefonseelsorge.org/index.php

Denmark□

70 20 12 01□www.livslinien.dk

Fiji□

Lifeline Fiji: 132454

Finland (Suomi)□

Kriisipuhelin 09 2525 0111 (suomeksi, 24/7)Kristelefon 09 2525 0112 (på svenska)Crisis Helpline 09 2525 0113 (in English and Arabic) / خط مساعدة الأزمات (باللغة العربية)

France□

Suicide Écoute - http://www.suicide-ecoute.fr/ 01 45 39 40 00sos-amitie - réseau de 50 postes d'écoute Téléphone: Numéros divers, carte iciChat: Disponible de 13h à 3h, 7 jours ici

Greece□

1018 or 801 801 99 99Greece - http://www.suicide-help.gr/

Iceland□

1717

India□

91-44-2464005 0022-27546669

Iran□

1480 6am to 9pm everyday

Ireland□

ROI - local rate: 1850 60 90 90ROI - minicom: 1850 60 90 91

Israel□

1201

Italia□

Telefono Amico: http://www.telefonoamico.it/ 199 284 284Samaritans onlus Italia: http://www.samaritansonlus.org/ 800 86 00 22

Japan□

Tokyo - Japanese: 3 5286 9090 befrienders-jap.orgTokyo - English: 03-5774-0992 telljp.comOsaka - Japanese: 06-6260-4343 spc-osaka.orgThe above sites maintain links to related resources in other cities and other formats like chat and text.

Korea□

LifeLine 1588-9191Suicide Prevention Hotline 1577-0199□ http://www.lifeline.or.kr/

Lebanon□

Embrace: https://embracelebanon.org/ Phone 1564

Malta□

179

Mexico□

SAPTel: http://www.saptel.org.mx/ (55) 5259-8121

Netherlands□

0900 0113□https://www.113.nl

New Zealand□

0800 543 354 Outside Auckland09 5222 999 Inside Auckland

Norway□

Kirkens SOS offers phone support and chat: 22 40 00 40 and http://www.kirkens-sos.no/Directory of additional resources here: https://www.psykiskhelse.no/hjelpetelefoner-og-nettsteder

Osterreich/Austria□

116 123

PortugalSOS VOZ AMIGA: 21 354 45 45 or 91 280 26 69 or 96 352 46 60 (Daily, 1600-2400h) http://www.sosvozamiga.org/ Telefone da Amizade: 22 832 35 35 or 808 22 33 53 (Daily, 1600-2300h) http://www.telefone-amizade.pt/

Romania□

0800 801 200

Serbia□

0800 300 303 or 021 6623 393

Singapore□

Samaritans of Singapore: 1800 221 4444 https://www.sos.org.sg/

South Africa□

LifeLine 0861 322 322Suicide Crisis Line 0800 567 567

Spain□

http://www.telefonodelaesperanza.org/

Sverige/Sweden□

mind.se phone: 901 01 chat: https://chat.mind.se/ Both available 0600-2400 daily.

Switzerland□

UK□

Samaritans (www.samaritans.org)Voice: 116 123 (24/7 Free to call, will not appear on phone bills, formerly 08457 90 90 90)Email: emailjo@samaritans.org Shout - Crisis Text Line UK (https://www.crisistextline.uk/)Text: SHOUT to 85258

Helplines for Men from thecalmzone.net:Voice: 0800 58 58 58 (5pm to midnight nationwide, also 0808 802 58 58 London and 0800 58 58 58 Merseyside)Text 07537 404717 (5pm to midnight, start your text with CALM2)Online Chat: https://www.thecalmzone.net/help/get-help/

ChildLine (childline.org.uk), for those 19 and under:Voice: 0800-11-11 (Free to call, does not appear on phone bills)Online Chat: http://www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx Email: http://www.childline.org.uk/Talk/Pages/Email.aspx

Papyrus HOPELINEUK, suicide prevention specialist service for children and young adults (under 35)Hours are 9am – 10pm weekdays 2pm – 10pm weekends 2pm – 10pm bank holidaysVoice: 0800 068 4141Text: 07786209697Email: pat@papyrus-uk.org

Directory of suicide-related services: http://www.supportline.org.uk/problems/suicide.php

United States□

National Suicide Prevention Lifeline: 1-800-273-8255 (TALK)Veterans press 1 to reach specialised support.Press 2 for Spanish-language support

Online Chat: http://chat.suicidepreventionlifeline.org/GetHelp/LifelineChat.aspx

Crisis Text Line: Text “HOME” to 741741.

Youth-Specific services (voice/text/chat/email) from the Boys' Town National Hotline: http://www.yourlifeyourvoice.org/Pages/ways-to-get-help.aspx

Trans Lifeline: 1-877-565-8860

EU Standard Emotional Support Number 116 123 - Free and available in much of Europe, you can check which 116 helplines are available in your country here

Uruguay□

Landlines 0800 84 83 (7pm to 11 pm)(FREE) 2400 84 83 (24/7)Cell phone lines 095 738 483 *8483

Darknet Markets

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.

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 (Radnom market) down?

If you cannot access a site, there is most likely a site-wide outage; you are not the only one having difficulties. Check the markets specific subdread 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 on /d/Darknetmarkets !

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 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.

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 from Dark.Fail, a market specific subdread

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.

Important tips for using markets□

- **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.

- Found a link on the hidden wiki or similar sites? It is very likely that they are a scam.

- **Never** use a market that requires javascript. Read about why here

- **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 or passwords. 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.

- 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.

- 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 /d/DarkNetMarkets or /d/Dread immediately.

- Use KeePassXC 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 PayPal’s 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.

Types of markets□

Before we can jump in and pick what market you want to use it’s important to understand the different types of markets you will or different some of the different payment methods you will come across. The three main ones are:

- Multisig
- Escrow
- Direct Deal

Each market does things slightly different so even if you see they are an escrow market make sure you take the time to read their user guides. Typically these are found on the market homepage, or on their market specific subdread.

Escrow□

In standard escrow the market holds the money during the purchase. They are typically the most common types of market you will find. You send your coins to the market controlled wallet. 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, Empire, evolution, abraxas, nucleus, middle earth marketplace.

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

Escrow□

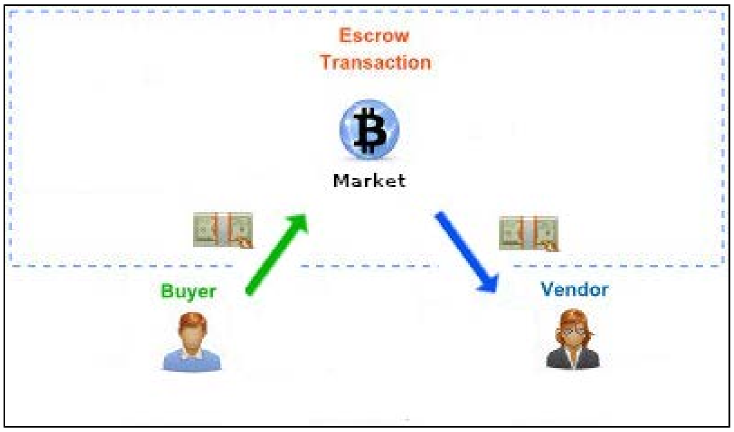
In standard escrow the market holds the money during the purchase. They are typically the most common types of market you will find. You send your coins to the market controlled wallet. If you received your order you tell the market to finalize your order and give the vendor your money.

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, Empire, evolution, abraxas, nucleus, middle earth marketplace.

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



Direct Deal/Finalize Early (FE)□

Vendors that have been around a very long time sometimes will join Direct deal markets, or have FE status granted to them on an escrow market. Typically these vendors are considered more "trust worthy"

Most markets now have rules in place that forbid vendors from requesting you FE them if they have not been granted that status. If you get a message asking you to FE from a vendor this should be a big red flag for you. Do not do it.

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?

Choosing a Darknet Market□

Choosing a market can be very overwhelming. More and more markets come out everyday. It is important to do your own homework about different markets, and vendors. Making constant posts on /d/DarknetMarkets asking “Which market is the best right now?” will just leave you getting results from market shills or others trying to phish you. Instead you can check out the Alternative SubDread List. It has an entire section with market subdreads, start there and just read up about different markets, and other user experiences. Check frequently on market subdreads before you make an order. This will keep you up to date on any policy changes, or just keep you safer from exit scams.

Each market processes orders slightly different, make sure you check out market user guides that are usually right on their subdread.

Where do I find links?□

Make sure you NEVER accept links from people on forums, or sending you messages. Chances are they are just trying to phish you so they can steal your coins. Markets usually put their address up on the sidebar or in their wiki.

You can also get onions from trusted sources such as DarkFail or DarkNetLive

Note: Before you login or create an account on any market, make sure you **VERIFY** the onion address. More on that can be found in the coming chapter, How to verify an onion address .

Finding Products□

The other important part is finding a good vendor. You always want to stick with domestic orders when possible so finding a good vendor can take some time. To start you can make a post on /d/DNMSourcing or the drug specific sub (For example /d/LSD requestings others to let you know some of the vendors they have dealt with. You can also visit /d/DNMAds to see if you can find a vendor there.

Once you have found a vendor you would like to deal with it's time to do some extra homework on them. For starters you can put their name into the dread search box, see if you can find anything on /d/reviews about them. If everything seems to check out go on a market they vend on, and check recent feedback. If you still feel unsure about the vendor you may also make a vendor inquiry on /d/Darknetmarkets

More in depth tips for what to look for when selecting a vendor will be covered in the next chapter.

How to verify an onion address□

Verifying onions. It's such an important thing yet so many people don't know how to do it properly. **Always,** regardless of where you get the onion from take the time to verify it. You never know when you have a typo, or a simple error. Taking the 10 seconds to verify can save your coins from falling to a phisher.

Darkfail has a great tool to help you do it, but no one resource should be blindly trusted. You should always **manually** verify the onion address yourself!

Note: Before you can verify you are on the correct Onion make sure you understand how to verify a PGP signature.

Now that you know how to verify a signature we can verify an onion address. First we need to get a markets pgp key. Most markets put them on their subdread, but if not you can put /pgp.txt at the end of the mirror you want to verify.It should look like this: MarketOnionAddress.onion/pgp.txt

You'll probably have to complete a captcha. Then you should see the markets PGP key. Import the key like normal. (See above if you neeed help)

Once you have it imported put /mirrors.txt at the end of the onion you are on.It should look something like this MarketOnionAddress.onion/mirrors.txt You should see a page with some information like this on it:

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

Here are our onion links:
```

```
ar3a3uxsmdjvlv3o.onion
effma5umlll2bxmd.onion
xw7w4apecxzw4t7h.onion

- SomeDarknetMarket

-----BEGIN PGP SIGNATURE-----

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

Note: Some markets don’t use mirrors.txt check their subdread for what you should put at the end to verify.

If you see a message like above you can now verify the message is signed by the market pgp key you imported. It should come back with good signature at the bottom ,and at the top you will see a list of the current market mirrors. **Make sure the address you are on matches one of the ones in the signed message.** If it does you are on a official market onion!

Once you do this a few times it really only takes about 15 seconds to do. Always take the time to verify an onion regardless of where you get them from

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 /d/DarknetMarkets or /d/Reviews 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 /d/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 /d/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□

Vendor Scams

Scam Field	Scam Description	How To Spot It	How To Prevent/Fix It
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.
Feedback	Vendor uses an alt/puppet account and vote on their own product.	Multiple feedback that have similar qualities & spelling similar to	Check the forums, reddit, and any vendor review threads for the

		vendor profile.	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.
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.
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.
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.
Feedback	Sends a fake love letter instead of the product	You get a love letter that does not look like it comes from an official source.	Check if it is known how a real love letter looks like, show the support the alleged love letter.

Buyer Scams

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

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, Coins 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 vendor’s 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 /d/DarkNetMarkets or /d/Reviews make sure you check the templates that are available on /d/Reviews To include images in your review, make sure you read and followed the uploading images securely chapter.

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 buyer 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 /d/DarknetMarkets naming and shaming the vendor as long as you also publish the proof for it.

IRL OpSec□

General□

This chapter is about how to keep your OpSec tight in areas that are not primarily related to DNMs. It includes for example reselling (since few of your friends would probably be willing to set up Tails just to communicate with you).

Keep your mouth shut

The golden rule is to **never tell anybody where you get your products from**. Period. No exceptions. Even if a long time friend is nagging you to tell him who you get that dank shit from, do not give in the temptation to tell him about your elaborate DNM setup and how you import drugs in bulk.

You can never take back what you said (let’s not talk about murder here). Once only one person knows about that, you never know who else will know it too. And one of these persons will spill the beans to law enforcement when they get arrested because the try to get themselves out of trouble by telling them all they know about the crimes others did. Then you will get a visit and, in the best case, you only have to pay several thousands of dollars in lawyer payments.

You know how that will look when someone gets busted because he could not keep his mouth shut? Here some examples:

> Franklin said 18-year-old Ryan Andrew Backer was under investigation after county drug agents learned LSD was sent to him from the Netherlands.

Source

> The Monroe County district attorney’s office said that earlier this year university police received a complaint that Mancini was ordering LSD online and selling it. Authorities said a resident director for Lenape Hall at the college noticed Tuesday that Mancini had received a letter from Hawaii. The director contacted police and police obtained a search warrant.

Source

So if someone asks where you get your stuff from, just tell them you get it from some guy but do not get into details. If that person keeps asking you, you should rethink your business relationship with them. If they just can not accept that you want to keep your sources secret, they will also rat you out as soon as you get in trouble.

Communicating

Asking your friends or customers to send you PGP encrypted emails will probably result in some perplexed faces. So you will have to adapt while still not creating massive evidence against you.

Asking your friends or customers to send you PGP encrypted emails will probably result in some perplexed faces. So you will have to adapt while still not creating massive evidence against you.It is therefore important that you keep your communications, which can play a big part in your prosecution, secure. So please read that IPhone guide and/or that Android guide.

It is also important to use Signal with your contacts and that you check your friends phones to make sure they have it enabled and that messages are getting automatically destroyed after a short period of time (e.g. after 24 hours). Also push full disk encryption of the phones with a strong passphrase.

Do not forget to also turn off Icloud/google cloud backups as they will try to upload messages and photos to the cloud where they can be seized by law enforcement with a simple subpoena.

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 that is well vetted do a search around dread to find one. 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”.

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.

OTR(Off the record)

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.

Chatting with someone□

After setting up your jabber account to chat with someone you will need to add them 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”

Now you both can chat securely!

Authenticating your buddy□

You should see at the bottom right it says “unverified” 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.

It should now say in Green “Private”

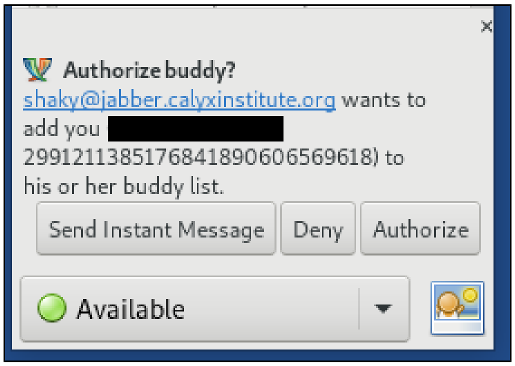
Chatting with someone□

After setting up your jabber account to chat with someone you will need to add them 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”.

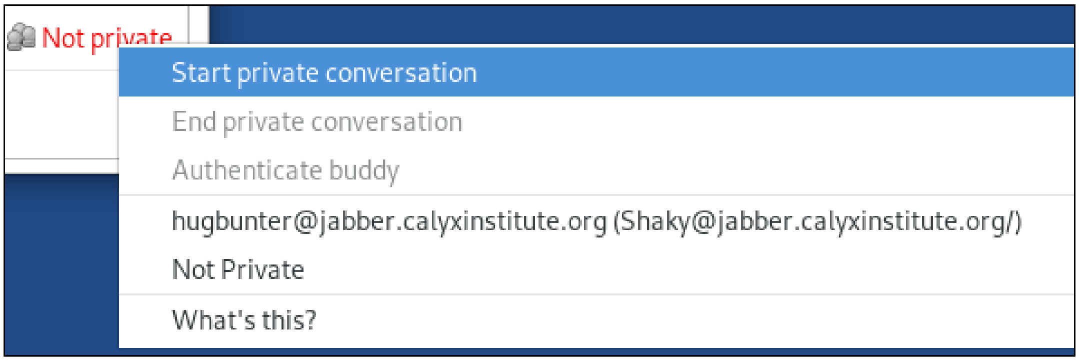
The user you want to add will receive a notification when he comes online again where he gets asked to authorize you (he sees your username). He has to click the “Authorize” button and confirm the new dialog window where he can also set a local alias for your username.

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.



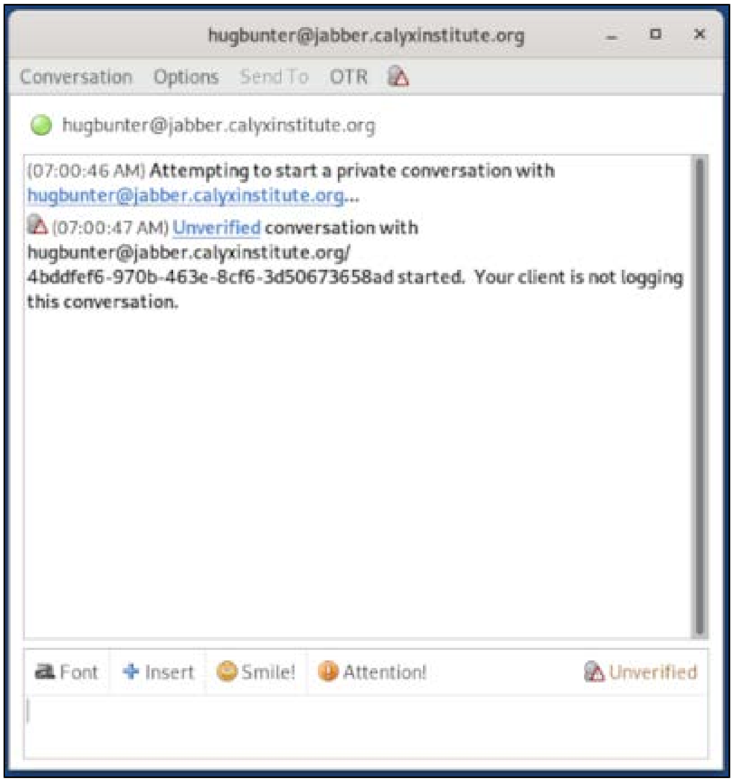
Authorize buddy?
shaky@jabber.calyxinstitute.org wants to add you [redacted] 29912113851768418906065696l8) to his or her buddy list.

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”.



Not private
Start private conversation
End private conversation
Authenticate buddy
hugbunter@jabber.calyxinstitute.org (Shaky@jabber.calyxinstitute.org/)
Not Private
What's this?

Then the chat window will print some messages like “Attempting to start a private conversation with other user’s username here”



hugbunter@jabber.calyxinstitute.org
Conversation
Options
Send To
OTR
hugbunter@jabber.calyxinstitute.org

(07:00:46 AM) **Attempting to start a private conversation with hugbunter@jabber.calyxinstitute.org...**
(07:00:47 AM) **Unverified conversation with hugbunter@jabber.calyxinstitute.org/ 4bddfef6-970b-463e-8cf6-3d50673658ad started. Your client is not logging this conversation.**

Font
Insert
Smile!
Attention!
Unverified

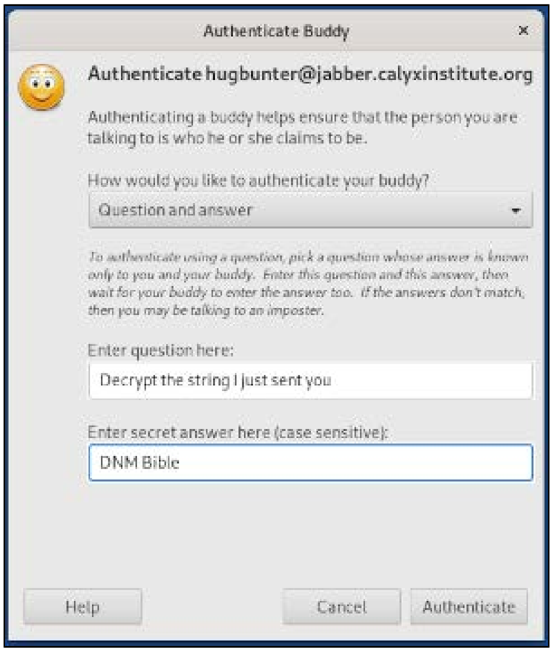
Now you both can chat securely!

Authenticating your buddy

You should see at the bottom right it says “unverified” 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.



Authenticate Buddy

Authenticate hugbunter@jabber.calyxinstitute.org

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?

Question and answer

To authenticate using a question, pick a question whose answer is known only to you and your buddy. Enter this question and this answer, then wait for your buddy to enter the answer too. If the answers don't match, then you may be talking to an imposter.

Enter question here: Decrypt the string I just sent you

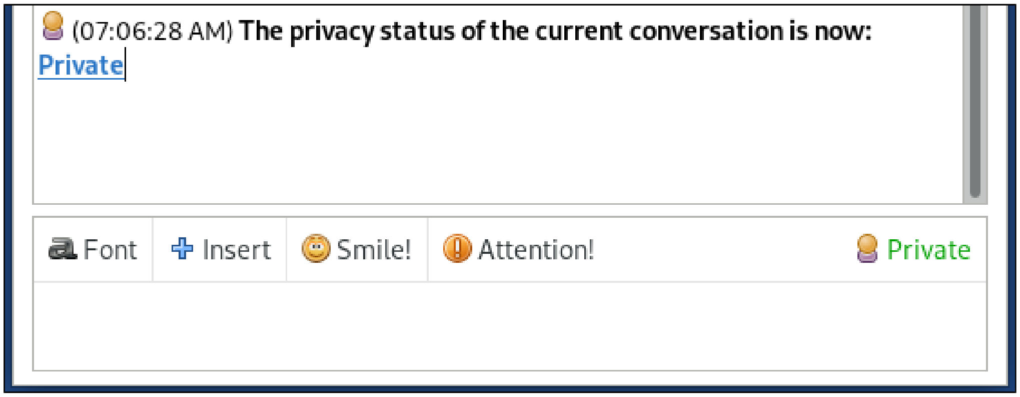
Enter secret answer here (case sensitive): DNM Bible

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.

It should now say in Green “Private”



(07:06:28 AM) **The privacy status of the current conversation is now:** Private

Here is a list of other well known services you can try out. Make sure you check their configuration for their server names, and port numbers.

- jabber.calyxinstitute.org
- creep.im
- thesecure.biz
- xmpp.jp
- jabber.hot-chilli.net
- jabber.otr.im
- chinwag.im
- jabb.im
- jabberes.org
- jabb3r.org
- conversations.im
- jabber.de
- kode.im

Bitmessage□

Note: It is important to note that most of bitmessage is written in Python2. Python2 was End of lifed in January 2020. This means that the core python team is no longer actively developing it, bugs or holes *could* eventually be found in python2 that might put risk on bitmessage, make sure anything sensative you still use PGP.

What is bitmessage?

Bitmessage is a decentralized, encrypted, peer-to-peer, trustless communications protocol that can be used by one person to send encrypted messages to another person, or to multiple subscribers.

Getting started

For Bitmessage to work we need to install Pythonqt4.

First thing you will want to do is make sure you have your persistence enabled, AND additional software. Check the setting up persistent volume chapter if you are unsure how to do that.

Next thing we need to do is boot tails with the Administration password enabled.

- On the Welcome Screen, enable the Administration Password. You can make it whatever you want it will reset after you shutdown tails. (Click the + in the bottom left)

Once you are booted into tails open root terminal

- Applications-system tools-Root Terminal.

You will be prompted for your password that you made at login.

In root terminal type the following two lines

```
apt-get update

apt-get upgrade

apt-get install -y python-qt4
```

- When the window pops up click install every time.
- Restart your system
- Once you restart you should see a notification that additional software is being installed.

Getting PyBitmessage

Now we can actually get bitmessage onto your system. To do this you need to download their source code.

- Go to Bitmessage.org it should automatically direct you to their onion address. or click here
- On their main page click Source code on github
- On github click Code->Download Zip.
- Once the download finishes extract the content to your persistence folder.
- Now navigate to the folder you just extracted. Places-> Persistent-> PyBitmessage
- Right click in the folder -> Open in terminal
- Type the following:

```
./bitmessagemain.py
```

Bitmessage should open up.

Configuring bitmessage

When bitmessage first launches you should be prompted with 3 options.

Connect now Let me configure special network settings first Work offline.

Check Let me configure special network settings first then ok.

- Change listening port to 9050
- Under Server/Tor change it to SOCKS5
- Server hostname should be localhost and port should be 9050
- Check the box that says Only connect to onion services (*.onion)

Now click the tab that says User interface

- Check the box that says run in portable mode.

This will save your keys and settings in the folder in your persistence storage. Make a backup of this folder so you don’t lose your keys!

Click ok. After a few minutes the light on the bottom right should change to yellow this is fine, and bitmessage will still be operating properly.

Creating a bitmessage address

To chat with people you will need to create an identity. On the main screen click new identity. A window will open read the different options

Since we are running in portable mode, and you made a backup of this folder with your keys in it (RIGHT!?) we can just make one with random number generator.

Click ok and you will see your new bitmessage number on the main screen.

Now you can also go to the send tab, where the options are pretty straight forward for sending a message. You can check the status of the message you sent on the main screen by going to your sent message.

And you’re done! You’ve successfully installed bitmessage!

Miscellaneous information□

The guides in this section you may never use. You should still take the time to get yourself familiar with some of it so that you can reference information from them if you ever need it. We will continue to expand this with extra information that can be useful.

Javascript warnings□

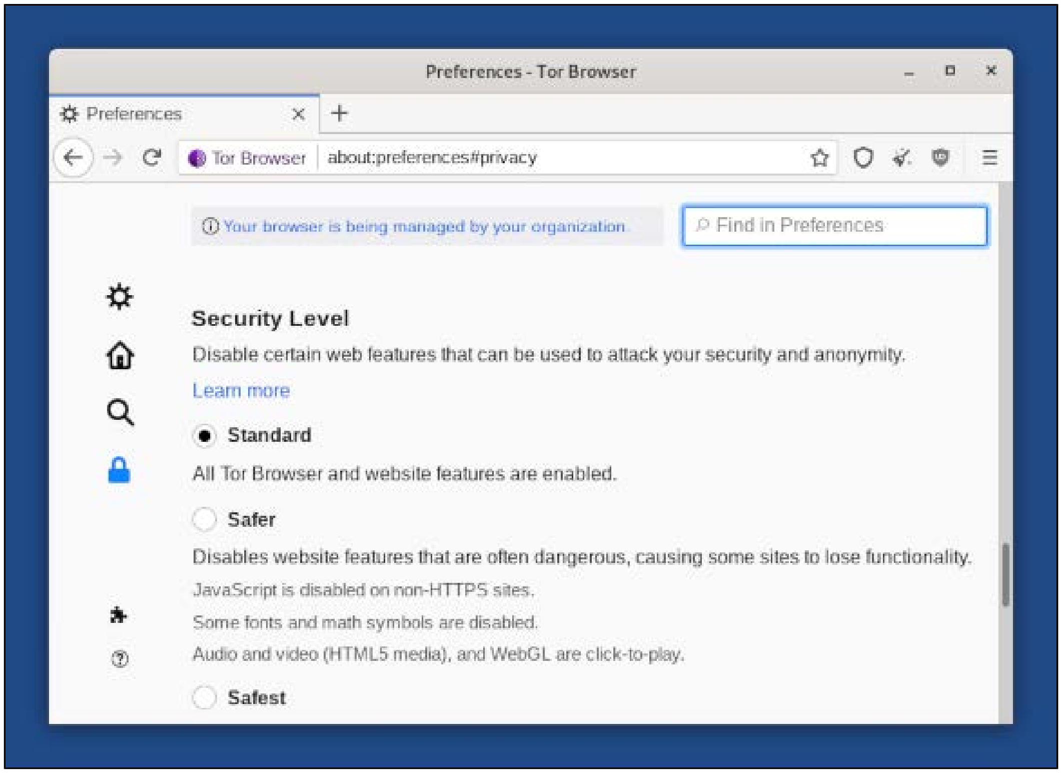
If you have javascript on you have probably gotten a warning on a few different sites by now. Javascript is not naturally dangerous, but it can be used in different situations to deanonymize who you are.

Again this is why we say keep your darknet activities, and clearnet completely seperate. Certain websites can use javascript to see what your real IP address is behind tor.

Disabling javascript□

Note: You will need to do this everytime you restart tails!

- When you first open tor click the 🛡 icon in your upper right hand corner.
- Next click Advanced security settings. You should see a window like this open:


Preferences - Tor Browser
Preferences
Tor Browser
about:preferences#privacy
Your browser is being managed by your organization.
Find in Preferences

Security Level

Disable certain web features that can be used to attack your security and anonymity.

Learn more

● Standard

All Tor Browser and website features are enabled.

○ Safer

Disables website features that are often dangerous, causing some sites to lose functionality.

JavaScript is disabled on non-HTTPS sites.

Some fonts and math symbols are disabled.

Audio and video (HTML5 media), and WebGL are click-to-play.

○ Safest

- Now click safest

Please note: You may still get an occasional message from a site saying you have javascript enabled. Due to it being blocked only by NoScript. NoScript will block javascript, but it ***could*** fail. For better results after you have set the security slider to safest, **and** do the following.

- In your address bar type About:config
- Click accept the risk and continue
- In the search bar type java
- Towards the top of the list you should see a value that says javascript.enabled double click that to set it to false.

and you’re done!

Removing exif data from images□

One day you might find yourself needing to take a picture of the product you ordered. Perhaps it’s for a review, or you’ve found yourself in a dispute.

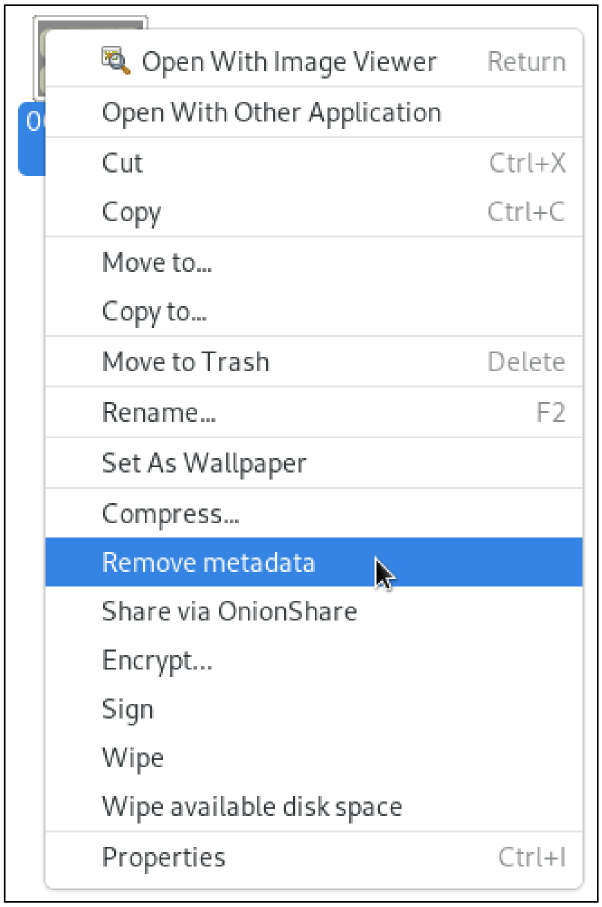
What is exif data?

EXIF stands for Exchangeable Image File Format. When you take a picture with your phone, camera, whatever it writes information in the file. This data ranges from information about your camera (or phone) to exact GPS coordinates. Before you upload an image make sure **you** remove the exif data yourself.

Note: Never use a service or website to remove the exif data for you! You never know when this service is saving a copy of the original image on their end!

Luckily Tails provides a very handy tool to remove this data!

- To remove this data simply right click on the image file you wish to remove it from.



- On the context menu click remove meta data.
- You will see a new file created that is cleaned of exit data.

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”).

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.

OpenBazaar□

Note: this chapter explains how to use a more secure alternative to the traditional, centralized darknet markets. While it is optional to use this alternative (called OpenBazaar) you should take a look at this guide and follow it if you have the choice to buy from a vendor through OpenBazaar (e.g. because he links his OpenBazaar store link in his profile description of a traditional market).

General□

OpenBazaar (short OB) is an open source project developing a protocol for e-commerce transactions in a fully decentralized marketplace. It uses bitcoin but also plans to support other cryptocurrencies in the future.

So basically it is a DNM as you know it but without anybody being able to shut it down since it is de-centralized (no single server that can get seized). Vendors are in control over their own stores and to take such a store down, LE would need to bust the vendor. Even then only one vendor would disappear with all the others still being able to vend as usual.

This is assuming that there is no grave bug / vulnerability in OB which makes it possible to disrupt the activity on OB or attack and possibly de-anonymize OB users in some way. To make sure the damage in such cases stays as small as possible it is extremely important that you not only set up OB properly but also follow the rest of the DNM bible. This is not the time for shortcuts. Your life and future is literally at stake. So take the extra mile and do it right.

Installing on Whonix□

To use OB on Whonix, do the following steps on the Whonix Workstation. Open the Konsole by double-clicking on the icon called “Konsole” on your Workstation desktop. Then enter the following command (you can copy it and paste it into the terminal / konsole by doing right-click -> “Paste”):

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

This makes sure that all your software is up to date. It should also ask you for your password that you should have changed when you set up Whonix. Then open the Tor Browser which is also linked on your desktop and visit the OB download page. Look out for the Linux category and click on the link that should be called “32-bit (deb)”.

Click on it and select “Save File” in the upcoming dialog, Then you get to choose where to save it, click on the “<” which is located between the “Save in folder:” text and the “Browser > Downloads” text. Then click on “user” which will be shown in the changed file path between “> home >” and “> .tb > tor-browser > Browser > Downloads”. Then simply double click on the folder called “Desktop” to enter it and press the “Save” button.

This description may be a bit confusing but it is to make sure you save the file in your normal user-directory and not the Tor browser directory (which has a similar structure and you may search forever when saving it there and later looking in the normal user-directory).

When the download is finished (which you can see at the download icon in your Tor browser that should be on the right of the address bar), switch to your desktop.

Once on your desktop make sure you only see one file with the OB name. If you see two, one of it should be called something like “openbazaar2_2.0.18_i386.deb.part” which means that the download is still running. Wait for the second file to automatically disappear which means that the download finished. Once that happened, right click on the remaining downloaded file -> select “Properties” -> switch to the permissions tab -> check the checkbox called “Is executable” and click the “OK” button.

Note: at the time of writing OB apparently did not offer any way to verify the downloaded file (like a signature file or hash) which is not ideal. The transmission of the file is still encrypted but if an attacker would have access to the download server it is stored on, he could replace it with a malicious version. If the developers should release signatures for the downloads in the future and it is not featured in this guide, please message the mods of /d/DarkNetMarketsNoobs □

You just started but you are already almost done! Now open the Konsole by double clicking on the icon called “Konsole”. Then enter the following command (you can copy it and then right-click and “Paste”):

```
cd ~/Desktop && sudo dpkg --install openbazaar2_2.0.18_i386.deb
```

Now this should ask you for your password first and then you should see lines containing an error due to software that is missing on your system but required to run OB (called dependencies). Do not worry about it, the next command automatically installs that required software and makes sure that your installation attempt of OB (that you did with your previous command) completes successfully.

```
sudo apt-get -f install
```

Press ENTER when you get asked “Do you want to continue? [Y/n]” and wait for the command to finish executing.

Done! You now have OpenBazaar installed. To open it simply open the Application Launcher which is the small “K” icon at the very bottom left (like the Start-Menu on windows) of your screen and type in “open” in the search bar. This should show you an entry called “OpenBazaar”, click on it.

Now the OB window will open and prompt you with a question dialog after some loading. Do not check the checkbox called “Use Tor”. Whonix already routes your entire internet traffic through Tor so you already got that covered. Click on the “Save” button and wait a bit till you get to a screen with the “Get started >” button. Click it and now you will be prompted to enter some information about yourself.

Obviously do not use your real name but choose an un-identifying username like “MichaelTheMan” (assuming that you are not named Michael) and leave out anything like your birth year or similar information. Now you can also set the currency to your preferred one. Leave out all the other options, they only harm your OpSec when setting them. The vendors you will be buying from will know your country you are from when you send them your PGP encrypted address and an avatar is just more data that could include digital traces leading to your true identity.

After clicking “Next”, skim the Terms of Service and agree with them.

Customizing the settings□

The last step you have to take in order to finish your OB setup is customizing the settings a little bit. To get there go to your “Home” tab and click on the “Customize” button. Then switch to the “General” tab located on the left side and set the option “Display Mature Content” to “Yes”. Click on the “Save” button again.

Then jump to the “Store” tab and set the option “Store” to “Off” since you are not a vendor and want to keep your attack surface as low as possible. Click on the “Save” button at the top right.

After that switch to the “Shipping Addresses” tab. **DO NOT ENTER YOUR ACTUAL ADDRESS THERE!** Only create a new one with the “Name” being your OB username and the country either being the default one or the one you are actually in. Leave out all the other options! The vendor will later receive all the shipping information in a PGP encrypted text you include in the order notes during your order. You can set your country if you want since it is not giving away much sensitive information which may be better for the vendor so he can work more efficiently (e.g. if he declines all orders coming from country x and he sees that you are coming from that country, he can decline it without having to decrypt your order note first).

Click on “Save” button after you added your dummy address.

You are now ready to buy in peace without any seizure banner greeting you! All you need is a vendor and you can follow the usual process with encrypting your address. If you already have a vendor with an OB store link you can visit his store now.

An OB store link should begin with “ob://” and then a long sequence of random letters and numbers, ending with “/store” or not, it does not matter as you will visit the same vendor any way. Simply copy that link from their market profile for example and paste it at the address bar on the top (they layout is similar to browsers like the Tor browser).

Note: be careful with random OB vendors! There is no guarantee that they are legit and actually selling the products they advertise. Maybe they are even LE and / or manipulated their feedback. Make sure you research your vendor properly before buying from him.

Tip: Whonix users can create an OB shortcut on their Desktop by clicking on the Start-Menu at the bottom left, typing “open” in the search bar -> right clicking on the OpenBazaar entry and selecting “Add to Desktop”.

- **Appendix**

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 /d/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

- Dread
- 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.

Resources□

The services listed here are for you to use at your own risk. Most are widely used and trusted, but you should never blindly trust any service.

Service name	Description of service
Erowid	Erowind is a service focused on education, and harm reduction. Click here for other harm reducti resources.
Dread	Dread is a darknet Reddit style forum.
Recon	Recon is a darknet market, and vendor search engine. Use this to locate vendors or do resarch on them
Dark Fail	Darkfail is service where you can get onions of markets, or other services
XMR Guide	The XMR guide will teach you everything about monero!
Dark Net Live	Dark net news, and onion monitoring.
Tails	Tails is the the go to operating system
Tor	If you’re reading this. Chances are you’re using tor

Note: want your service listed here? Please send us a message in modmail on /d/Darknetmarkets we will review it there.

Glossary□

A

Alprazolam (Alp) - A benzodiazepine sold under the brand name Xanax.

Alt - Alternate account, the term for when a user has two or more active accounts on a site.

Altcoin - Any cryptocurrency alternative to Bitcoin.

Amnesiac - “Forgetful” software that doesn’t save data, such as Tails OS.

Amphetamines - A type of stimulant drug.

B

Bars - A form of drug shape, usually long and thin. Most often used for benzodiazepines.

Bartard - A derogatory term for someone whose mental state is negatively affected by benzodiazepines.

Bayonet, Operation - A law enforcement operation resulting in the concurrent takedowns of AlphaBay and Hansa Market.

Benzodiazepine (Benzo) - A type of depressant drug, often used to treat anxiety or panic attacks.

Bitcoin (BTC) - The most popular cryptocurrency.

Blockchain - A public or private ledger of cryptocurrency transactions.

Bootable - A software or operating system able to be launched from removable media such as a USB stick or SD card.

Bunk - SLang term for fake narcotics with no effect.

Busted - Arrested or compromised.

C

Caps - A popular form of drug shape made by putting powder or small bits of narcotic into a small container. **Carding -** A type of fraud based around the use of credit cards.

Cocaine (Coke) - A stimulant drug, one of the most popular in the world.

Controlled Delivery (CD) - A law enforcement tactic involving monitoring buyer’s receival of a seized package.

Cryptocurrency - A type of decentralized electronic currency.

Cryptography - The study of encryption.

D□

Darknet Market (DNM) - A Tor-based commerce site, usually allowing the sale of illegal narcotics.

Dash - A popular form of altcoin.

DDoS - Distributed Denial of Service, in which an attacker forces a site offline with an unblockable amount of rapid connections.

Dealer - A salesman, usually of drugs.

Decoy - An innocuous item placed in a package to distract law enforcement and obscure illegal contents.

Decrypt - To reverse an encryption method and reveal the message to read easily.Deep Web - Any site, file, directory or anything else not indexed by search engines. Often erroneously confused with “Darknet”.**Dimethyltryptamine (DMT)** - A popular psychedelic and the most powerful on earth.

Direct Deal (DD) - To conduct business with a vendor directly, rather than through a market with escrow.

Dox - To leak or publicly post personally identifying information of a person, including name, address, or description.

Drop Ship - A vending tactic involving the vendor passing the buyer’s address on to another vendor to ship to, eliminating any need for the middleman (dropshipper) to handle anything illegal in person.

E□

Electrum - The most popular type of Bitcoin wallet.

Encrypt - To use an encryption program or method to render a message unreadable to all those without the means to decrypt.

Entactogen - A type of drug often associated with stimulants, named after their ability to enhance user’s emotions.

Escrow - A form of buyer and vendor protection in which a third party (aside from the vendor and buyer) holds money in place until the buyer receives their product.

Exit Scam - A type of scam in which a vendor or market convinces users to release as much money as possible into their control, before disappearing with the funds.

F□

Fake ID - Any form of fraudulent identification.

Fentanyl (Fent) - A dangerous and highly-potent opiate.

Finalise Early (FE) - To release money from escrow before receiving a product.

Forum - A form of social media site where users can discuss a range of subjects.

Fraud - A method of using deception or unlawful methods to gain money.

Free Open-Source Software (FOSS) - Software with the source code freely posted on the

Internet for anyone to use, replicate, and add to.

FUD - Fear, Uncertainty and Doubt; basically unverifiable or false rumours meant to make people lose trust in a site, service, person or group.

H□

Hitmen - A myth based around the urban legend of being able to contract murderers-for-hire on the Darknet.

Honeypot - A fake site run by law enforcement to gather information or money on criminal users.

Hotspot - When a product has "hot spots" and "cold spots", it means it is more or less potent in different areas of the pill, cap, bar, crystal, tab, or other form of consumption.

I□

I2P - A type of anonymity network similar to Tor, based on the Invisible Internet Project protocol.

J□

Jabber - A type of communication method.

L□

Linux - A brand of operating systems, usually FOSS. Many are based around different usages, including security, anonymity, pentesting, convenience or web hosting.

Litecoin - The first and possibly most popular altcoin.

Love Letter (LL) - An official notice from law enforcement to a buyer informing them of a seized illegal package.

Low-Hanging Fruit - A forum of buyer, vendor, or other user that is incredibly gullible or insecure.

LSD - Lysergic acid diethylamide, a popular form of psychedelic drug.

M□

Magic Mushrooms - A family of psychedelic fungi containing psilocybin.

Mariana's Web - A fictional "deeper layer" of the Darknet.

MDMA - Methylene Dioxymethamphetamine, a popular entactogen, stimulant and party drug.

Metadata - User and device information saved in a photo, screenshot, or similar type of file media. Usually removed by the security-minded before being shared.

Meth - Methamphetamine, a popular stimulant.

Microdose - The practice of taking a small dose of a narcotic, below the dosage at which it usually shows effects, for perceived nootropic or cognitive effects.

Monero - A popular privacy-based altcoin.

Multisig - The practice of two or three out of three people in a transaction (Buyer, Vendor, and Market) hold keys to an escrow wallet, meaning the money can only be released by the appropriate number of people using their keys.

Murder Homeless People - A popular joke term used as a euphemism for dealing drugs in real life.

O□

Onion - The TLD for all websites based on the Tor network, described as “hidden services”. It is referred to as that because of the “layered” approach to relays on the Tor Browser.

Onymous, Operation - A law enforcement operation resulting in the takedown of a number of hidden services, including Silk Road 2, Doxbin, and Cloud 9.

Opsec - Operation Security, the practice of remaining secure and anonymous on the Darknet.

Overdose - The effect of taking more than a safe amount of a particular narcotic relative to the user’s physical condition and tolerance. An overdose can result in physical or mental harm, or even death.

P□

P2P - Peer To Peer Networking, a form of networking in software in which every participant (or “peer”) is equally privileged and shares tasks equally.

PGP - Pretty Good Privacy, a populat encryption program.

Persistent - The opposite of Amnesiac, a persistent software or OS stores data upon shutdown to be used the next time it is launched.

Pharma - Pharmaceutical-grade narcotics, made in an official laboratory.

Phishing - A method of fraud involving the creation of fake login pages for websites to steal user data.

Pidgin - A software used for communication with others using IRC, XMPP, or similar protocols.

PIHKAL - Phenethylamines I Have Known and Loved, a well-known book by Alexander and Ann Shulgin.

Pills - A form of drug similar to a bar, but usually smaller.

Private Key - One part of an encryption keypair, a private key is used to sign or encrypt messages by one party, and should NEVER be shared.

Psychonaut - A term for someone who frequently uses psychedelics.

Psyops - Psychological Operations, a type of psychological warfare.

Public Key - One part of an ecryption keypair, a public key is shared with other people to allow them to encrypt messages to you or verify messages you have signed with that key.Purity **-** The measure of how clean or potent a drug is.

Q

Qubes - A form of compartmentalized and security-focused operating system based on Linux.

R

Reagent - A chemical added to another chemical to cause a reaction. This method is often used in test kits to verify the makeup of an unknown narcotic.

Red Rooms - A type of urban legend based around the myth of finding live-streamed torture and murder videos on the Darknet.

Research Chemical (RC) - A type of designer drug, often sufficiently new as to have no official legislature against the use of them.

Re-Up - Slang term for a street dealer or vendor buying a new batch of a product to refill their stocks.Review **-** A public form of feedback on a vendor’s shipping ability, communication, and product quality.

S

Scam - When one vendor, buyer, or other user steals money from another.

Seized - A package is seized if it is discovered by law enforcement and taken.

Selective Scam - A form of scam in which a vendor sends the majority of products, but scams every once in a while.

Serotonin Syndrome - A type of medical effect that happens after the careless use of entactogen, stimulant, or similar drugs.

Sheet - A page of tabs/blotters, usually up to 200 or so.

Shill - A user giving good or bad feedback on someone else with the intention of changing public opinion, while secretly benefitting from doing so.

Socks5 - A popular type of proxy software.

Subdread - A subforum based on popular Darknet social media site Dread.

Subreddit - A subforum based on popular clearnet social media site Reddit.

SWIM - Someone Who Isn’t Me, a saying on illegalist forums and sites to distance a user from illegal activity (e.g.: “SWIM would like to order drugs on the Darknet”).

T□

Tab - A form of drug consumption media created by absorbing dissolved or liquid narcotic substance into a piece of perforated or unperforated paper. Also known as a “blotter”.

Tails - An amnesiac, bootable operating system with a focus on anonymity.

Telegram - A popular type of messaging software.

Test Kit - An apparatus used for finding out the active ingredient in an unknown narcotic.

TIHKAL - Tryptamines I Have Known and Loved, a popular book by Alexander and Ann Shulgin and the sequel to PIHKAL.

Tor - A type of anonymity network accessed via the Tor Browser.

Tor 2 Door (T2D) - The time it takes between a vendor accepting an order and it arriving at the buyer’s address.

Tripping - The act of being under the influence of a mind-altering, usually psychedelic substance.

Tripsitter - A sober person employed by a person under the effects of a psychedelic substance to watch out for their wellbeing.

TrueCrypt - A now-defunct software for encrypting and securing files.

Tweaker - A derogatory term for someone negatively mentally impaired by stimulants, usually amphetamines or methamphetamine.

V□

V2 - A type of onion address comprised of 16 characters, widely considered less secure and DDoS-proof than the alternative, v3 addresses.

V3 - A type of onion address comprised of 56 characters, ostensibly more secure and impervious to DDoS than v2 addresses.

Vendor - A person who sells narcotics or other goods or services on a Darknet Market.

Veracrypt - The successor to TrueCrypt, a software available for file encryption and security.

VPN - Virtual Private Network, a type of proxifying anonymity software.

VPS - Virtual Private Server, a virtual machine used as a hosting server for a website.

W□

Whonix - An anonymity-focused and Linux-based operating system, often used with Qubes. It is mostly catered to experienced Linux users with a higher risk profile than Tails users.

Wickr - A popular type of communication software.

X□

XMPP - A type of communication protocol, compatible with numerous software, including Pidgin.

2□

2C-B - A psychedelic party drug, often sold in powder or pill form.

Frequently Asked Questions□

Why am I getting Javascript warnings?□

Read about why here.

Can’t I just use a burner phone instead of a secure OS?□

No. Cell phones are not secure at all. They have a lot of exploits in them. Go on craigslist/ebay whatever buy a laptop that is a few years old. It does not need to be anything special or expensive.

Do I really need to convert my coins if I’m only buying personal amounts?□

Yes! You wouldn’t just hand a dealer drugs in front of LE in real life, don’t do it here.

What are the odds of (INSERT DRUG) getting seized? or my door getting kicked in?□

No one can give you a 100% answer on this. If you read through the entire bible you can greatly minimize your risk. If you select a vendor that has complete shit stealth, order from a hot country the odds will go up.