DNM Bible

https://vaiyo.io/dnm-bible/

DNM Meaning

The term **DNM** indeed stands for **DarkNet Markets**. These are hidden online marketplaces that operate on the dark web, a part of the internet that is not indexed by standard search engines and requires specific software, configurations, or authorization to access. DarkNet Markets facilitate the buying and selling of a variety of illegal goods and services, including drugs, counterfeit items, malware, and other illicit materials. Transactions on these markets often use cryptocurrencies due to their pseudonymous nature, which can provide a layer of anonymity for users. Due to their illegal nature, DarkNet Markets are subject to law enforcement actions and are often shut down, only to see new ones emerge.

Table of Contents

        - Erowid
        - National Harm Reduction Coalition
        - Tripsit
        - DanceSafe
        - Drugs and Me
        - DrugWise
        - SaferParty
        - SocietalActivities
    - Labs
        - Energy Control International
        - DrugData
        - Wedinos
        - Get Your Drugs Tested
            - How We Test Your Drugs
        - Vancouver Coastal Health
        - Drug Foundation
    - Suicide Hotlines
        - United States
        - Canada
        - United Kingdom
        - Australia
        - New Zealand
        - Ireland
        - South Africa
        - India
- Darknet Markets
    - FAQ
    - Important tips for using markets
    - Types of markets
        - Multisignature (Multisig) Markets Explained
        - Escrow
        - Direct Deal
    - Choosing a Darknet Market
    - Choosing a vendor
        - Tips
        - When a Vendor Doesn't Accept Your Order
    - Tips for Being an Effective Buyer
    - Getting a lawyer
        - If you get in legal trouble.
        - Selecting and Preparing for Legal Representation
    - Making a purchase
        - Essential Tips for a Smooth Transaction

Introduction to the DNM Buyer's Bible

Greetings and a warm welcome to the guide designed for DNM purchasers, affectionately known as the DNM Bible.

This manual serves as an exhaustive resource for individuals seeking to make secure transactions on darknet markets. Drawing upon the principles of operational security (OpSec) best practices, adherence to the guidelines provided within will significantly reduce the likelihood of detection by authorities. Absolute security is an unattainable goal; however, the DNM Bible equips buyers with strategies to make the endeavor of apprehension by law enforcement exceedingly difficult and not worth the effort.

Should you be navigating these waters for the first time, with little to no familiarity with concepts such as Tails, Monero, and PGP, prepare to dedicate several hours to understanding and implementing the advice contained in this guide. Immediate success in purchasing from darknet markets is unlikely; setting up a secure environment as outlined in the DNM Bible is a time-consuming process. Nevertheless, once the initial setup is complete, subsequent transactions will become straightforward, requiring only repetition of the established secure procedures.

Engaging with DNMs may not suit everyone. Individuals with limited computing skills or those unwilling to allocate the necessary time might find more safety in traditional procurement methods, avoiding the potential legal ramifications associated with misuse of DNMs.

For those ready to commit time and effort to learn, this guide is your roadmap. Follow each directive carefully. Should obstacles arise, refer back to the DNM Bible for guidance.

To enhance understanding, certain sections include images to demonstrate

specific actions. These are intended as supplementary visuals; given the rapid evolution of software, these images may soon become outdated. Always prioritize the written instructions and linked resources. The images are there to assist should you encounter confusion.
Enjoy your reading, and prioritize your safety.

Overview

The creation of the DNM Bible was made possible through the incredible efforts of numerous individuals who volunteered their time and expertise to develop the tools recommended within this guide. To express gratitude for their contributions, consider supporting them by donating to the Tor Project, Tails, and/or GnuPG occasionally. If you can afford to purchase substances, allocating funds to appreciate those who facilitate secure and safe transactions to your doorstep is equally important.

Preparation Guidelines

Before diving into the procedures detailed in the DNM Bible for engaging in activities that are, frankly, illegal, and minimizing your chances of detection, heed this crucial advice: Avoid conducting any activities associated with the darknet on your regular operating system or standard web browser. It's vital to dissociate your darknet dealings from your actual identity as much as possible. For instance, your web browser might retain a history of the sites you've visited, potentially exposing your activities to someone else using your computer. Moreover, platforms like Reddit may sell the data they accumulate about you to third parties (such as advertisers), inadvertently broadcasting your interest in procuring illicit substances online. Reddit's tracking across various websites can link your disparate online personas (like your Facebook account), possibly leading to the discovery of your real name.
Safeguarding your anonymity to ensure that no one can trace your awareness of DNMs is surprisingly straightforward. Therefore, please pay close attention to the upcoming section and adhere to the recommended practices. It would be regrettable if a neglect of such basic precautions resulted in legal repercussions.

Regarding Video Tutorials

While video tutorials are available, their use is discouraged for several reasons:

- Viewing these tutorials can jeopardize your operational security (OpSec), as platforms like YouTube will record your interest in online drug purchases.
- Many tutorials omit critical information necessary for making informed purchases.
- Unlike the DNM Bible, which benefits from the scrutiny and contributions of a broad community, video tutorials are typically the work of an individual and lack communal vetting.

Additional Note: Over time, this guide has expanded considerably. Although some of the content in the Miscellaneous Information chapter might seem irrelevant at first, all information provided could prove beneficial eventually. Even if you do not

immediately apply all the knowledge, being acquainted with these additional insights is advantageous.

Operating System

A critical component of navigating the darknet securely is the selection of a robust operating system. The primary focus of the DNM Bible is on Tails, though mentions of Whonix and Qubes are also included.

IMPORTANT REMINDER: As reiterated throughout the guide, it's crucial to avoid using Windows or Mac for these activities.

Selecting your setup

This section delves into various secure configurations, predominantly centered around Tails. Below, we outline three common setups utilized by users.

Tails

Ideal for beginners or those not well-versed in technology, Tails is a user-friendly choice. Operating as a live system from a USB stick, Tails leaves no trace once the session ends, unless the persistence feature is activated (which we'll explore further on). Equipped with all necessary tools from the start, Tails is designed for ease of use. This guide mainly caters to users of Tails, recommending it for its simplicity and comprehensive features.

Whonix

Whonix suits those with intermediate knowledge. It operates through a host system and VirtualBox, allowing for the possibility of USB-based operation. However, due to significant data writing, installing it on a dedicated hard drive is advised. This setup requires manual encryption and familiarity with terminal commands. Whonix supports multiple workstations with all traffic funneled through a gateway, enabling isolation. If you're not comfortable with its complexity, Tails might be a better choice.

Whonix/Qubes

The Whonix/Qubes combination represents one of the most secure configurations available, recommended for advanced users. Incorrect setup can compromise your operational security. Qubes, serving as the host OS, integrates Whonix seamlessly, facilitating the operation of isolated Qubes for enhanced security. If you're new or unsure about the technical demands, sticking with Tails is advisable.

For the majority, Tails emerges as the optimal choice, providing automatic encryption and a suite of tools for safety. Those interested in Whonix can find more details in the DNM Bible.

For insights into how Whonix, Tails, and running Tor alone compare, further reading is recommended within the guide.

Guidance on the Host Operating System

Critical Advisory

As we progress, grasping the significance of avoiding Windows or Mac for your darknet activities is crucial. A common misconception is that running Whonix within a VirtualBox environment on these platforms equates to security. While

using Tor on Windows might seem harmless to many, this guide aims to elevate your security far beyond such basic measures.
Both Windows and Mac are fraught with vulnerabilities and have corporate policies that do not hesitate to collaborate with law enforcement agencies. This guide's intention is to fortify your privacy and security measures. Operating on Windows or Mac makes you more susceptible to law enforcement interception, likening users to easy targets.
A paramount principle in darknet dealings is the absolute segregation of your darknet persona from your real-life identity. Compromising your everyday digital life with darknet activities is a risk no one should take.

Advice for Mac Users

Mac users might encounter compatibility issues with running Tails due to hardware incompatibilities. This, however, should not be seen as a loophole to compromise on operational security by resorting to VirtualBox as a workaround.
An effective solution is to acquire an affordable, used laptop via platforms like Craigslist, eBay, or local pawn shops. A modest investment can secure a device capable of running Tails efficiently, often for under $100.
For a comprehensive overview of the pitfalls associated with using Windows or Mac and further justification for the recommended practices, the DNM Bible provides detailed insights.

Tails

Tails stands as a portable operating system that can be launched on virtually any machine using a DVD, USB stick, or SD card. Its primary goal is to protect your anonymity and privacy by offering features that:

- Enable anonymous internet use and bypass censorship, as it routes all online traffic through the Tor network,
- Ensure that no digital footprint is left on the device utilized, unless explicitly permitted, and
- Provide advanced encryption tools for securing your files, emails, and instant messaging.

Tails is exceptionally beneficial for activities you wish to keep private. Furthermore, it's fully equipped for darknet market activities without the need for additional software installations. All necessary tools for purchasers are pre-installed.
The standard Tails desktop environment is designed for efficiency and ease of use, embodying the operating system's commitment to security and privacy as highlighted in the DNM Bible.

Is Utilizing Tails Imperative?

Absolutely. You may consider yourself an insignificant target, believing that no one would bother pursuing you. However, let's examine a scenario to illustrate the importance of Tails: Imagine you place an order using the Tor browser on a Windows system, and all seems to proceed smoothly. Unfortunately, the package is intercepted by customs due to improper packaging by the vendor. This leads to law enforcement initiating an investigation into the attempted delivery of illegal

substances to your address. A likely strategy they might employ is a controlled delivery, where the package is delivered, but followed by a raid on your premises for possession of illegal drugs.
Operating on a Windows platform, which lacks robust security, would leave tangible evidence for authorities to build a case against you. This predicament is avoidable with Tails, as it leaves no digital footprint or evidence of your activities, including any files saved in the persistent storage. Tails operates without leaving any trace of its use on your computer.
Hence, the value of Tails extends beyond merely evading detection; it significantly reduces the repercussions if you are, unfortunately, apprehended.

Do You Require a VPN?

Generally speaking, **no**.
Here's a summary from the Tails website regarding VPNs:
The request for VPN support in Tails stems from a misconception that adding more layers, such as VPNs, enhances Tor's anonymity. This belief is fundamentally flawed. VPNs can actually compromise anonymity by serving as a constant entry point (if used before Tor) or as a fixed endpoint (if used after Tor).
Moreover, replacing Tor with a VPN does not align with Tails' mission, as it significantly degrades anonymity.
This is a direct quote from the official Tails website.
The primary purposes of using a VPN might be to a) conceal your Tor usage from your Internet Service Provider (ISP) and b) introduce an additional layer of security.

- a) To hide Tor usage from your ISP, Tails offers a configuration option upon startup. By selecting **More Options** at the greeting screen, then choosing **This computer's Internet connection is censored, filtered, or proxied** you can mask your Tor usage. This feature, however, is intended for users in restrictive regimes where Tor is banned or dangerous to use openly. Utilizing this option without necessity diverts resources from those in dire need of it.
- b) In the scenario where law enforcement compromises the Tor network to trace your IP address, they would identify your or the WiFi owner's real location. Using a VPN in this context would lead them to the VPN server's IP instead, assuming correct setup of both Tails and the VPN. Nonetheless, law enforcement pursuing such an extensive effort to trace a small-scale buyer through Tor de-anonymization is highly improbable. No precedent exists of a buyer being caught this way, and it's unlikely to occur.

There are numerous operational security (OpSec) considerations more critical than the combination of Tails with a VPN. Prioritize these areas first.
For those still interested in integrating Tor with a VPN, further reading is advised.

Previously Made Purchases Without Tails?

Not utilizing Tails for your prior transactions was an oversight. The immediate

concern isn't necessarily that law enforcement will track you down for those actions, but if issues arise later, evidence of past transactions could be discovered and used against you. It's crucial to eliminate any such evidence promptly and enhance your operational security (OpSec) for future dealings.

Begin by removing all applications involved in your previous orders from the non-secure operating system you used. This includes uninstalling the Tor browser, any PGP encryption tools, Bitcoin wallets, etc.

Next, you'll need to overwrite the unused space on your hard drive. This step makes it more difficult for anyone to recover the deleted applications (and thus, evidence that could compromise you), without affecting other files or personal documents, such as photos in your home directory. This process ensures that the spaces previously occupied by the uninstalled applications are overwritten, but your personal files remain untouched.

Instructions on how to execute this on Windows, Mac, and Linux are provided.

Keep in mind, this method isn't foolproof. Your operating system may have generated log files that indicate the use of software commonly associated with DNM transactions (like PGP encryption tools). It's imperative to adhere to the outlined measures and, moving forward, confine all DNM-related activities to Tails.

Utilizing Tails on Your Own or Shared Computers

Operating Tails on any computer does not affect nor is it affected by the computer's existing operating system. This means Tails can be used interchangeably on your personal computer, a friend's, or even a public one at a library. When Tails is shut down, the computer reverts to its original operating system for normal use.

Tails is meticulously designed to avoid utilizing the computer's hard drives, including any swap space. It operates exclusively in RAM, which is cleared upon shutdown, ensuring no remnants of the Tails system or its use remain. This feature earns Tails its description as an "amnesic" operating system.

This capability ensures the safety of working with sensitive information on any computer, safeguarding against the potential for data recovery post-shutdown. While Tails avoids leaving traces on the computer, it still permits the explicit saving of documents to external storage devices like USB sticks or hard drives for later access.

In summary, Tails offers a secure environment for sensitive tasks on any computer without necessitating the purchase of a dedicated device for these purposes.

Accessing Tails Via Your Personal WiFi

When operating Tails or utilizing Tor on your personal WiFi network, your Internet Service Provider (ISP) can detect that Tor is being used but cannot discern your activities. For users concerned about ISPs detecting Tor usage, Tails allows the configuration of bridges during startup. This is achieved by selecting "Yes" to more options on the welcome screen, then choosing the "My computer's Internet connection is censored, filtered, or proxied" setting. Employing bridges masks your Tor usage from the ISP. However, this precaution is generally unnecessary unless you're in an environment where Tor usage is restricted or illegal. Utilizing

bridges without such a necessity diverts resources from those in urgent need. The sole advantage of connecting to a network other than your own would be to mask your actual IP address in the unlikely event of a de-anonymization attack, presenting the network's IP (like a coffee shop's WiFi) instead. Yet, the feasibility of such attacks targeting individual buyers is low, and the additional risks introduced by using public networks (such as potential observation by others or surveillance cameras capturing your identity) do not justify the method for buyers. Adhering to the comprehensive security measures outlined in the DNM bible while using your personal WiFi offers a more secure approach.

Utilizing WiFi Networks That Require Login

Engaging with WiFi networks that necessitate login credentials, occasionally linked to your real identity such as university WiFi, is a consideration for Tails users. Tails automatically alters MAC addresses, providing an added layer of anonymity by making it appear as though a different device is accessing the network with your credentials. This feature introduces a level of plausible deniability, allowing you to assert that your login details were compromised and used on another device. Moreover, the entirety of Tails' internet traffic is funneled through the Tor network, ensuring encryption and obfuscating the destinations of your online activities. Consequently, using Tails on a WiFi network requiring login credentials is feasible.

Do DNS Leaks Pose a Risk?

Within the Tor network, DNS requests for websites you visit are not made by your personal computer but by the exit node – the final relay in the Tor chain responsible for directing your traffic. This mechanism is in place because Tor supports TCP traffic but not UDP. By utilizing Tails, which automatically directs all internet traffic through the Tor network, concerns regarding DNS leaks are mitigated. The DNM bible emphasizes the importance of using Tails to ensure such security measures are automatically handled.

Selecting a New Computer for Optimal Tails Compatibility

If you're in the market for a new computer and intend to run Tails, most systems will suffice. However, to ensure the best experience, the DNM bible suggests adhering to the following advice during your selection process:

- Avoid purchasing an Apple product, such as a Mac or MacBook, as they may encounter compatibility issues with Tails.
- Verify that the computer does not contain hardware components listed under Tails' known compatibility issues.
- Preferably, opt for a computer that does not come pre-installed with Windows 8 or 10, as these operating systems have a higher likelihood of causing conflicts compared to machines with older versions of Windows or no operating system at all.

It's been noted by some users that Alienware computers exhibit good compatibility with Tails. Additionally, a list of laptops known to perform well with Tails is also available for reference.

Do I always need to use the most recent version of Tails?

Definitely. Always use the latest version of Tails at all times. Updates are very important because they often address security vulnerabilities that might otherwise leave you unprotected. Therefore, it is highly recommended that you take a few minutes to update Tails after you receive notification of an available update.

Recommended Hardware for Tails Compatibility

Encountering compatibility issues between Tails and your current hardware may prompt you to consider alternative devices. If feasible, first attempt to use Tails on a different computer. Below is a list of hardware that has been verified to work with Tails, as detailed in the DNM bible:

USB Flash Drives

Confirmed compatible USB drives with Tails 3.0 include:

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

These drives are widely available online and are priced between $6 to $15. The Onn brand is specifically available at Walmart stores, while Lexar drives are commonly found at Target.

It's worth noting that the Onn brand is produced by Sandisk for Walmart, a fact discovered post-testing but considered valuable enough to retain in this list.

USB WiFi Adapters

Before considering the purchase of a new WiFi adapter, it's advisable to try a direct Ethernet connection as a simpler and often more reliable alternative.

For those requiring a USB WiFi adapter, the following models have been tested and work with Tails:

- CanaKit Raspberry Pi WiFi Wireless Adapter/Dongle (available on Amazon)
- Edimax EW-7811Un 150Mbps WiFi Adapter (available on Amazon)
- Belkin N300 High-Performance WiFi USB Adapter

USB Ethernet Adapters

For users needing an Ethernet adapter, the following USB Ethernet adapters are confirmed to function with Tails:

- Plugable USB 3.0 to Ethernet Adapter (available at plugable.com/products/usb3-e1000)
- Plugable USB 3.0 Hub with Ethernet (available at plugable.com/products/usb3-hub3me)

Is It Safe to Purchase USB Sticks With Pre-installed Tails?

It is not recommended to buy USB sticks that come with Tails already installed. The core issue is the risk of the seller having altered the Tails setup on the USB to, for instance, capture and send your passwords to them. The DNM bible advises to personally download, verify, and install Tails to ensure the integrity and security of

your setup.

Why Is JavaScript Globally Enabled by Default With Security Slider Set to Low?

The decision to enable JavaScript globally and set the security slider to a lower setting by default in Tails is aimed at accommodating users who may not be technically proficient. Adjusting to high-security settings can be challenging for those not familiar with the nuances of such configurations, potentially hindering their user experience. As a result, the developers have opted for more accessible default settings to facilitate a smoother experience for these users, as highlighted in the DNM bible.

Nonetheless, it's imperative for you to manually adjust the security slider to the highest setting each time you launch the Tor browser. This is crucial for enhancing your security, especially since these settings cannot be preserved between sessions, even with persistence enabled.

Guidance on Installing Tails

For those looking to install Tails, comprehensive guides are available to assist you through every step of the process, ensuring a smooth installation regardless of your operating system.

- For **Windows** users, follow the specific guide tailored to Windows installations.
- **Mac OS** users can access a guide designed for Mac environments.
- **Linux** users are not left out, with a guide available for installations from Linux platforms.

Should you use a keyboard layout different from the standard American layout, you'll need to adjust this at the Tails welcome screen. Simply navigate to the dropdown menu in the bottom right corner, scroll to find your layout, or choose "Other..." and type in the name of your layout (for example, typing "ser" for Serbian) until it appears. Select it, press enter twice, and you'll return to the welcome screen with the new layout activated.

It's important to note that downloading Tails via the clearnet is perfectly legal and doesn't require Tor or a VPN. However, post-download, verifying the integrity of the .iso file is crucial to avoid potentially compromised versions that could jeopardize your security.

A handy tip for those having trouble accessing the BIOS/boot menu: holding down the shift key while selecting restart will bring up the option to boot from a USB device or navigate to advanced UEFI options, facilitating the boot process.

Essential Settings and Advice as per the DNM Bible

- Each session you initiate with the Tor browser, it's imperative to adjust the security slider to the 'safest' setting. This action turns off JavaScript by default, a critical step since JavaScript can be exploited by websites to compromise your anonymity, and activates additional security measures.
- For those times when you must access clearnet sites requiring JavaScript (for example, to interact on reddit.com), modify the NoScript settings for

easier script management, allowing you to selectively enable or disable JavaScript as needed.

- Should you encounter a darknet market (DNM) requesting JavaScript activation, exit the site immediately.
- Upon deciding to power down Tails, ensure your device is fully shut off before extracting the USB drive.
- Regarding leaving Tails unattended: it's advised against leaving Tails operational if you're stepping away for more than a brief period (such as 10 minutes). Although rebooting may seem cumbersome, shutting down represents a vital security protocol to prevent law enforcement or anyone else from accessing unencrypted data should they gain physical access to your machine.
- Running Tails within a virtual machine is not recommended. Tails is crafted to operate as a live OS, ensuring optimal performance and security only when used in its intended form. Further details on this topic are available in the guidance provided by the DNM Bible.

Setting Up and Managing Persistent Storage

By design, Tails is amnesic, meaning it does not retain any changes or data once rebooted. This feature is essential for maintaining privacy and security. However, when engaging with DNMs, there's a necessity to preserve certain files and settings across sessions. This is where the Persistent Storage feature comes into play, allowing for the encryption and retention of data after restarting Tails. The system employs LUKS (Linux Unified Key Setup) for data encryption. For those interested in a deeper understanding of LUKS, further information is readily available.

It's crucial to verify the functionality of the Persistent Storage before relying on it. For instance, after setting up a cryptocurrency wallet as outlined in the DNM bible, reboot your system to ensure the persistence of your data and settings.

A critical reminder: the persistence password is your lifeline to accessing the encrypted data. Losing this password equates to losing access to the entirety of your Tails setup, including PGP keys, market accounts, and Electrum wallets. Always secure your wallet's seed phrase by writing it down.

Persistent Storage allows you to save:

- Personal Data
- Browser Bookmarks
- Network Connections
- Additional Software
- Printers
- Thunderbird email client
- GnuPG for encrypted communications
- Bitcoin Client for transactions
- Pidgin for instant messaging

- SSH Client for secure connections
- Dotfiles for custom configurations

Each option offers a detailed explanation upon activation, guiding you through the process of ensuring your essential data and settings are preserved according to the principles outlined in the DNM bible.

Establishing Persistent Storage

- To initiate or adjust Persistent Storage within Tails, navigate through: Application->Tails->Configure persistent volume.
- You'll be prompted to enter a passphrase. Input your chosen passphrase in both the 'Passphrase' and 'Verify Passphrase' fields. For crafting a passphrase that's both secure and easy to recall, consider using a mnemonic—a sequence of five or more words is advisable.
- Proceed by selecting the 'Create' button.
- Subsequently, a catalog of Persistent Storage features will be displayed, each representing various files or settings you can opt to preserve. Select your desired features and click 'Save' at the end.

NOTE: For newcomers unsure about which features to activate, it's advisable to start with Personal Data, GnuPG, Bitcoin Client, and Dotfiles. You can always incorporate more features later on.

- Following these steps, restart your computer.
- Upon logging in again, you'll notice a new setup.

You're now equipped to store personal files and documents in the Persistent folder. To access this folder, go to Places -> Persistent. The tools and features you've enabled will automatically save their data here.

NOTE: Deselecting a feature in the Persistent Storage settings will not erase its associated data stored previously. For deletion instructions, refer to the subsequent section as mentioned in the DNM bible.

Removing Persistent Storage

There may be times when you need to erase your Persistent Storage. While the process is straightforward, it's important to note that this method may not entirely prevent a determined attacker from retrieving files using sophisticated data recovery methods.

For a thorough erasure of Persistent Storage, it's necessary to securely wipe the entire USB stick, a process that is considerably more time-consuming.

- Boot Tails from the USB stick you intend to clear.
- At the Welcome Screen, do not unlock Persistent Storage.
- Navigate to Applications -> Tails -> Delete persistent volume.
- Confirm the deletion by clicking 'Delete'.

If your goal is to remove files associated with a specific tool without eradicating all data:

- Boot Tails and create an administration password on the Welcome Screen by clicking the plus sign. This password can be temporary as Tails will

reset it upon reboot.

- Access Applications -> System Tools -> Root Terminal to launch a terminal with admin privileges.
- Enter 'nautilus' to open the file manager with administrative rights.
- Proceed to /live/persistence/TailsData_unlocked in the file manager.
- Locate and delete the folder for the specific feature you wish to remove.

Upgrading Process

For updating Tails, simply adhere to the instructions provided in the guide on the Tails official website.
Encountering a 'not enough space' error during the upgrade? This indicates the need for a manual update. If you're puzzled by the lack of space, especially with a high-capacity USB stick, the DNM bible offers insights and explanations for this issue.

Data Backup Strategy

Ensuring the safety of your data is paramount, not only for the information stored on Tails but also for all other critical documents. This segment, focuses specifically on securing the persistence data within Tails. The risk of losing access to crucial assets such as your market accounts and digital wallets is not one to take lightly, hence the importance of following the prescribed backup procedures. While the task of backing up may seem tedious and often overlooked, the inconvenience pales in comparison to the potential loss of your Tails USB stick, along with all associated market accounts and cryptocurrency.
Committing a few minutes to perform regular backups is a small yet significant step towards robust data security.
Initiating the backup process requires an additional USB stick designated for storing your backup data.

Cloning Tails

Before proceeding, it's essential to clone your current Tails drive. For those who have already completed a Tails clone, you may skip to the section on backing up Persistent Storage.
Note: Cloning does not include Persistent Storage backup. Cloning must be performed prior to backing up Persistent Storage.

- Begin by booting from the Tails USB you intend to back up. After logging into Tails, connect the USB stick designated for backup.
- Navigate to Applications -> Tails -> Tails Installer, accessible from the sidebar.
- Upon opening the installer, you'll be prompted with a window.
- Choose 'Clone the current Tails' and select your backup USB from the 'Target USB stick' dropdown menu.
- Proceed by clicking 'Install'.
- A warning message will appear in a confirmation dialog. Confirm your action by clicking 'Yes'. The duration of the installation process varies by computer, with the progress bar often pausing momentarily during

synchronization.
- Completion is indicated by an ‘Installation Complete!’ message.

Congratulations, you have successfully cloned Tails.

Securing Persistent Storage with Backup Utility

Note: For those initiating a backup to a USB for the first time, you must first boot from your backup USB and activate the Persistent Volume along with any desired features (such as Electrum, GnuPG, Dotfiles).

- After configuring your backup USB, reboot using your primary Tails USB—the one you intend to back up. At the Welcome Screen, set an Administration Password of your choice; this will be reset upon shutting down Tails. (Look for the “+” icon at the bottom left to do this.)
- Once Tails starts with the Administration Password set, navigate through Applications -> Accessories -> Files to access the file manager.
- Connect your backup USB stick to the computer.
- In the file manager’s sidebar, you’ll find an encrypted volume. Click on this volume and enter the Persistent Storage password designated for your BACKUP Tails.
- This action will mount the TailsData volume, making it visible on the sidebar.
- Proceed to Applications ▸ System Tools ▸ Back Up Persistent Storage.
- Select ‘update’ to commence the backup process.

Congratulations, you have now successfully backed up your entire Tails drive, ensuring your critical data is preserved.

Securely Backing Up Persistent Storage Using Terminal

Note: For first-timers backing up to this USB, initiate by booting from your backup USB to activate the Persistent Volume along with any additional functionalities you require (like Electrum, GnuPG, Dotfiles).

- After setting up your backup USB, reboot from your primary Tails USB—the one you’re backing up. At the Welcome Screen, establish an Administration Password of your choosing, which will reset upon Tails shutdown. (Activate this by clicking the “+” at the bottom left corner.)
- With the Administration Password enabled, boot up Tails and navigate to Applications -> Accessories -> Files to open the file manager.
- Connect your backup USB.
- In the file manager, look for an encrypted volume listed in the sidebar. Click it and input the Persistent Storage password for your BACKUP Tails, making the TailsData volume visible in the sidebar.
- Launch the root terminal by either searching for ‘terminal’ and selecting ‘root terminal’ or through Applications -> System Tools -> Root Terminal, then enter the Administration Password you previously set.
- Execute the backup command in Terminal:

“`

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

Upon completion, Terminal will display statistics about the data transferred, indicating a successful backup:

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

Congratulations, you've effectively backed up your entire Tails drive! Future backups won't require a full drive clone; simply boot with the administrator password, unlock your backup, and execute the command to update your backup efficiently.

This process requires merely 5 minutes—commit to regular backups to safeguard your valuable data.

Installing Optional Debian Packages at Boot

This section of the DNM bible is optional. Follow these instructions only if you find it necessary to install additional packages beyond what Tails includes by default. Tails comes equipped with all essential software, and adding extra applications may introduce security risks. Nevertheless, Tails provides a feature for the automatic installation of Debian packages upon startup.

- **Boot Tails** and activate persistence along with an administrative password. To utilize this feature, activate the following persistence options in the Tails persistence configuration wizard (found under Applications -> Tails -> Configure persistent volume), ensuring they are marked with a green check:
- APT Packages
- APT Lists

If these options were not previously activated, reboot your system for the changes to apply. Upon restarting, re-enable persistence and set an administrative password once more. Proceed to open a root terminal (Applications -> System Tools -> Root Terminal) and input the following command to update your package lists:

```
apt-get update
```

This update process might take around 5 to 10 minutes. For demonstration, let's install the GPA package (GNU Privacy Assistant, a graphical PGP client) with the commands:

```
apt-get install gpa
```

Confirm the installation by pressing 'y'. Then navigate to your persistent storage

directory:
“`
cd /live/persistence/TailsData_unlocked
“`
Open or create the `live-additional-software.conf` file with gedit:
“`
gedit live-additional-software.conf
“`
In the newly opened file, add the package name:
“`
gpa
“`
Save and close gedit. Although gedit may display warnings, they can be disregarded. Normally, software installed via apt-get is not retained after shutdown, necessitating reinstallation upon next boot. However, by configuring apt persistence and listing packages in `live-additional-software.conf`, the system will automatically reinstall these packages at each startup without significantly delaying the boot process. A notification will appear once the installation is complete, indicating “Your additional software / The upgrade was successful”.
To launch the GPA PGP client, navigate through Applications -> Accessories -> GNU Privacy Assistant.

Troubleshooting Common Issues

Encountering challenges with Tails, from installation hiccups to boot problems, is not uncommon. The DNM bible offers several strategies to troubleshoot and resolve these issues effectively. Here’s a consolidated guide to assist you:

- **Secure Boot:** Verify if secure boot is disabled in your BIOS settings, as it’s a frequent impediment to Tails functioning correctly.
- **Known Hardware Conflicts:** Check the list of known issues on the Tails website for any hardware you’re using (like specific USB brands or network cards) and apply any provided solutions. Testing Tails on a different computer can help determine if the issue is hardware-specific.
- **Tor Connectivity Problems:** If Tor isn’t ready or you’re facing internet connection issues, try waiting 5 to 10 minutes after logging into Tails before rechecking. Persistent issues may require a reboot, or disabling MAC address spoofing through the Tails greeting screen’s “More Options”.
- **Password Recognition Issues:** Ensure the correct keyboard layout is selected at the Tails greeting screen, as incorrect settings can lead to password mismatches.
- **Boot Issues Despite Correct Instructions:** Confirm your USB stick isn’t listed under problematic devices on the Tails website.
- **Tails Freezing at Boot:** If Tails freezes post-selection in the boot menu, allow the countdown to complete without interaction. Repeated freezing

upon startup may resolve after several reboots.

- **Persistent Blue Screen Freezes:** Entering specific commands at the initial boot menu (nouveau.modeset=0, modeset.blacklist=nouveau, nosplash) can bypass this issue, though it requires repetition at each startup.
- **Persistence Access Issues:** Reconfiguring your persistence settings via Applications > Tails > Configure persistent volume might restore access.
- **Mac-Specific Booting Issues:** Mac users struggling to boot Tails might need to install rEFInd and temporarily disable SIP to facilitate the installation process.
- **WiFi Connection Troubles:** Continuous password prompts despite correct entry might indicate driver recognition problems, solvable by using a compatible WiFi adapter or an Ethernet connection.
- **Installer Functionality:** If the Tails installer fails to respond, exploring alternative installation methods or troubleshooting steps is recommended.
- **Cloning Authentication Password Request:** A workaround involves preparing the target USB with a specific file system format before cloning if prompted for authentication.
- **Screen Resolution Adjustments:** Solutions for resolution-related issues are available within the Tails documentation.
- **Mac Installation/Booting Difficulties:** Specific steps tailored for Mac users can aid in successfully installing or booting Tails.
- **Missing Top-Right Screen Icons:** This graphical glitch has recognized fixes detailed in Tails resources.
- **Live System Medium Error:** Altering the USB creation method or partition scheme, as well as attempting a second boot after a complete shutdown, may resolve booting errors.

For further details on each point, including step-by-step solutions, refer to the comprehensive troubleshooting section.

Whonix

When you should use this guide?

This section of the DNM bible introduces Whonix as a secure alternative for users who may encounter issues with Tails or seek different options. While Tails is often recommended for its ease of use and speed, Whonix presents a robust alternative for those who find Tails challenging, despite exploring solutions through online searches, and specialized forums. Whonix offers a secure setup without resorting to less secure options like Windows, which is humorously referred to as a “get-in-jail-free card.”

Important Update: Previously, Ubuntu was suggested as the host operating system for running Whonix. However, following recommendations from Whonix developers, Ubuntu has been deprecated in favor of more secure alternatives.

Despite Ubuntu being a better option than Windows or Mac, switching to Debian or other Linux distributions offering Full Disk Encryption (FDE) is advised for enhanced security.

Guide Overview

This guide is tailored for users installing Whonix on Linux distributions known for their security features, such as Debian, Manjaro, or Linux Mint, particularly those supporting FDE. For newcomers to Linux, Debian or Linux Mint are recommended for their user-friendly nature and extensive support resources.

Critical Advice: Avoid running Whonix on Windows or OS X, as these operating systems compromise operational security.

While integrating Qubes with Whonix can offer heightened security, this setup is geared towards more technically proficient users or those with high-security needs. This guide focuses on utilizing Whonix without Qubes, with information on Qubes integration expected in future updates.

What is Whonix?

Whonix operates as a secure, Tor-integrated Linux OS, designed to run within another OS (your host OS). For example, you might boot Ubuntu from a USB stick and run Whonix within Ubuntu. Described by its developers, Whonix is crafted for advanced security and privacy, countering potential threats while remaining user-friendly. It leverages the Tor network across a Debian-based system running inside virtual machines, providing a robust defense against malware and IP leaks. With pre-installed, pre-configured applications, Whonix allows for secure browsing, application installation, and customization without compromising security. It stands as the only OS developed specifically to be run in a VM alongside Tor.

For detailed information and further guidance, visiting the Whonix website is recommended.

Setting Up Your Host Operating System for Whonix

Before you can embark on using Whonix, selecting and installing a host operating system (OS) is a prerequisite. This host OS serves as the foundation upon which Whonix operates, akin to running a program, with the distinction that Whonix is an entire OS in itself.

For those less familiar with technical intricacies, Manjaro, Debian, or Linux Mint come highly recommended. Each of these options provides a user-friendly interface and robust support. To install Debian, follow the designated instructions, or refer to the respective guides for Manjaro and Linux Mint. A critical step in the installation process is ensuring the full encryption of your device. Opt for “Guided – use entire disk and set up encrypted LVM” during the OS setup to secure your host OS effectively.

Tip: For optimal performance, consider using an external SSD or, at the very least, a USB 3.0 stick as your installation medium.

Post-installation, it’s crucial to regularly update both your host OS and its installed software. Neglecting updates can expose your system to vulnerabilities, compromising your security. The DNM bible underscores the importance of maintaining your system to ensure a secure and efficient Whonix experience.

Setting Up Whonix

In preparation for installing Whonix, it's essential to understand that Whonix is not a singular operating system but comprises two distinct parts: the Whonix Gateway and the Whonix Workstation. Your direct interactions, including web browsing with the Tor browser and decrypting PGP messages, happen within the Workstation. This Workstation then communicates with the Gateway, which in turn connects to the Tor network, routing all your internet traffic through it for enhanced security. This setup effectively means you're operating three systems simultaneously: your chosen host OS (like Debian), the Whonix Gateway, and the Whonix Workstation. Unlike a traditional setup where only one OS can be run at a time, VirtualBox allows for the simultaneous operation of multiple systems. While this might sound complex, the process is straightforward if you follow the guided steps.

For the installation of Whonix, refer to the detailed instructions provided on their official page. During the "Install Whonix" phase, access the terminal with CTRL + ALT + T and input the commands as directed in the guide.

A critical step in the process, as highlighted in the guide, involves verifying the integrity of the Whonix download to ensure its authenticity. Additionally, for security reasons, you must change the default "changeme" password on both the Whonix Workstation and Gateway to maintain a secure environment.

Starting and shutting down Whonix

Starting

Begin by launching the Whonix-Gateway. In VirtualBox, locate the Whonix-Gateway and either click the prominent Start button or double-tap its listing on the left side.

Usability Tip: Once activated, consider enlarging the window sizes of both the Gateway and Workstation for a better interface experience.

After the desktop environment becomes visible, indicating a successful load, initiate a terminal session by double-clicking the terminal icon on the desktop. Here, you'll change your initial password by entering:

"`

passwd user

"`

Upon prompt, replace:

- The default username, which is `user`
- The default password, `changeme`, with a new password of your choosing. While it need not be overly complicated, avoiding the default password is advisable for security reasons.

Keyboard Layout Adjustment: To modify the keyboard layout, navigate through the Start menu located at the bottom left corner, proceed to Computer -> System Settings -> Input Devices, and select the "Layouts" tab. Here, ensure "Configure layouts" is enabled, then "Add" your preferred layout. It's recommended to remove the English (US) layout default and finalize your settings with "Apply".

Command Tip: For ease, commands can be copied and pasted directly into the

terminal window either by right-clicking and selecting paste or using the keyboard shortcut CTRL + SHIFT + V.
Continue by updating your system with the following terminal commands:
“`
sudo apt-get update && sudo apt-get dist-upgrade
“`
This action ensures your system is current with the latest updates and security patches, reinforcing the security framework for operating Whonix efficiently.
Important: Whonix diligently performs checks every 24 hours to identify if there are any updates needed for the software installed on both the Gateway and Workstation.
To update, simply copy this command, launch the terminal as guided, paste the command, and execute it by pressing ENTER. The system will prompt you with a confirmation message:
“`
Do you want to continue? [Y/n]
“`
Respond with ‘y’ and ENTER, then patiently wait for the process to complete, signified by the prompt returning to `user@host:~$`. At this point, it’s safe to close the terminal and restart both the Whonix Gateway and Workstation.
Updates might occur for either the Gateway or Workstation independently. If so, just apply the updates as instructed without concern. Should there be any issues with the update process, a simple reboot of both the Gateway and Workstation might resolve the issue, allowing for a fresh attempt at the update command.
Even if no updates are found, indicating your system is current, an informational message will still display, reassuring you of your system’s status.
Once updates are completed, navigate back to your host OS’s VirtualBox interface, select the Whonix-Workstation, and initiate it to revisit the steps outlined in the DNM bible’s “Starting Whonix” section within your Workstation environment.
Remember, password changes for both the Gateway and Workstation are required only once and not after each reboot.
Following the update process, it’s time to install the Tor Browser by double-clicking its desktop icon and selecting the appropriate version. Avoid alpha (‘a’) or beta (‘b’) versions to steer clear of unreleased features and potential bugs.
Upon installation, adjust the Tor Browser’s security settings by setting the security slider to high for an optimized security posture, a practice also recommended for Tails users but applicable and retained in Whonix to disable JavaScript globally, ensuring safer DNM interactions.
JavaScript (JS) now globally disabled, your setup aligns with the security protocols recommended for DNM activities.
User Interface Customization Tip: In the upper right corner of your screen, click the icon displaying three horizontal bars to access the “Customize” menu. Here, you can easily drag bookmarks and download icons to your menu or toolbar for quick access. Finalize your customization by selecting “Exit Customize” found

within the green box at the bottom right.

Shutting down

When concluding your Whonix session, adhere to a specific shutdown sequence for optimal security:

1. **Workstation Closure:** Begin by shutting down the Whonix-Workstation.
2. **Gateway Shutdown:** Follow by turning off the Whonix-Gateway.
3. **VirtualBox Closure:** Once both VirtualBox instances are closed, proceed to exit VirtualBox itself.
4. **Host OS Shutdown:** Complete the process by powering down your host operating system.

For those operating a terminal-based version of the Gateway, particularly for enhanced performance, shutting down is straightforward:

```
sudo poweroff
```

Execute this command in the terminal and confirm with ENTER to power off the Gateway securely.

Optimizing Whonix Performance

Managing the operation of three systems simultaneously — your host OS, Whonix Gateway, and Whonix Workstation — can demand a significant portion of your computer's resources, particularly when running from a USB stick instead of a faster internal SSD. Here are several performance enhancement tips for your Whonix setup. These suggestions are optional and best applied if you're experiencing performance lags. If your system runs smoothly, it's advisable to stick with your current setup to avoid unnecessary adjustments.

Before implementing any performance tweaks, ensure you've adequately set up your Whonix following the guidelines in previous chapters. This ensures you're optimizing a secure environment without compromising your setup or needing to restart the configuration process, especially critical for those avoiding the use of Whonix on less secure operating systems like Windows.

Important Reminder: Adjustments involving VirtualBox settings for your VMs — specifically the Whonix Gateway and Workstation — necessitate that these VMs be powered down first. Therefore, initiate only your chosen Linux distribution (such as Ubuntu or Linux Mint) that serves as the foundation for running Whonix, without launching the Whonix VMs themselves.

Optimizing Workstation CPU Utilization

Given the Whonix Workstation's role in handling extensive tasks, optimizing CPU allocation is essential for maintaining smooth performance. To adjust CPU settings for the Workstation within VirtualBox, follow these steps from the DNM bible:

1. Open VirtualBox and right-click on "Whonix-Workstation" listed on the left pane.
2. Choose "Settings" and navigate to the "System" category.

3. In the System settings, switch to the “Processor” tab.

Here, you’ll find two adjustable sliders: “Processor(s)” and “Execution Cap”. Ensure the “Execution Cap” is set to 100 percent, indicating full utilization of the allocated CPU power. For the “Processor(s)” slider, if it’s active, adjust it to a mid-range value — for instance, set it at 2 for a system with a maximum of 4 CPUs, or 4 if the maximum is 8 CPUs.

Should the “Processor(s)” slider appear inactive, a simple BIOS or UEFI adjustment is required. This involves enabling “VT-x technology” or a similarly named virtualization feature. While this might seem daunting, it’s a straightforward process that can significantly enhance performance. Here’s a brief overview:

- Access your BIOS/UEFI settings during boot-up (commonly by pressing a key such as F2, F10, DEL, or ESC, depending on your computer).
- Locate the virtualization option, often labeled as “Virtualization Technology (VT-x)” or simply “Virtualization”.
- Enable this feature, save your changes, and restart your computer.

Upon reboot with these new settings activated, the previously disabled “Processor(s)” slider in VirtualBox should now be adjustable. Follow the initial instructions to allocate the appropriate number of CPUs to your Whonix Workstation, optimizing its performance as recommended in the DNM bible.

Optimizing Gateway RAM Usage

To enhance your computer’s overall performance while running Whonix, consider reducing the RAM allocated to the Whonix-Gateway. This step, as recommended in the DNM bible, can help lighten the workload on your system. Before making any adjustments, review the initial guidelines, then proceed with modifying the settings in VirtualBox.

1. Navigate to the VirtualBox interface, right-click on the **Whonix-Gateway** listed on the sidebar, and select **Settings**.
2. Under the **System** category, locate the **Base Memory** slider within the **Motherboard** tab. According to guidelines, the Gateway can function with a minimum of 256 Megabytes of RAM. It’s advisable to allocate slightly more than this minimum, around 300 MB, to maintain a balance between performance and functionality. Adjust further based on the performance of both the Gateway and Workstation.

Post-adjustment, the Gateway operates in a terminal-based mode, conserving resources without compromising its operational capabilities.

Utilizing the Gateway

Upon starting the Gateway and reaching the login prompt, enter the default credentials (“**user**” for username and “**changeme**” for password). When the Gateway checks for updates, it temporarily overrides the command line, displaying update progress instead of the prompt. Await the completion of this process, indicated by a return to the normal command prompt.

Should you encounter a message indicating available updates, execute:

“`

```
sudo apt-get update && sudo apt-get dist-upgrade
```
Confirm updates by pressing ENTER or typing ‘y’ followed by ENTER, as the system prompts. This step is crucial for maintaining security and functionality.
Simplified Update Command Application
For applying updates, you can copy the command directly from the update notification by highlighting, right-clicking to copy, and then pasting it into the terminal with a right-click. This method streamlines the update process compared to the more interactive update notifications experienced on the Workstation.
Shutting Down the Gateway
To power down the Gateway, simply input:
```
sudo poweroff
```
and confirm with ENTER. This command efficiently closes the Gateway, ensuring a secure and orderly shutdown as outlined in the DNM bible, preserving the integrity of your setup.

Switching to an SSD

For those running Ubuntu or Linux Mint as part of their Whonix setup, upgrading to an SSD from a traditional USB stick could greatly enhance your system’s performance. SSDs are known for their rapid data access speeds, offering a noticeable improvement in operational efficiency. Affordable external SSDs with modest storage capacities—50 to 75 Gigabytes—are ample for your needs and readily available online or at retail outlets. Should an SSD upgrade not be feasible, opting for a USB 3.0 flash drive used in conjunction with a USB 3.0 port is a viable alternative, providing superior performance compared to older USB 2.0 technology.

Qubes/Whonix

This section of the DNM bible delves into the sophisticated setup of Qubes/Whonix, a combination not typically recommended for beginners. For those new to privacy-focused operating systems or less confident in their technical skills, starting with Tails might be more appropriate.

Understanding Qubes

Qubes OS is a free, open-source operating system designed for secure single-user computing. It utilizes Xen-based virtualization to facilitate the creation and management of isolated compartments, known as Qubes. These virtual machines can host a variety of isolated applications for personal, professional, or security purposes, including network management and firewalling. Qubes can run either full operating systems or minimalistic ones, depending on the user’s needs, with trust levels set according to each Qube’s specific role.
A key feature of Qubes is its template system, which simplifies the installation of commonly used Qubes for privacy enhancement. These templates can be configured as either disposable or persistent, tailoring to different operational requirements. For more detailed information, Qubes’ introductory resources at

qubes-os.org/intro are highly recommended.

Whonix: A Privacy Fortification

Whonix is celebrated as one of the most secure operating systems for privacy, operating on a dual-OS model to ensure comprehensive anonymity online. It achieves this by routing all internet traffic through the Tor Network, offering a level of privacy unattainable with VPNs, which, despite their speed and ease of use, fall short in terms of anonymity due to potential logging by VPN administrators. Whonix comprises two separate operating systems:

- **The Gateway OS**: Dedicated to routing all traffic through Tor and acting as a robust firewall.
- **The Workstation OS**: Where applications are run securely, with internet connections routed through the Gateway.

In a move to streamline privacy-focused computing, Whonix has been bundled with Qubes, offering an integrated solution for enhanced security.

Prerequisites for Qubes/Whonix Setup

- **Minimum RAM**: 8GB, with 16GB recommended for optimal performance.
- **CPU Requirements**: Support for virtualization technology (VT-x with EPT, AMD-V with RVI, Intel VT-d, or AMD-Vi [AMD IOMMU]).
- **Storage Space**: At least 32GB of free storage.
- **USB Drive**: 8GB or larger for installation purposes.

Adhering to these prerequisites ensures a smoother setup and operation of your Qubes/Whonix system.

Setting Up Qubes

Downloading and Preparing Installation Media

1. Visit qubes-os{dot}org to acquire the most recent ISO version.
2. Transfer the ISO file to a USB drive for installation purposes.
3. Initiate your computer from the installation USB to start the setup process.

Proceeding with Qubes Installation

- Prior to installation on your chosen storage medium, adhering to DoD standards for data destruction is advised to ensure maximum security.
- When the boot menu appears, opt for ‘Test Media and Install Qubes OS X.X.X’.
- Choose your preferred language and keyboard configuration.
- In the ‘Installation Destination’ section under system settings, opt for auto-configuration unless custom partitioning is necessary.
- Opt for ‘I would like to make additional space’, then select ‘Encrypt My Data’.
- Creating a Disk Encryption password will be prompted upon clicking ‘Done’; it’s crucial this password is lengthy yet memorable.
- Safeguard your Disk Encryption Password.
- Proceed with ‘Delete All’ followed by ‘Reclaim Space’ to remove existing

partitions.
- Set your timezone by navigating back to the main menu, then to ‘Date & Time’.
- It’s recommended to keep the root account disabled for security purposes.
- Create a user account, ensuring the password is robust and distinct from your disk encryption password.
- Returning to the main installation window, initiate the installation by clicking ‘Begin Installation’.
- Await the completion of the Qubes OS setup.
- Following a successful installation, opt to ‘Reboot System’, completing the process.

Configuring Qubes OS

- Upon starting Qubes, ensure the Hypervisor is enabled for secure entry.
- Decrypt your disk as prompted to access the main Qubes OS selection.
- Choose the Qube templates you wish to install, such as Fedora 36, Debian 11, or Whonix, tailored to your preferences and needs.
- Activate the option to use the sys-net qube for networking and USB device management.
- Opt for system and template updates via the Tor anonymity network with Whonix for enhanced security.
- Conclude the setup by selecting ‘Done’ followed by ‘Finish Configuration’, and patiently await the installation of default templates, noting that occasional freezing is normal.

Familiarizing Yourself with Qubes Desktop

- Log into your established user account to explore the Qubes environment
- The Qube Manager Tray, identified by a blue cube icon at the top-right, allows for monitoring and management of your qubes.
- Utilize the Qube Manager for creating, deleting, and configuring your qubes as needed.
- Access various tools and isolated application qubes from the System Menu at the top-left.
- Manage connected devices and configure passthrough permissions for specific qubes via the Qubes Devices menu, noting that USB passthrough is restricted by default for security.
- The Network Manager, also at the top-right, facilitates connections to WiFi and ethernet networks.

Network Device Configuration

- Open the Qube Manager and shutdown the sys-net qube to adjust settings.
- In the sys-net qube’s settings, navigate to the devices tab to find your

USB controllers, keeping this window open until changes are finalized.
- Assign necessary USB controllers to the right panel for activation, advised only if essential for USB storage or network adapters.
- Apply changes cautiously; improper USB passthrough configuration might disable internal USB peripherals like keyboards, potentially compromising your setup. Incrementally adjust USB passthrough settings, restarting sys-net after each change to ensure internal peripherals function correctly.
- Restart the sys-net qube and await its initialization for network adapter access.
- Proceed to connect to the internet, ensuring all configurations are securely applied.

Updating Qubes OS

- Access the Terminal Emulator from the System Menu located in the top-left corner of your screen.
- Execute the update command appropriate for your Qubes OS version.

For Qubes R4.0 and earlier versions, use:

```
sudo qubes-dom0-update
```

For Qubes R4.1 and subsequent versions, input:

```
sudo qubes-dom0-update –show-output –console
```

- Initially, this command might not succeed, potentially triggering a Connection Wizard pop-up to adjust your internet settings for Whonix.
- Retry the update command after configuring your connection. Note that updates via the Tor Network can significantly extend the update duration.
- When the update process prompts for package verification, type Y to proceed. Defaulting to NO will necessitate restarting the update procedure.

Installing Essential Software in Whonix Template

For enhanced security and functionality within Whonix, installing additional software is recommended:

- Navigate to the System Menu, locate the Template: whonix-ws-XX, and launch the XFCE terminal.
- Begin by updating the Whonix template with:

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

To incorporate PGP encryption capabilities, install Kleopatra with:

```
```

```
sudo apt-get install kleopatra
```
Conclude by closing the XFCE terminal.

Setting Up VeraCrypt on Debian-11 Qube

To enhance your security setup with VeraCrypt encryption tools, follow these steps, noting that this process is specifically for a **debian-11 qube** within Qubes OS.

Preparing VeraCrypt Installation

1. Access the terminal from the System Menu under the Template: debian-11.
2. Update the system template with the commands:

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

Downloading and Installing VeraCrypt

1. Navigate to www.veracrypt.fr to obtain the VeraCrypt download link for Debian 11. Ensure to verify the PGP signatures of the download to maintain security integrity.
2. Use the wget command to download VeraCrypt, replacing `VERACRYPT_DOWNLOAD_LINK` with the actual link:

```
wget VERACRYPT_DOWNLOAD_LINK -o vc.deb
```

Proceed with the installation of the downloaded .deb package:

```
sudo dpkg -i vc.deb
```

If the installation prompts any errors, resolve them with:

```
sudo apt-get –fix-broken install
sudo dpkg -i vc.deb
```

Configuring Software in Whonix Template

1. In the Qube Manager, locate the whonix-ws-XX template and access its Settings > Applications.
2. Add KeePassXC and Kleopatra to the selected applications by moving them to the right panel.
3. Apply the changes and confirm by clicking OK.
4. Shutdown the anon-whonix qube via the Qube Manager, then repeat the application configuration process for KeePassXC and Kleopatra, applying the changes.

Installing I2P

With Qubes OS correctly installed and configured, you’re now ready to set up and

utilize I2P for anonymous networking. Follow the dedicated guide for I2P installation and usage instructions.

Mobile Security Guide

This chapter of the DNM bible navigates the intricacies of utilizing mobile devices securely. It's critical to acknowledge that mobile devices are generally considered less secure for OpSec purposes, recommended only under exceptional circumstances. For comprehensive security, desktop operating systems like Tails or Whonix, equipped with essential tools such as PGP and XMR, are preferred.

Introduction to GrapheneOS

GrapheneOS stands out as a mobile operating system prioritizing privacy and security, featuring compatibility with Android apps. Its development is centered around enhancing privacy and security technologies, including advanced sandboxing, exploit mitigation, and a robust permission model.

Functionality of GrapheneOS

GrapheneOS distinguishes itself by fundamentally enhancing security and privacy. It employs a variety of technologies to address and mitigate vulnerabilities comprehensively, making exploitation more challenging. These enhancements not only secure the OS itself but also bolster the security of applications running on it. Importantly, GrapheneOS does not include Google apps or services, reinforcing its security posture.

Compatibility and Installation of GrapheneOS

GrapheneOS is specifically designed for Google Pixel devices, although it can be compiled for other devices from its source tree without modifications. Extending support to additional devices often requires significant effort to meet GrapheneOS's security standards. Due to hardware and firmware limitations, achieving a secure configuration on non-Pixel devices may be impractical. As of this writing, the following Pixel devices are officially supported:

- Pixel 7 Pro (cheetah) — experimental
- Pixel 7 (panther) — experimental
- Pixel 6a (bluejay)
- Pixel 6 Pro (raven)
- Pixel 6 (oriole)
- Pixel 5a (barbet)
- Pixel 5 (redfin)
- Pixel 4a (5G) (bramble)
- Pixel 4a (sunfish)
- Pixel 4 XL (coral)
- Pixel 4 (flame)

Security Features of GrapheneOS

GrapheneOS's security is not just surface-level; it's built into the very foundation of the operating system. Without any Google integration or bloatware, it leverages Android's native security features while introducing additional protections.

Features such as disk encryption, enhanced clipboard security, protection against hardware identifier tracking, IOMMU-based baseband isolation, and an integrated firewall with customizable rules, establish GrapheneOS as a formidable choice for users prioritizing security and privacy.

Installation

It's important to understand that mobile platforms generally offer inferior OpSec compared to dedicated systems like Tails or Whonix.

Installation Methods for GrapheneOS

GrapheneOS supports two main methods of installation, catering to different levels of technical expertise:

- **WebUSB-based Installer**: This is the preferred option for the majority of users, designed for straightforward and accessible installation.
- **Command Line Install**: Aimed at users with advanced technical skills, this method offers more control over the installation process.

Preparing for Installation

To ensure a smooth installation process, start by installing a compatible operating system on your device. Your system should have at least 4GB of RAM and 32GB of available storage space. The following operating systems are officially supported:

- **Windows**: Version 10 and 11
- **macOS**: Catalina (10.15), Big Sur (11), and Monterey (12)
- **Linux**: Arch Linux, Debian 10 (Buster), Debian 11 (Bullseye), Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS
- **Other**: ChromeOS, GrapheneOS, Google Android (stock Pixel OS), and certified Android variants

Before proceeding with the installation, make sure your operating system is fully updated to avoid any compatibility issues.

Starting the Installation

Supported Browsers

For the installation, use a browser compatible with the WebUSB feature, except for Ubuntu's Chromium due to its limitations. Recommended browsers include:

- **Chromium** (for non-Ubuntu systems)
- **Vanadium** (specific to GrapheneOS)
- **Google Chrome**
- **Microsoft Edge**
- **Brave**

Ensure your browser is current, and avoid using incognito or private browsing modes during the installation.

Enabling OEM Unlocking

- Activate developer options by navigating to Settings -> About this phone and tapping the build number repeatedly until developer mode is enabled.
- Within Settings -> Developer options, enable the OEM unlocking toggle.

Preparing Linux for Non-root Flashing
Specific to Arch Linux and Debian/Ubuntu, install necessary packages for device recognition:
For Arch Linux:
```
sudo pacman -Syy android-udev
```
For Ubuntu:
```
sudo apt-get install android-sdk-platform-tools-common
```
Booting into Bootloader

- Restart your device, holding down the volume down button during boot until it enters the bootloader interface.

Connecting Your Device

- Connect your phone to your computer. Linux users may need to reconnect if udev rules were not established beforehand.
- Windows users without fastboot drivers should install them now for Pixel devices or obtain the latest drivers.

Proceeding with Installation

- Visit the official GrapheneOS website, navigate to the install section, and select the web installer.
- Continue to the 'Unlocking the bootloader' section as instructed on the website.
- Follow the on-screen installation steps, noting that further detailed steps require interaction with the website's WebUSB commands.

Securing Your Device Post-GrapheneOS Installation

Following the successful installation of GrapheneOS, enhancing your device's privacy and security settings is crucial. Implement the following adjustments to fortify your setup:
Essential Privacy Settings

- **Disable Camera and Microphone Access**: Navigate to Settings -> Privacy and restrict access to both the camera and microphone to prevent unauthorized use.
- **Location Services**: Turn off location tracking by going to Settings -> Location -> Use location.
- **Auto Reboot Schedule**: Enhance security by setting an automatic reboot time via Settings -> Security -> Auto reboot.
- **Pin Scrambling**: Activate pin scrambling under Settings -> Security to add an extra layer of security during screen unlock attempts.
- **Screen Lock Camera Access**: Prevent camera access from the lock screen by disabling it in Settings -> Security.

App Store and Recommended Apps

After adjusting your settings, proceed to install F-Droid from your browser, serving as a reliable app store for open-source applications. Incorporate these recommended apps to elevate your device's functionality and privacy:

- **OpenKeychain**: Facilitates easy PGP encryption.
- **AuthPass**: A KeePass-compatible password manager.
- **InviZible Pro**: Enhances online anonymity and security.
- **Fennec F-Droid**: A privacy-focused web browser.
- **Tor Browser for Android**: Offers anonymous browsing via the Tor network.
- Explore F-Droid for FOSS (Free and Open Source Software) alternatives to conventional PlayStore applications.

Configure each app according to your privacy and security needs. For web browsing enhancements, specifically with Fennec, consider following additional setup guides for I2P browsing.

Final Thoughts

By completing these steps, you've significantly improved your mobile device's security posture. Remember, the effectiveness of these security measures largely depends on your vigilance with app installations, permission management, and active settings. Although using cellular services inherently compromises anonymity, employing a faraday bag or box can mitigate tracking risks.

Stay vigilant and regularly update your system with the latest patches from GrapheneOS. For comprehensive guidance and FAQs, the official GrapheneOS website is an invaluable resource.

KeePassXC

Securely Managing Credentials with KeePassXC

KeePassXC serves as a robust password management tool, designed to securely store your sensitive information such as usernames, passwords, and other confidential details. This utility features an integrated password generator, promoting the use of strong, unique passwords for each of your accounts to minimize the risk of unauthorized access by hackers or law enforcement. All your credentials are safely housed within an encrypted database, accessible solely through a master password. This singular password approach simplifies secure access to all your accounts, reducing the need to memorize multiple passwords.

Essential Data for KeePassXC Storage:

- **Market Accounts and Forum Logins**: Securely keep track of your usernames and passwords.
- **Cryptocurrency Seeds and Wallet Passwords**: Safeguard your digital currency access.
- **PGP Key Passwords**: Store passwords related to your PGP encryption keys securely.

Launching KeePassXC:

- **On Tails**: Navigate through “Applications” -> “Accessories” -> “KeePassXC” to open KeePassXC and start managing your passwords efficiently.
- **For Whonix Users**: KeePassXC is also integrated within Whonix, allowing you to use the same operational guidelines as provided for Tails users.

By adopting KeePassXC as recommended in the DNM bible, you enhance your operational security, ensuring your sensitive information is well-protected and easily accessible when needed.

Creating a KeePassXC database

To begin securing your passwords and sensitive information with KeePassXC, ensure you’ve first initialized and unlocked the persistent volume on your device. From the KeePassXC welcome screen, select ‘Create new database’. Alternatively, navigate through the menu bar by selecting “Database” -> “New database”.
It’s crucial to save your new database within the persistent volume. Neglecting this step means risking data loss upon restarting Tails.

Establishing a Master Password

- **Master Password Creation**: This step involves setting a robust master password, the key to accessing your entire database of secrets. Choose a password that’s both complex and resistant to brute-force attacks or guesswork by potential intruders. This password encapsulates the security of your entire database.
- **Mnemonic Passphrase**: For a strong yet memorable password, consider creating a mnemonic consisting of at least five words. The KeePassXC built-in passphrase generator can aid in this process. Access it by clicking the dice icon, select “Passphrase”, adjust your word count, and generate until a suitable passphrase is found. Utilize the “Copy” function to save your chosen passphrase, then exit the generator.
- **Memory Techniques**: To facilitate recall of your mnemonic, weave the words into a narrative or story. If there’s a concern about forgetting your master password, temporarily note it down on paper and store it securely until memorized.

After setting your master password, proceed by clicking “OK”.
It’s advisable to reboot Tails following these adjustments to verify that your database persists correctly on the volume and remains accessible.

Opening a KeePassXC database

To open your database, select “Open existing database”. Proceed to locate the directory containing your database file and double-click the .kdbx file to select it. Input your master password when prompted, then confirm by clicking “Ok” to gain access to your stored information.

Inserting New Entries in KeePassXC

Imagine you need to securely store the login details for a market account. Here’s

how to proceed in KeePassXC:

1. Start by selecting “Entries” -> “Add new entry”.
2. For the entry title, use the market’s name, and for the username, input your specific market username.
3. To create a strong password, click on the dice icon to the right of the password field. To view the generated password, click on the eye icon located directly below the dice icon.

Enhancing Your Password:

- Click on the button labeled “/*_…” next to the “0-9” button. This action introduces special characters into your password, significantly enhancing its strength. If satisfied with the generated password, click “Apply” to confirm your selection.

Verifying Your Password:

- To double-check the accuracy of your password, use the eye icon above the dice button. This will reveal the password you’ve chosen in both the “Password” and “Repeat” fields. Once verified, click “OK” to finalize the entry, which will then appear in your database list.

Always Save Changes: It’s crucial to save your database after making any modifications to ensure no data is lost.

For Tails users, KeePassXC automatically saves changes after each modification. However, when saving critical information, such as cryptocurrency seeds, take an extra step to confirm the database’s integrity. Close and reopen your KeePassXC database to check that your new entry has been correctly stored, safeguarding your valuable data.

Retrieving Your Stored Data

To access your saved credentials or other information within KeePassXC follow these steps:

1. Locate the desired entry, such as one labeled with your market’s name for which you wish to log in.
2. Right-click on this entry to unveil a context menu that offers options to copy either the username or password directly to your clipboard.

After copying, navigate to the corresponding site (like a registration or login page) and paste the copied information where required. Remember, KeePassXC is designed to automatically clear your clipboard after 10 seconds for security purposes, so prompt action is necessary.

For accessing additional details stored in an entry:

- Right-click on the entry again and select “Copy attribute to clipboard” to copy other stored attributes like URLs or notes.

To edit an entry:

- Double-clicking on an entry will open its editor window. Exercise caution in this mode to avoid inadvertently modifying any critical information.

PGP

General

With the release of Tails 5.0, the Tails development team updated the PGP encryption software used within the operating system. If you're operating on an older version of Tails, it's crucial to upgrade to the latest release to follow the modern encryption protocols. This guide is tailored for users of Tails version 5.0 and newer.

Understanding PGP

Pretty Good Privacy (PGP) stands as a cornerstone encryption tool, offering cryptographic security for digital communication. Its application spans encrypting, signing, and decrypting text, emails, and files, enhancing the confidentiality and integrity of email exchanges.

For users navigating the darknet, PGP serves multiple essential purposes:

- **Encrypting Messages**: Encrypt sensitive information, such as shipping addresses, ensuring that only the intended recipient, typically the vendor, can decrypt and read the message.
- **Decrypting Messages**: Vendors often send encrypted messages containing sensitive details like tracking codes, which require decryption on the recipient's end. Additionally, decryption is sometimes necessary for market login authentication.
- **Verifying Messages**: Validate the authenticity of market links to guard against phishing attempts, verifying that communications are legitimate and untampered.

The Importance of Mastering PGP

Grasping the functionality of PGP is imperative for safeguarding your personal information from unintended recipients, including law enforcement. The DNM bible strongly advises dedicating time to fully understand and proficiently utilize PGP encryption. To practice and refine your PGP skills, consider engaging with communities or resources dedicated to PGP practices.

By adhering to the guidance provided in the DNM bible and staying updated with the latest versions of Tails, you ensure a fortified layer of security for your digital communications, essential for maintaining privacy in the darknet realm.

FAQ on PGP Usage

Sending Messages Without PGP Encryption

Q: What should I do if I sent a message containing sensitive information without PGP encryption?

A: Immediately cease using the current market account and establish a new one. This measure is not excessive; historical seizures of platforms like Silk Road revealed numerous unencrypted messages with plaintext addresses. Law enforcement agencies have utilized such information to apprehend buyers. To mitigate risk, initiate a fresh market account dedicated to consistently encrypting sensitive data, such as addresses, with PGP. This practice, as emphasized in the DNM bible, prevents the accumulation of incriminating evidence.

Market’s Built-in Encryption Reliability

Q: Is it safe to rely on a market’s built-in encryption for messaging?

A: No. Messages processed through market’s built-in encryption are vulnerable to interception if the server is compromised, as the server handles messages in plaintext. Always encrypt sensitive content personally to ensure security.

Necessity of Encrypting All Messages

Q: Do all messages require PGP encryption?

A: Encrypt only messages that contain sensitive data, like addresses or packaging details, typically exchanged between a vendor and a buyer. Generic messages, such as expressing gratitude, do not necessitate encryption.

Decrypting Sent PGP Messages

Q: Can I decrypt a PGP message after I’ve sent it?

A: No, decryption is exclusively possible by the recipient who possesses the corresponding public key used for encryption. However, including your own public key alongside the recipient’s during the encryption process enables you to decrypt the message. Detailed instructions on this process are provided later in the guide.

PGP vs. GPG

Q: What distinguishes PGP from GPG?

A: The differences between PGP (Pretty Good Privacy) and GPG (GNU Privacy Guard) are delineated in the specified section.

Adhering to these guidelines from the DNM bible ensures that your communications on darknet platforms remain secure, minimizing the risk of exposure to unauthorized parties.

Generating a PGP Key Pair

Creating a PGP key pair is a fundamental step in securing your digital communications. This process yields two distinct keys: a public key, which you can share freely, and a private key, which must remain confidential at all times. Your public key is used by others to encrypt messages intended for you, ensuring that only you, with your private key, can decrypt and read them.

Market Account Security

When registering on a marketplace, you may be asked to provide a public key. To safeguard your anonymity and prevent potential account linkages, it’s imperative to generate a new key pair for each new account you create. Reusing a public key across multiple accounts compromises your operational security.

Uploading your public key enables vendors to send encrypted information, such as tracking numbers for shipments, securely. Additionally, it can act as a form of two-factor authentication for market login procedures, where decrypting a message with a unique code each time you log in verifies your identity.

Managing Private Keys

It is crucial not to retain private keys that are no longer in use. If you register a new market account, ensure to delete the previous key pair and create a new one. Similarly, if a market faces legal action or executes an exit scam, promptly remove all associated keys. Limiting access to your private keys minimizes the risk of an attacker decrypting sensitive information.

Tails

- create a new key first Open application -> Accessories -> Kleopatra
- File -> New Keypair
- Create personal OpenPGP keypair
- Enter a name: Usually your account name for this key. **Not your real name!**

It’s advisable not to fill in the email field unless necessary. If email contact is preferred, ensure it meets the criteria outlined in the email section.

- Advanced Configuration
- Opt for the 4096-bit encryption over the 3072-bit option for enhanced security.
- Assign an expiration date for your key, typically one to two years ahead, to encourage regular updates of your key pair.

Important Consideration: An expiration date doesn’t inhibit the decryption of messages with the corresponding public key in the future. Should your private key be compromised, it remains vulnerable to decryption by unauthorized parties even post-expiration. The purpose of an expiration date is to act as a prompt for you to update your key pair regularly, thus reducing the risk associated with a single private key’s exposure. Upon updating your key pair, inform your contacts by signing your new public key with the old one, ensuring a seamless transition.
Key rotation primarily concerns keys used outside of marketplaces, such as those added to profiles on platforms like Dread. Market-related keys typically have shorter lifespans and shouldn’t be retained for extended periods.

- Click ok
- Next
- Create
- Enter a strong password
- You will now see a message box creating your keys. Once it is done you will see a notification letting you know it is finished.

Congratulations on setting up your PGP key pair, enhancing your digital security and privacy.

Finding your public key

To locate your public key, simply double-click on the newly created key’s name. Select the “Export” option. You’ll encounter a block of text resembling the following:

“`

——BEGIN PGP PUBLIC KEY BLOCK——

Version: GnuPG v2

mQGNBF0j2XYBDADsQj2L7HravPZHY622SSZ1sNOXeC+5gJED2W3VgJ0BpZYfW3Bq

JQFIPRfEJgz8LsuP4A8QwR8DWVQO5qEUN0pLDqJZzPqEd+V0AikN3KxQKbTIy3kL

5zyY5+QhO0qlJzK4V8ZvFpZUmYgDQUCPjYZ6c+KJUbK5xTIJN7BzRrJ3FWWj+mp

s
ay1uN2RwR2D9+HMIKSl0PhzKXIkH2PI8TnRiZGZqFy2h2ooMblO5H3sGkSgEdxpi
cCUFD2VJ3B3QePE3a3JQwz5Sh5PeJ8KHN0Q3VJbBq+GsDQDzjMvpH4gU5nS3E
3Sf
UkHr+vC/rqKxVrL5P/7LM5Vo5J8ARSzqD5K3JU3kYdWJw0J8Lb0+ZMdI5x9UjT3I
o3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9TeP4E0
AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHVwb25
0QGV4
YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJdI9l2
AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAxLkC
GyQM
AIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z0jMg
RXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSeq3sL
E2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45ndWJw0J8Lb0+ZMdI5x9U
jT3Io3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9Te
P4E0AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHV
wb250
QGV4YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJ
d
I9l2AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAx
LkC
GyQMAIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z
0jMgRXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSe
q3sLE2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45
——END PGP PUBLIC KEY BLOCK——
“`

Whonix

For optimal operational security, it’s recommended to use PGP keys of 4096 bits, as the GNU Privacy Assistant limits key creation to 3072 bits and lower. This process will be carried out in the terminal of the Whonix Workstation.
Generating a 4096-Bit Key in Terminal:

1. **Launch Terminal:** Open a new terminal window.
2. **Generate Key:** Input the command `gpg –full-generate-key`.
3. **Key Strength:** Select `1` for RSA and RSA (default) and specify `4096` for the key size.
4. **Expiration:** Decide on an expiration date for your key and confirm with `y`.
5. **Identity:** Enter a pseudonym for your key. Avoid using real names or any personal identifiers.
6. **Email:** Optionally add an email address or press Enter to bypass this step.
7. **Comment:** Add a comment if desired or skip with Enter.
8. **Review:** Confirm your details by typing `o` if all information is correct.

A password creation prompt will appear. Utilize KeePass to generate and securely store a password for this key set. Engaging mouse movements during this phase aids in the generation of your PGP key. Subsequently, your new key should be visible within the GNU Privacy Assistant.
Exporting Your Public Key:
To share your public key, navigate to the “Key Management” window in the GNU Privacy Assistant, right-click your key, and select the option to copy. This copies your public key, ready for pasting where necessary.
A typical public key format:
“`
——BEGIN PGP PUBLIC KEY BLOCK——
Version: GnuPG v2
mQGNBF0j2XYBDADsQj2L7HravPZHY622SSZ1sNOXeC+5gJED2W3VgJ0BpZYfW3
Bq
JQFlPRfEJgz8LsuP4A8QwR8DWVQO5qEUN0pLDqJZzPqEd+V0AikN3KxQKbTIy3k
L
5zyY5+QhO0qlJzK4V8ZvFpZUmYgDQUCPjYZ6c+KJUbK5xTIJN7BzRrJ3FWWj+mp
s
ay1uN2RwR2D9+HMlKSl0PhzKXIkH2Pl8TnRiZGZqFy2h2ooMblO5H3sGkSgEdxpi
cCUFD2VJ3B3QePE3a3JQwz5Sh5PeJ8KHN0Q3VJbBq+GsDQDzjMvpH4gU5nS3E
3Sf
UkHr+vC/rqKxVrL5P/7LM5Vo5J8ARSzqD5K3JU3kYdWJw0J8Lb0+ZMdI5x9UjT3I
o3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9TeP4E0
AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHVwb25
0QGV4
YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJdI9l2
AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAxLkC
GyQM
AIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z0jMg
RXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSeq3sL
E2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45ndWJw0J8Lb0+ZMdI5x9U
jT3Io3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9Te
P4E0AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHV
wb250
QGV4YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJ
d
I9l2AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAx
LkC
GyQMAIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z
0jMgRXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSe
q3sLE2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45
——END PGP PUBLIC KEY BLOCK——
“`
Note that the actual key content will be more extensive than shown.

Important Consideration: An expiration date for your key doesn't inhibit the decryption of previously encrypted messages. It acts as a cue for key rotation, minimizing the risk associated with prolonged use of a single key pair.

Importing a public key

To send encrypted messages, such as your address to a vendor, you'll need to obtain their public key. This can typically be found on the vendor's profile page, often labeled as "PGP key" or "Vendor public key." Sometimes, the key may be directly displayed on their profile.

Here's an example of what a public key might look like:

```
—–BEGIN PGP PUBLIC KEY BLOCK—–
Version: GnuPG v2
mQGNBF0j2XYBDADsQj2L7HravPZHY622SSZ1sNOXeC+5gJED2W3VgJ0BpZYfW3
Bq
JQFlPRfEJgz8LsuP4A8QwR8DWVQO5qEUN0pLDqJZzPqEd+V0AikN3KxQKbTly3k
L
5zyY5+QhO0qlJzK4V8ZvFpZUmYgDQUCPjYZ6c+KJUbK5xTIJN7BzRrJ3FWWj+mp
s
ay1uN2RwR2D9+HMIKSl0PhzKXIkH2Pl8TnRiZGZqFy2h2ooMblO5H3sGkSgEdxpi
cCUFD2VJ3B3QePE3a3JQwz5Sh5PeJ8KHN0Q3VJbBq+GsDQDzjMvpH4gU5nS3E
3Sf
UkHr+vC/rqKxVrL5P/7LM5Vo5J8ARSzqD5K3JU3kYdWJw0J8Lb0+ZMdI5x9UjT3I
o3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9TeP4E0
AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHVwb25
0QGV4
YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJdI9l2
AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAxLkC
GyQM
AIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z0jMg
RXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSeq3sL
E2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45ndWJw0J8Lb0+ZMdI5x9U
jT3Io3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9Te
P4E0AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHV
wb250
QGV4YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJ
d
I9l2AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAx
LkC
GyQMAIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z
0jMgRXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSe
q3sLE2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45
—–END PGP PUBLIC KEY BLOCK—–
```

Tails

To import a public key using Kleopatra, follow these steps:

1. Select the notepad icon to open a new text field.
2. Copy and paste the public key you wish to import into this field.
3. Choose the option to import from the notepad.
4. A notification will appear, prompting you to certify the imported key.
    - If confident in the key's authenticity, proceed by clicking 'Yes', then 'Certify'.
5. A confirmation message, 'Certified successfully', will display upon successful certification.
6. Return to your keyring by selecting the notepad icon once more, where you'll find the imported key listed by name.

Whonix

To import a public PGP key into GPA, follow these steps:

1. Locate and copy the desired public key to your clipboard.
2. Open a text editor, such as Mousepad, and paste the public PGP key into a new document.
3. Save this document with a name like "vendor.asc".
4. Launch GPA and select the option to import keys.
5. In the window that appears, navigate to and select the file you've just saved containing the public PGP key.
6. Upon successful import, a confirmation message will be displayed. Close this window by clicking "OK".

Next, verify the key has been added to your list of PGP keys:

1. Locate the newly imported key in your GPA key list.
2. Right-click on the key and choose "Key Properties".
3. In the "Owner trust" field, change the setting to "Ultimately" using the dropdown menu, then confirm by clicking "OK". This adjustment streamlines the process of encrypting messages for the corresponding vendor.

Troubleshooting:

- If you encounter an error stating "Key importing failed...", the issue likely stems from a formatting error in the key. Ensure you include the complete key in your copy, including the "—–BEGIN PGP PUBLIC KEY BLOCK—–" and "—–END PGP PUBLIC KEY BLOCK—–" lines, as well as the five dashes at both the beginning and end. PGP keys require precise formatting to be recognized and imported correctly.

Encrypting a message with PGP

Always personally encrypt sensitive information using PGP. Relying on a market or third-party service for encryption is not secure.

Tails

To securely send a message using PGP, you must first have the recipient's public key imported, enabling you to encrypt messages meant for them.
Here's how to do it using Kleopatra:

1. **Launch Kleopatra** and select the Notepad feature.
2. **Compose Your Message**: Enter your message into the text area provided.
3. **Navigate to Recipients**: Switch to the Recipients tab.
4. **Uncheck "Sign As"**: Opt out of signing the message if preferred.
5. **Encrypt for Yourself**: If you wish to access this message later, ensure "Encrypt for me" is checked and select your key. This step is optional; skipping it means only the intended recipient can decrypt the message.
6. **Encrypt for the Recipient**: Select "Encrypt for others" and enter the recipient's name as it appears on their public key.
7. **Encrypt the Message**: Click on "Encrypt Notepad". A confirmation, "Encryption succeeded," will appear, alongside additional details.

Upon returning to the Notepad tab, you'll find your message encrypted, looking something like this:
"`
——BEGIN PGP PUBLIC KEY BLOCK——
Version: GnuPG v2
mQGNBF0j2XYBDADsQj2L7HravPZHY622SSZ1sNOXeC+5gJED2W3VgJ0BpZYfW3Bq
JQFlPRfEJgz8LsuP4A8QwR8DWVQO5qEUN0pLDqJZzPqEd+V0AikN3KxQKbTIy3kL
5zyY5+QhO0qlJzK4V8ZvFpZUmYgDQUCPjYZ6c+KJUbK5xTIJN7BzRrJ3FWWj+mps
ay1uN2RwR2D9+HMlKSl0PhzKXlkH2Pl8TnRiZGZqFy2h2ooMblO5H3sGkSgEdxpi
cCUFD2VJ3B3QePE3a3JQwz5Sh5PeJ8KHN0Q3VJbBq+GsDQDzjMvpH4gU5nS3E3Sf
UkHr+vC/rqKxVrL5P/7LM5Vo5J8ARSzqD5K3JU3kYdWJw0J8Lb0+ZMdI5x9UjT3Io3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9TeP4E0AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHVwb250QGV4
YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJdI9l2
AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAxLkCGyQM
AIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z0jMg
RXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSeq3sL
E2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45ndWJw0J8Lb0+ZMdI5x9U
jT3Io3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9Te
P4E0AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHVwb250

QGV4YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJd
I9I2AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAxLkC
GyQMAIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z
0jMgRXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSe
q3sLE2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45
—–END PGP PUBLIC KEY BLOCK—–
“`

Note: The “gibberish” portion, your encrypted message, will typically be longer. Finally, copy this encrypted message and paste it into the desired communication platform (marketplace or email service) in the appropriate message field and send it. This process ensures that only the holder of the corresponding private key can decrypt and read your message.

Whonix

To securely send a message using PGP, you must first have the recipient’s public key imported, enabling you to encrypt messages meant for them.
Launch GPA and navigate to the clipboard option to begin the encryption process for your message, such as your address.

1. **Input Your Message**: Type the text you wish to encrypt directly into GPA.
2. **Initiate Encryption**: Click on the encryption icon to proceed.

A dialog box will appear, prompting you to select the recipient of your encrypted message. Confirm your choice by clicking “OK”. If you encounter a warning about an “unknown key,” it indicates that the trust level for the key wasn’t set during importation. If you trust the key, proceed by selecting “Yes.”
Upon successful encryption, the text in the editor will be transformed into an encrypted format, resembling the following structure:
“`
—–BEGIN PGP PUBLIC KEY BLOCK—–
Version: GnuPG v2
mQGNBF0j2XYBDADsQj2L7HravPZHY622SSZ1sNOXeC+5gJED2W3VgJ0BpZYfW3Bq
JQFlPRfEJgz8LsuP4A8QwR8DWVQO5qEUN0pLDqJZzPqEd+V0AikN3KxQKbTIy3kL
5zyY5+QhO0qlJzK4V8ZvFpZUmYgDQUCPjYZ6c+KJUbK5xTIJN7BzRrJ3FWWj+mps
ay1uN2RwR2D9+HMlKSl0PhzKXlkH2PI8TnRiZGZqFy2h2ooMblO5H3sGkSgEdxpi
cCUFD2VJ3B3QePE3a3JQwz5Sh5PeJ8KHN0Q3VJbBq+GsDQDzjMvpH4gU5nS3E3Sf
UkHr+vC/rqKxVrL5P/7LM5Vo5J8ARSzqD5K3JU3kYdWJw0J8Lb0+ZMdI5x9UjT3Io3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9TeP4E0AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHVwb250QGV4
YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJdI9I2

AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAxLkC
GyQM
AIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z0jMg
RXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSeq3sL
E2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45ndWJw0J8Lb0+ZMdI5x9U
jT3Io3W3+ZUhVnkBj8ZqI/eM+KcF+jDs9vMzI+Mk3A7kSdI9I0W+UcN4FW6Lr9Te
P4E0AeLRR2EAEQEAAbQdTWFyaWUgRHVwb250IChOT05FKSA8bWFyaWUuZHVwb250
QGV4YW1wbGUuY29tPokB1AQTAQoAPhYhBBDZb4hJ5xS1BTTK1uMjI3mJAxLkBQJd
I9I2AhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEMjI3mJAx
LkC
GyQMAIBqAFvO5Vt9s3CiQPA7/u72C+SV1+HqPviYvLe8No8pfL+r2LXv4MQLVl5Z
0jMgRXkUpCQWIRHxF5Ujt0WGsRJSGeY8IYqP2T5HbTIq3kqJeBmStJbnj+tzBpSe
q3sLE2PPlL5C3EP286ZgGJ/lJq9LZ8Xl2WOK1+et2cIFFH45
—–END PGP PUBLIC KEY BLOCK—–
“`

Note that the encrypted message (“the gibberish in the middle”) will likely be longer in your case.

Important: Once encrypted, you cannot decrypt the message yourself unless you’re among the selected recipients. To read the encrypted message later, ensure you also select your own key as a recipient during the encryption process.

Following encryption, simply visit the intended platform (market or email service), paste the encrypted message into the message field, and send it.

Remember to close the clipboard window after completing these steps, securing your communication effectively.

Verifying a message with PGP

Verification of messages through PGP is a crucial step for confirming the authenticity of market links. Markets often release signed messages with links directing to their platforms. Possessing the market’s public key enables you to authenticate these messages, ensuring they indeed originate from the market and that the contained links are valid.

Additionally, market operators, vendors, and moderators frequently sign their announcements or alerts. Employing PGP verification for these communications further guarantees their legitimacy and source integrity.

Tails

To authenticate a PGP-signed message, you first need to acquire and **import** the public key of the individual who signed the message. This could be found on a vendor’s profile within the marketplace or on related community platforms.

Steps to Verify a PGP Signed Message:

1. **Importing the Public Key**: Locate the public key, often available on the signer’s market profile or official communication channels, and import it to your PGP software.
2. **Using Kleopatra**:

- Launch Kleopatra and select the Notepad feature.
- Copy the entirety of the PGP signed message and paste it into the provided text field. The message will typically start and end as follows:
  ```
  ——BEGIN PGP SIGNED MESSAGE——
  Hash: SHA512[Text of the PGP signed message.]——BEGIN PGP SIGNATURE——[PGP Signature]——END PGP SIGNATURE——
  ```

3. **Verification**:
   - Click on the “Decrypt/Verify” button to proceed with the verification process.
   - If the signature corresponds with a public key you’ve previously imported, and the message remains unaltered, Kleopatra will display “Valid Signature” in green, confirming its authenticity.
   - Should there be any modification to the message, even as minor as an additional letter or space, or if the signature does not match any imported key, a “Invalid Signature” alert in red will appear, indicating the message’s verification has failed.

This process ensures that you can confidently trust the authenticity of the message, verifying that it indeed comes from its purported source without any alterations.

Whonix

To authenticate a PGP-signed message, the initial step involves **importing** the public key of the individual who signed the message. This key can typically be found on locations such as the vendor’s profile on the marketplace or a dedicated subforum.

Process Overview:

1. **Locate and Import the Public Key**: Identify the public key’s location, for instance, on the vendor’s market profile or a specific community platform, and import it into your PGP software.
2. **Copying the PGP Signed Message**: The signed message will resemble the following format:
   ```
   ——BEGIN PGP SIGNED MESSAGE——Hash: SHA512[Content of the PGP signed message]——BEGIN PGP SIGNATURE——[PGP signature details]——END PGP SIGNATURE——
   ```
3. **Verification with GPA**:
   - Open GPA and navigate to the clipboard section.
   - Paste the entire signed message you’ve copied earlier into the clipboard.

    - Select the “Sign/Verify” option to initiate the verification process.

Should the verification be successful, a notification will appear indicating a “Good signature from [name of the key pair that signed the text]”. This confirms the integrity and origin of the signed message, verifying that it has not been tampered with and originates from the expected source.

Decrypting a message

Tails

- First open Kleopatra and click Notepad
- Copy and paste the PGP message into the text field
- Click Decrypt/Verify

Whonix

Launch GPA and navigate to the clipboard feature. Here, paste the encrypted message into the provided text area. Choose the decrypt option to proceed.
You’ll be asked to input the password associated with your key. After entering your password, the decrypted message will be displayed.

Signing a message with PGP

Signing a message with PGP is a process distinct from encrypting sensitive information like your address or private communications.
By signing a message, you authenticate it as your own creation. Anyone in possession of your public key can confirm your signature’s validity. While signing messages is typically not a requirement for standard DNM transactions, should the need arise, here’s how to proceed.

Tails

To sign a message with PGP using Kleopatra, follow these steps:

1. Launch Kleopatra and select the Notepad feature.
2. Enter the message you wish to sign in the text field.
3. Navigate to the Recipients tab.
4. Activate the option “Only sign as:” and specify the key you intend to use for signing.
5. Deselect “Encrypt for me” and “Encrypt for others.”
6. Choose “Sign Notepad,” then return to the Notepad tab.

Your message will now be formatted as a signed PGP message, resembling the following structure:

```
—–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—–
[PGP signature details]
—–END PGP SIGNATURE—–
```

The encrypted portion of your message will be more extensive. To share this signed message, simply paste it into the appropriate field on a marketplace or in an email and send it as needed.

Whonix

Initiate GPA and navigate to the clipboard feature. Enter the message you intend to sign within the text area. Upon completion, opt for the “sign the buffer text” option and select the key you wish to use for the signature. You’ll be prompted to input the password associated with your key.
Upon successful signing, the clipboard content will be formatted as follows:
“`
——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——
[PGP signature details]
——END PGP SIGNATURE——
“`
Note, the “gibberish” section, which is the actual signed part of the message, will likely extend further in your actual message. Now, simply proceed to the intended platform—be it a marketplace or an email service—paste the signed message into the appropriate area, and dispatch your message or email.
Conclude by closing the editor window, selecting “Discard” when prompted whether you wish to save the document, effectively completing the process of signing your message.

Cryptocurrencies

Cryptocurrency Usage

Cryptocurrencies are essential for transactions on the darknet, offering a means to purchase goods or services while striving to maintain anonymity. Among the various cryptocurrencies, Monero (XMR) is recommended for its enhanced privacy features. Whenever feasible, convert your assets to Monero to obscure their trail back to your identity. If starting with Bitcoin or Litecoin, consider converting them to Monero as a crucial step for privacy.

Key Points:

- **Public Ledger**: Remember, all Bitcoin and Litecoin transactions are public and traceable via the blockchain. Opt for Monero when initiating transactions for an added layer of privacy.
- **Conversion to Monero**: If your transaction requires Bitcoin or you initially possess Bitcoin/Litecoin, refer to guidelines on converting your funds to Monero to safeguard your anonymity.
- **Direct Transfers**: Avoid sending cryptocurrencies directly from an exchange to a vendor or marketplace. This practice can jeopardize your privacy and security.

Frequently Asked Questions:

Is converting to XMR essential? Aren't the fees high?

Absolutely, converting to XMR is crucial for maintaining privacy. Just as you wouldn't openly transact with a dealer in a risky environment, you shouldn't compromise your anonymity online. The necessity to use XMR is unequivocal.

How does the fluctuation in cryptocurrency prices affect DNM listings?

Market listings remain priced consistently in fiat currency terms. A $20 item remains priced at $20, regardless of cryptocurrency value fluctuations. It's the crypto equivalent that adjusts according to current rates, impacting the vendor's profit margin post-transaction, especially if the cryptocurrency's value decreases.

Do both the sender and receiver's wallets need to be active simultaneously for a transaction?

No, simultaneous wallet activity isn't required for transactions. Bitcoin transactions are processed automatically on the blockchain, ensuring your transfers are completed even if the recipient's wallet isn't online at the moment. Following privacy-preserving practices detailed in subsequent sections is critical.

What is a Satoshi?

A Satoshi represents the smallest unit of Bitcoin available, recorded on the blockchain. It equals one hundred millionth of a single Bitcoin (0.00000001 BTC), offering granularity in transactions and value representation. Further information on Satoshi units can be found in detailed cryptocurrency resources.

Monero (XMR)

Monero (XMR) is a privacy-focused cryptocurrency designed to offer secure, private, and untraceable transactions. It was launched in April 2014 and operates on the principle of anonymity and decentralization. Unlike Bitcoin and many other cryptocurrencies, Monero transactions obscure the sender, recipient, and amount transferred using several advanced cryptographic techniques:

1. **Ring Signatures**: This technique combines a user's account keys with public keys obtained from Monero's blockchain to create a 'ring' of signers, making it extremely difficult to trace the origin of the transaction.
2. **Stealth Addresses**: These are one-time addresses, generated randomly for each transaction on behalf of the recipient, which ensures that the true destination of the transaction is hidden from outsiders.
3. **Ring Confidential Transactions (RingCT)**: Introduced in January 2017, this feature hides the amount of XMR being transferred, further enhancing privacy.

Monero's strong focus on privacy and security makes it a popular choice for users seeking anonymity in their transactions. It uses a proof-of-work (PoW) consensus mechanism to validate transactions and secure its network, similar to Bitcoin, but with a different hashing algorithm called RandomX, which is designed to be ASIC-resistant. This means it's more accessible for individuals to mine Monero using standard computer hardware, promoting greater decentralization.

Monero's blockchain is intentionally opaque. It records all transactions, but

disguises the parties involved and the amounts exchanged, making it very different from transparent blockchains like Bitcoin's, where transactions can be traced and wallet balances viewed by anyone.

The privacy features of Monero have led to its adoption for a range of uses, both legitimate and illicit. On the one hand, it offers a means for individuals to keep their financial transactions private, away from the prying eyes of corporations, governments, or malicious actors. On the other hand, these same features have made it a preferred currency for darknet markets and other illegal transactions. Despite the controversies surrounding its use, Monero remains an important project in the cryptocurrency space, highlighting the demand for digital currencies that offer privacy and security. Its development is ongoing, with a strong community of developers and users dedicated to enhancing its privacy features and user experience.

Monero FAQ Guide

Routing Coins Safely:

Transfer your cryptocurrencies using the path: Exchange -> Monero Wallet (on Tails or Whonix) -> Destination. Refer to subsequent posts for in-depth guidance.

Dealing with Bitcoin-only Vendors:

Convert Monero to Bitcoin via an exchange service, then transfer to the destination, or Monero Wallet -> Exchange Service -> Bitcoin Wallet -> Destination. Utilize Tor with an instant exchange service for anonymous conversions. To avoid payment delays, especially for time-sensitive orders, transfer Bitcoin to your personal wallet first.

Purchasing Monero on KYC Exchanges:

For most scenarios, purchasing Monero directly on a KYC-compliant exchange is considered safe.

Direct Purchase vs. Conversion:

Directly buying Monero is preferable to purchasing Bitcoin and converting it, minimizing exposure to transparent blockchains.

Anonymously Acquiring Monero:

Use cash-by-mail options on platforms like LocalMonero.co for anonymity.

Transaction Visibility Issues:

Ensure your wallet is up-to-date and synchronized. Verify transaction existence on block explorers like xmrchain.net. For non-appearing transactions, follow specific wallet guidance for importing or rescanning transactions.

Outgoing Transaction Failures:

Address failed transactions in Feather by resending, or in GUI by changing nodes and rescanning wallet balance. Report persistent node issues for community assistance.

Remote Node Connection over Tor:

Connecting to remote nodes via Tor is safe for most users. Rotate nodes between sessions for enhanced security, a feature automated in Feather wallet.

Running a Full Node on Tails:

Consult available guides for setting up a full node on Tails.

Setting Up Remote Nodes:
For public/private remote node setup, refer to comprehensive guides.
Speeding Up Synchronization:
Switching remote nodes can enhance synchronization speed. Follow wallet-specific instructions for node changes.
Transferring Addresses Between Machines:
Transfer your address using a secondary USB, encrypted email, or scanning the QR code with another device.
Wallet Technical Issues:
For wallet malfunctions, contact community moderators with detailed information for troubleshooting.
Morphscript / MorphToken Usage:
MorphToken has restricted all Tor exit nodes, affecting Morphscript functionality on Tails/Whonix. Explore alternative exchange services listed in the community resources.
Additional Resources:
Block Explorers:

- **Non-Javascript**: https://xmrchain.net/
- **Onion service**: http://theblock755bysooet2texualb4detjjcvkxs2nxuiumln4bacjh3rqd.onion

This FAQ addresses key aspects of using Monero for transactions within the context of privacy and operational security.

How to Buy Monero

Setting Up Monero

Due to frequent updates and modifications in the Monero ecosystem, we advise consulting our comprehensive Monero Guide for the latest instructions and recommendations.
Access the guide at: http://xmrguide25ibknxgaray5rqksrclddxqku3ggdcnzg4ogdi5qkdkd2yd.onion
This resource covers a range of topics, including various wallet options available for installation and their usage, ensuring you have the most current and effective information.

Creating Monero Wallets

Due to frequent updates and modifications in the Monero ecosystem, we advise consulting our comprehensive Monero Guide for the latest instructions and recommendations.
Access the guide at: http://xmrguide25ibknxgaray5rqksrclddxqku3ggdcnzg4ogdi5qkdkd2yd.onion
This resource covers a range of topics, including various wallet options available for installation and their usage, ensuring you have the most current and effective information.

Litecoin (LTC)

Litecoin (LTC) is a cryptocurrency that was designed to offer fast, secure, and cost-effective payments by leveraging the unique properties of blockchain technology. It is based on the Bitcoin protocol but differs in terms of hashing algorithm, hard cap, block transaction times, and a few other factors. Litecoin is known for its short block time of 2.5 minutes and low transaction fees, making it suitable for micro-transactions and point-of-sale payments. The cryptocurrency was created by Charlie Lee, a former Google employee, with the intention of making Litecoin a "lite version of Bitcoin." It has become popular due to its simplicity and clear utility benefits, being accepted by over 2,000 merchants worldwide.

Litecoin was launched via an open-source client on GitHub on October 7, 2011, and went live on October 13, 2011. Since then, it has been widely adopted and remains among the top cryptocurrencies by market capitalization. As of January 2021, there were 66.245 million LTC in circulation, out of a total maximum supply of 84 million, with estimates suggesting it will take over 100 years to reach full dilution.

One of the significant updates to the Litecoin network was the MimbleWimble Extension Block (MWEB) upgrade, which promises to enhance privacy and scalability for users. This upgrade, however, led to some regulatory challenges, particularly in South Korea, where several exchanges delisted LTC due to concerns over its enhanced privacy features making compliance with specific financial transaction regulations difficult.

Overall, Litecoin's success can be attributed to its fast and cost-effective transactions, making it an appealing choice for both users and merchants alike.

Installing Litecoin in Tails

To get started with Litecoin on Tails, ensure you've activated both the persistent volume and dot files. If they're not set up, remember to perform a system reset after enabling these features.

Installation Steps:

1. **Download Electrum-Litecoin**: Visit the official website at https://electrum-ltc.org/ to download the Linux app image.
2. **Save the App Image**: Transfer the downloaded file to the Tor Browser (Persistent) or another folder within your Persistent storage. This step prevents the need for re-downloading after rebooting Tails.
3. **Enable Execution**: Right-click the App Image, navigate to Properties -> Permissions, and tick the option "Allow executing file as program." Close the window afterward.
4. **Launch Electrum-Litecoin**: Double-click the App Image to open Electrum-Litecoin. Set it up following the same procedure as for the standard Electrum wallet. Refer to the Bitcoin section for detailed setup instructions.

Handling Electrum-Litecoin Data:

Unlike its counterpart, Electrum-Litecoin doesn't support a portable mode, meaning Tails won't automatically preserve your wallets across sessions. To address this:

- **Option 1**: Manually save your wallet's seed phrase, possibly using KeePass for secure storage. This method requires you to restore your wallet with each new Tails session.
- **Option 2 (Recommended)**: Move the Electrum-LTC data to a persistent location.
    - Open Places -> Home and press Control+H to reveal hidden folders.
    - Locate and drag the .electrum-ltc folder into the Dotfiles directory in the sidebar.
    - Reboot your system to verify that your wallet data is preserved.

Final Steps:

Upon successful setup, a blue indicator at the wallet's bottom-right corner signifies a connection to the Litecoin network. If encountering issues, such as seeing a red indicator, check your proxy settings to ensure "Use Tor proxy at port 9050" and "Use proxy" are selected.

Following these steps ensures you have Litecoin ready and operational on Tails, with secure and persistent wallet management.

Bitcoin (BTC)

Bitcoin (BTC) is a form of digital currency, known as a cryptocurrency, which operates independently of a central bank. It was invented in 2008 by an anonymous person or group of people using the name Satoshi Nakamoto. The network came into existence in 2009 with the release of the first open-source Bitcoin software and the mining of the genesis block of bitcoin.

Key features of Bitcoin include:

- **Decentralization**: Bitcoin operates on a decentralized network of computers (nodes) around the world. No single institution or government controls the Bitcoin network, making it a decentralized digital currency.
- **Blockchain Technology**: Bitcoin transactions are recorded on a public ledger known as the blockchain. This technology ensures transparency and security, as the ledger is maintained by a network of nodes following a consensus protocol.
- **Limited Supply**: The total supply of Bitcoin is capped at 21 million coins. This scarcity mimics the properties of precious metals like gold and is intended to prevent inflation.
- **Mining**: New bitcoins are created through a process called mining, which involves using computer power to solve complex mathematical problems that validate transactions on the network. As a reward for their services, miners are awarded newly created bitcoins as well as transaction fees.
- **Peer-to-Peer Transactions**: Bitcoin allows for direct transactions

between users without the need for intermediaries, such as banks or governments. This can reduce transaction fees and increase efficiency.
- **Security and Privacy**: Bitcoin transactions are secure, thanks to the use of cryptography. Although transactions are recorded on the blockchain, the identities of the parties involved are encrypted and represented only by their public addresses.

Bitcoin has seen widespread adoption and has paved the way for the development of thousands of other cryptocurrencies. Its market price can be highly volatile, influenced by factors such as regulatory news, market demand, and technological advancements. Despite this, Bitcoin remains a popular choice for investment, online transactions, and as a potential hedge against fiat currency inflation.
Keep in mind that starting with Bitcoin may lead to your transactions being traced back to your real identity. If direct purchase of Monero isn't an option, ensure you convert your existing coins to enhance privacy.

Key Bitcoin Tips

- **Secure Your Electrum Seed**: It's crucial to safeguard your Electrum wallet seed. Record it on paper, save in a text file, or memorize it. This ensures you can retrieve your bitcoins if your Tails USB is lost or damaged.
- **Receiving Bitcoins**: To receive bitcoins, direct them to an address listed under the "Addresses" tab in your wallet. There's no need to use the "Receive" tab unless you're organizing your transactions.
- **Utilize New Addresses for Transactions**: For enhanced security, generate and use a new Bitcoin address for each transaction. Electrum provides multiple addresses; using them boosts your operational security without incurring extra costs.
- **Budget Appropriately for Transactions**: Always ensure you have sufficient bitcoins to cover both the cost of your order and shipping fees, with a slight margin for unexpected expenses.

How to buy bitcoins

1. Cryptocurrency Exchanges

- **Description**: Online platforms where you can buy, sell, or exchange cryptocurrencies for other digital currency or traditional currency like US dollars or Euro.
- **Examples**: Coinbase, Binance, Kraken.
- **Pros**:
  - Wide range of cryptocurrencies available.
  - Various payment options (bank transfer, credit/debit card, etc.).
- **Cons**:
  - Can be complex for beginners.
  - Some exchanges have high fees.

2. Peer-to-Peer (P2P) Platforms

- **Description**: Allows you to buy Bitcoin directly from other individuals without the need for an intermediary.
- **Examples**: LocalBitcoins, Paxful.
- **Pros**:
  - More privacy and sometimes better exchange rates.
  - Flexible payment methods, including cash.
- **Cons**:
  - Higher risk of scams.
  - Can be more time-consuming to find the right seller.

3. Bitcoin ATMs

- **Description**: Physical machines located in public places where you can buy Bitcoin with cash or debit card.
- **Pros**:
  - Anonymity for smaller purchases.
  - Instant acquisition of Bitcoin.
- **Cons**:
  - High transaction fees.
  - Limited availability in some areas.

4. Brokerages

- **Description**: Firms that buy and sell Bitcoins on your behalf, not unlike stock brokerages.
- **Pros**:
  - Simplicity and ease of use.
  - Suitable for beginners.
- **Cons**:
  - Higher fees than exchanges.
  - Less control over purchase prices.

5. Direct from Someone You Know

- **Description**: Buying Bitcoin directly from friends, family, or anyone willing to sell their Bitcoin to you.
- **Pros**:
  - Potentially no or low transaction fees.
  - Trusted environment.
- **Cons**:
  - Limited by the Bitcoin holdings of acquaintances.
  - Lack of market rate comparison.

Considerations Before Buying Bitcoin:

- **Security**: Use secure wallets and exchanges with a good reputation.
- **Fees**: Be aware of transaction fees, which can vary widely.
- **Regulations**: Understand the legal and tax implications in your country.
- **Volatility**: Be prepared for the price of Bitcoin to change rapidly.

Configuring Your Bitcoin Wallet on Tails

Note on Two-Factor Authentication (2FA):
Avoid using Electrum wallets with 2FA on Tails. While 2FA is beneficial for market activities, it complicates Electrum usage by involving your smartphone and requiring Google apps, which compromises anonymity. Secure your wallet by safeguarding your seed phrase and using KeePassX for your wallet's password.
Electrum on Whonix:
Whonix users can utilize the pre-installed Electrum wallet following the same setup instructions.
Electrum Setup Guide:

- **Accessing Electrum**: Navigate to "Applications" > "Internet" and select "Electrum Bitcoin Wallet."
- **Persistence Warning**: If you see a warning about persistence being disabled for Electrum, set up persistence to safeguard your bitcoins.
- **Installation Wizard**: Follow the wizard to set up your wallet. Name your wallet, select "Standard Wallet," then "Create a new seed." Opt for the "Segwit" seed type.
- **Seed and Security**: Securely record your seed phrase. It's crucial for recovering your bitcoins. Confirm your seed, then set a strong password with KeePassX.
- **Final Adjustments**:
    - Under "Tools" > "Preferences," adjust your settings:
    - General: Set "Base unit" to BTC and adjust "Zeros after decimal point."
    - Transactions: Enable "Replace-By-Fee," "Use multiple change addresses," and set "Online Block Explorer" to a .onion blockchain explorer.

Important Considerations:

- Electrum's server list is not anonymous. However, using Tails routes your traffic through Tor, masking your IP but not the association between your wallet's addresses. Adhere strictly to the guidance in the sending bitcoins section to maintain anonymity.
- **Troubleshooting**:
    - If Electrum fails to start, verify your seed is accessible. Try launching Electrum from the terminal (`electrum` command) or adjusting persistence settings for the Bitcoin client.
    - Corrupted Electrum files can be fixed by deleting or renaming the Electrum folder in your persistence directory and restoring your wallet from the seed.

Transferring Bitcoin Safely

This section outlines the steps for securely sending Bitcoin from its source (such as an exchange) to its intended destination (like a Darknet Market, DNM). Direct

transfers from exchanges to DNMs are discouraged due to the risk of account suspension.

The Transfer Path:

Caution: Using Electrum exposes the linkage between wallet addresses and the IP addresses querying their balances. To enhance privacy:

- **Preferred Path**: Exchange -> BTC Wallet1 -> Convert to XMR -> XMR Wallet -> DNM. Convert back to BTC if necessary, as detailed in the conversion section.
- **Important**: Maintain separate wallets for your initial BTC storage and the Electrum wallet on Tails.

Breaking the Chain:

This method obscures the trail leading back to you, providing plausible deniability. Once your funds are converted to Monero (XMR), they become untraceable. Claiming ignorance about the wallet's current status or its transactions becomes more credible.

Sending with Electrum:

1. **To Transfer**: In Electrum, navigate to the "Send" tab, input the recipient's Bitcoin address under "Pay to," and let Electrum dynamically set the transaction fee for timely confirmation.
2. **From Non-Tails Wallet to Tails**: First, obtain a receiving address from your Tails Electrum wallet under "Addresses." Label the address as "used" after the transaction to avoid reuse.
3. **Setting Fees Manually**: If preferred, manually adjust the fee based on current network conditions for faster confirmations. Refer to bitcoinfees.21.co for recommended rates and adjust in Electrum under Tools -> Preferences.

Key Considerations:

- **Seed Phrase**: Securely store your Electrum seed phrase for wallet recovery.
- **Use Unique Addresses**: For every transaction, use a distinct Bitcoin address to enhance operational security.
- **Transaction Costs**: Ensure you have sufficient funds to cover both the purchase and potential transaction fees.
- **Market Minimums**: Be aware of and comply with minimum deposit amounts set by DNMs to avoid loss of funds.
- **Future Transactions**: For subsequent DNMs deposits, adhere strictly to the recommended transfer path for improved security.

Following these guidelines enhances the safety and anonymity of your Bitcoin transactions within the DNM ecosystem.

Understanding Bitcoin Transaction Confirmations

Bitcoin transactions are verified and recorded on the blockchain through a process conducted by miners. The speed at which a transaction is confirmed typically

depends on the transaction fee it carries; higher fees usually result in faster confirmations. Congestion on the Bitcoin network, characterized by a high volume of unconfirmed transactions, can also delay the confirmation process. If you're experiencing delays, patience is key as confirmations can take from a few hours to more than a day depending on network conditions.
During this waiting period, ensure the transaction was sent to the correct address; a mistake here means the bitcoins may never arrive at the intended destination. For future transactions, utilizing the dynamic fee recommendation by Electrum (found under the "Send" tab) can help avoid delays, as it aims to get your transaction confirmed within five blocks.
Speeding Up Unconfirmed Transactions
If your transaction is taking longer than expected to confirm, you have a couple of options to expedite it:

1. **Increase the Transaction Fee**: This method is applicable to transactions marked as "replaceable," which requires prior activation of the "Replace by Fee" option in Electrum's settings. Should the initial transaction linger unconfirmed, you can right-click it and opt to increase the fee, thereby boosting its priority among pending transactions.
2. **ViaBTC Transaction Accelerator**: For transactions sent to addresses outside your control, such as a DNM, you might try the ViaBTC Transaction Accelerator. Its effectiveness varies, and it may not always lead to faster confirmations.

Frequently Asked Questions

- **Can I cancel a pending Bitcoin transaction?**
  Unfortunately, once a transaction is initiated, it cannot be canceled. You must wait for it to be either confirmed or rejected by the network.
- **Will I lose my bitcoins due to a delay?**
  No, your bitcoins are not lost. Delays in confirmation do not affect the ultimate arrival of your funds, though patience is required during periods of network congestion.

Understanding these aspects of Bitcoin transactions and utilizing available tools to manage fees and confirmation times can help navigate the complexities of transacting on the blockchain.

Shipping

Understanding Postal Systems for Mail Delivery

The process of sending and receiving mail, whether it's a letter or a parcel, is facilitated by postal systems present in almost every country around the globe. The movement of mail within the same country is referred to as "domestic" mail, while mail exchanged between different countries is known as "international" mail. Postal systems across nations may differ in their operational specifics, yet they commonly feature mail sorting centers and customs inspection facilities. International shipments undergo inspections at two customs points: one in the originating country and another in the destination country. Such international

shipments are scrutinized more heavily than domestic ones, potentially subject to opening and X-ray inspections based on the respective country's regulations and practices. In contrast, in the United States, domestic First-Class mail enjoys legal protection from unwarranted searches and seizures.

Moreover, international shipping tends to be more costly and carries a higher risk of loss compared to domestic shipping. Some countries, notably Singapore, Australia, New Zealand, Israel, Norway, Sweden, Finland, and several countries in the Middle East and Asia, are recognized for their stringent customs inspections of incoming mail. Consequently, individuals considering the shipment of contraband through international mail to these locations should be cautious, given the increased likelihood of detection and potential legal consequences.

Timing Between Orders: Best Practices

To minimize risks, it's advised to limit yourself to having only one package in transit to you at any given time. Should you receive your package without any issues, you can then proceed with placing your next order. This cautious approach ensures that, in the unfortunate event of package interception, law enforcement will find only a single package associated with illegal contents and your address. The discovery of multiple packages containing contraband significantly complicates your ability to claim unawareness, presenting a more challenging scenario for both you and your legal representation in court.

Is it necessary to alter my shipping address?

Not required, provided you adhere to the guidelines in the DNM Bible and limit yourself to one package at a time; your address can remain the same.

Package Received in Damaged Condition

Packages may occasionally arrive slightly damaged without being fully opened. It's important to remember that these packages undergo rough handling; they could be dropped, bent, roughly handled by workers, or damaged by sorting machines. Opening someone else's mail without authorization is against the law. However, if the damaged packaging exposes its illegal contents, it's advisable to refrain from placing orders for some time. On the other hand, if the contents remained concealed due to protective packaging or a decoy used by the sender, it's likely that there won't be any issues, even if the package arrived in a damaged state.

Is It Possible to Have Orders Delivered to a University or Dormitory?

Indeed, it is feasible to have orders delivered to a university residence or dormitory. However, it's crucial to verify that you have not relinquished any rights that would permit the educational institution to conduct searches of your mail. Be aware that universities have the authority to inspect dormitory rooms without prior notice or specific reasons.

Is It Advisable to Have Orders Sent to My Workplace?

Absolutely not. Mixing Dark Net Market activities with your professional environment is highly risky. It could potentially lead to both job termination and legal consequences. It's essential to maintain a strict separation between your online activities and your place of employment.

Is It Safe to Track My Package?

For U.S. residents, enrolling in USPS Informed Delivery is an option. This service allows you to monitor incoming packages without specifically requesting tracking numbers, offering a layer of plausible deniability since it's a service promoted by USPS for all users.

Generally, avoid tracking your package unless it's significantly overdue. Tracking leaves digital footprints that don't expedite delivery but could potentially expose you. For further insight, refer to guidelines on handling undelivered packages. If you find it absolutely necessary to track (which should be rare), avoid using Tor, as it's a known method that raises suspicion with law enforcement. Instead, consider using third-party websites like TrackingEx or PackageMapping for tracking, which aren't directly linked to your carrier. Ensure you're not using your personal WiFi; opt for a public connection or a VPN within your country to avoid drawing attention.

In the event of receiving more items than you ordered, additional products, or goods you didn't request, what steps should you take?

Reach out to the seller. Should the item be of use to you, propose to compensate them for it. In cases where the item is only partially useful or you didn't initially want it, think about covering the shipping costs plus half the price of the item. If the item is something you don't want or can't use, inform the seller regardless. Maintaining positive relations with reputable sellers is advisable, as it often leads to better service.

Disposing of Packaging Material

After removing the contents from your package, you'll be left with packaging materials. To avoid potential self-incrimination, it's advisable not to dispose of these materials in your personal trash. Consider burning them or discarding them in a public trash receptacle not linked to your residence or places you frequent. Law enforcement agencies often examine a suspect's garbage for evidence related to drug offenses, making careful disposal essential.

Origin Countries

The primary guideline is: prioritize local whenever feasible. Shipments that remain within one's own country are scrutinized less than international mail, significantly reducing the likelihood of package loss or legal complications.

On the flip side, a drawback is that domestic prices may be slightly elevated compared to offerings from international vendors. The decision between accepting a higher risk for a lower cost or opting for security at a premium rests with you. For those making their initial purchases or are relatively new to this, choosing local, despite the potential for higher costs, is advisable. Newcomers often experience undue stress (e.g., paranoia) or commit errors during their early transactions. Choosing local shipments can offer a sense of reassurance, typically ensuring a greater probability of success.

Countries of Concern for International Shipping

If you're contemplating an international order, it is highly advised to reconsider

ordering from the subsequent countries known as 'high-risk' areas. Mail originating from these territories often undergo stringent inspections:

- The Netherlands (NL) – Renowned as a source country for various illegal substances
- Colombia (CO) – Infamous for cocaine and heroin production
- Peru (PE) – Notable source of cocaine
- Bolivia (BO) – Infamous for cocaine production
- Venezuela (VE) – Considerable, but lesser-known cocaine producer on the rise
- Ecuador (EC) – Notable, yet under-reported cocaine source
- Canada (CA) – Highlighted on Israel's watch list for drug-source countries. In particular, XpressPost deliveries from Canada are often subject to random inspections by US Customs. However, Non-XpressPost deliveries generally do not raise additional concerns.
- Spain (ES) – Featured in Israel's watch list, impacting imports into Israel.
- France (FR) – Included in Israel's list of drug-source countries, affecting imports.

While lists may vary slightly among global customs agencies, including US Customs, the US State Department provides a useful index of countries they view as significant drug sources. Detailed in their annual International Narcotics Control Strategy Report, the countries considered to be "Major Illicit Drug Producing, Drug-Transit, Significant Source, Precursor Chemical" are as follows (based on INCSR 2018 Volume 1):

Countries that Substantially Contribute to Illicit Drug Manufacture, Transit, and Significant Source Countries

Countries that are Major Illicit Drug Producers and Predominant Drug-Transit Countries

A country is deemed a significant illicit drug producer when:

- 1,000 hectares or more of illicit opium poppy are cultivated or harvested annually B. 1,000 hectares or more of illicit coca are cultivated or harvested annually C. 5,000 hectares or more of illicit cannabis are cultivated or harvested annually, unless the President concludes that such illicit cannabis production does not impact the United States significantly.

A predominant drug-transit country is defined as:

- A country that serves as a significant direct supplier of illicit narcotics or psychotropic drugs or other controlled substances impacting the United States considerably, or B. A country which significantly transports such drugs or substances.

On September 13, 2017, the President notified Congress that the following countries are substantial illicit drug manufacturers and/or drug-transit territories: 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.
Countries Identified as the Primary Sources of Precursor Chemicals for Illicit Drug Production:
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, the Republic of Korea, Singapore, South Africa, Switzerland, Taiwan, Thailand, the United Kingdom, and Venezuela.

Countries known for strict customs enforcement on inbound international mail

Some nations are notorious for their rigorous inspection of incoming international postal items. The onus of ordering prohibited items through international mail to and from these countries falls on the buyer. But generally, it's deterred because of the heightened chances of unearthing and apprehension. Noted countries include:

- Australia (AU)
- New Zealand (NZ)
- Israel (IL) – it's advised against sending drugs from Canada, Spain, France or the Netherlands to Israel
- Norway (NO)
- Sweden (SE)
- Finland (FI)
- Singapore (SG), and several other Asian nations
- Most Middle Eastern nations

Moreover, familiarize yourself with whether your nation is a member of any consortium or has trade agreements with other countries that facilitate mail dispatch with lesser scrutiny.

Stealth

The concept of stealth is pivotal when it comes to safely receiving ordered products at your doorstep, particularly when discussing the dispatch and packaging of certain items by vendors. It's not solely the vendor's responsibility; as a customer, vigilance is key to avoid legal complications by selecting a vendor with a reputation for inadequate stealth measures.
Stealth, in this context, involves packaging the product in such a way that it looks ordinary and does not attract unwanted attention, effectively masking any potential indicators, including odors, that could reveal the contents. On the other hand, a decoy is specifically employed within the package as a means of concealing the actual product. This is particularly crucial for international shipments, which undergo customs inspections at both the origin and destination countries, making the use of decoys vital to evade detection. For domestic orders, the necessity for decoys diminishes since the packages do not cross international borders and are subjected to less scrutiny.
Therefore, when placing international orders, it's advisable to thoroughly examine

vendor reviews—paying special attention to their use of decoys and overall stealth practices—as outlined in the guidance for choosing a vendor. This ensures a higher degree of discretion and safety in the delivery process.

Non arriving packages

General

When you're eagerly waiting for a package and it hasn't arrived on time, it's important to consider various factors that might be causing the delay. Sometimes, sellers mark an item as shipped well before it's actually dispatched. They might do this for various reasons, such as to enhance security measures or simply because they're behind on their shipping schedule. This discrepancy can set unrealistic expectations about the delivery timeline.

Delays can also arise from a multitude of other sources, not just the seller's shipping practices. Adverse weather conditions, postal service strikes, and other unforeseen events can all contribute to your package taking longer to reach you than initially anticipated. It's essential to remain patient and consider these potential obstacles when waiting for your shipment.

Testing if your mail gets intercepted

To determine whether your mail is being intercepted, you can conduct a simple experiment by sending a package to yourself, ideally from a post office that is not in your immediate vicinity. Here's how you can go about it:

1. **Package Preparation**: Start by packaging the item yourself. Pay close attention to how you arrange everything inside the package. If necessary, take photographs to remember the exact placement of items.
2. **Customize Your Package**: Get creative with the packaging. Use colorful tape to create unique patterns or shapes over the seals of the package. Count out a specific number of packing peanuts and remember the amount. Wrap the item in festive, thin wrapping paper for an additional layer of uniqueness, and secure it with tape. The appearance of the package doesn't need to be conventional; in fact, a more unusual look might be advantageous for this test.
3. **Content of the Package**: The choice of what to send is flexible, as long as it adheres to legal guidelines. One intriguing option is a motion sensor camera, like those used by hunters to capture wildlife activity at night. This item isn't crucial to the experiment's success, but it's important that whatever you choose to send is permissible by mail.
4. **Addressing the Package**: Consider handwriting the address and return information on the package to add another personal touch.
5. **Repeat the Process**: If necessary, send multiple packages using this method to thoroughly test if any tampering occurs during transit.

The goal of this experiment is to ascertain whether your mail undergoes any unauthorized opening or inspection. By taking these steps, you can assess the security and privacy of your mail delivery system.

Got “Undeliverable as Addressed”?

When you encounter the message “Undeliverable as Addressed,” it signifies that the postal service could not deliver your package due to issues with the recipient’s address. This issue might arise for various reasons. Perhaps the address is incomplete—maybe you omitted your apartment or unit number. There could be mistakes in the address, such as typos or incorrect information. It’s also important to use your real name and address details to avoid complications. Other reasons for non-delivery include the postal worker’s difficulty in reading the address, damage to the label that makes the address illegible, or an oversight by the vendor, like forgetting to include an apartment number even though it was provided.

Imagine you’re eagerly anticipating the arrival of your order. You believe today is the day it should arrive, so you check the tracking status, only to find it marked as “Undeliverable as Addressed – package will be shipped back to sender if sender address is valid.” Initially, you might feel a wave of panic, but then you regain your composure. Fortunately, you’re reading this guide, which will help you navigate through this situation.

If your package has been marked as “Undeliverable as Addressed” and it’s been less than a day since this occurred—for instance, if it’s 12 pm and your package was marked undeliverable at 7:30 am—here’s a structured approach to address the situation:

1. **First Attempt: Call the Local Post Office**
   – Start by calling the post office where your tracking information indicates your package is currently located. It might be challenging to get through as local post office numbers often lead to dead ends, or the staff may not answer. However, if you do get through, explain your situation calmly, providing your name and the correct shipping address. They might suggest you come to pick up the package personally.
2. **Visiting the Post Office**
   – If calling doesn’t yield results, your next step is to visit the post office mentioned in your tracking details. Bring identification (ID or proof of residency at the shipping address) with you. Although not strictly necessary, having your package’s tracking number can be very helpful. Approach the staff courteously, addressing them with respect, and explain that you were directed to pick up a package that couldn’t be delivered. When asked, provide your ID and the tracking number. They should be able to locate your package if it’s there.
3. **Dealing with Service Challenges**
   – If your visit to the post office does not resolve the issue, or if the interaction is less than pleasant, don’t lose hope. Your next step is to contact the USPS customer service via their toll-free number. Expect to be on hold for a significant period, ranging from 30 to 90 minutes. Once

connected with a customer service agent, explain your situation clearly, providing your name and the accurate address.

4. **Follow-Up and Patience**
   – The customer service representative will likely assure you that they'll attempt to redeliver your package. Be prepared for a wait of an additional 5 to 10 days for the delivery. This timeframe allows for the retrieval of your package and the update of its shipping label. Note that if a considerable amount of time has passed, updating the label might not be possible, but this initial period should not pose such an issue.

This approach balances proactive steps with the need for patience and respect in interactions with postal service workers and customer service representatives. Remember, the goal is to resolve the situation with your package while maintaining a positive and polite demeanor throughout the process.

If your eagerly awaited package has been tagged with the dreaded "Undeliverable as Addressed" status for more than a day—let's say it's January 15th and the status changed on January 13th—here's a streamlined guide to navigate this hiccup.

Firstly, arm yourself with patience and dial the USPS customer service hotline (a quick search will reveal the toll-free number). Prepare for a bit of a wait, ranging from 30 to 90 minutes. Yes, it might seem like an eternity, but perseverance is key here. Once the hold music graciously bows out and a customer service agent graces your call, present them with the situation, courteously providing your name and the accurate address.

The agent will likely assure you with a hopeful "We should be able to resolve this," but it's wise to temper expectations. Anticipate a waiting period of an additional 5 to 10 days for the delivery, contingent on whether they can intercept and relabel your package. Occasionally, this might not be feasible.

This snag often arises if the attempt to rectify the "Undeliverable" status of the package is made belatedly, limiting the USPS's ability to amend the shipping details and relegating them to merely redirect it back to your city. However, don't let despair set in. Provided you act swiftly this round, following the outlined steps should reunite you with your package. Patience and timely action are your allies in ensuring a joyful parcel retrieval.

Drop

Ensure your surroundings are pristine and devoid of any questionable items or substances, such as drug paraphernalia, whenever you're anticipating the arrival of a delivery. This precaution extends beyond your primary residence to any property associated with you. The reason is straightforward: in the event of an unforeseen complication, there's a significant likelihood that your premises may be subject to a thorough search. Should the authorities discover any illegal items during their inspection, defending your innocence and law-abiding status in a legal setting becomes considerably more challenging, especially if there are allegations

involving illicit substances mailed to your address.

Is it advisable to utilize my genuine name when arranging deliveries to my residence?

Indeed, this question ranks among the most hotly debated by purchasers since time immemorial, culminating in a unanimous consensus: Opt for your authentic identity. Dismiss the notion that your strategy is groundbreaking or that you're somehow an exception to the established norm. Employing your actual name does not inherently heighten your culpability. The rationale behind this strategy is to ensure your parcel seamlessly integrates with the rest of your incoming mail. The United States Postal Service (USPS) meticulously records the names associated with delivered parcels. An alias is glaringly conspicuous to your local mail carrier and the sophisticated USPS tracking systems.

In the event of a package interception, the critical factor is not the name on the label but the ability to substantiate your involvement in the order. Adherence to the guidelines laid out in the DNM bible significantly diminishes the likelihood of such a predicament. Using your real name enhances the prospects for a hassle-free delivery process.

Residing Under Your Parents' Roof?

Navigating life under your parents' roof comes with its set of unspoken rules, particularly when it comes to respecting their space and privacy. It's crucial to remember that, regardless of whether they monitor your mail or are unaware of your activities, inviting trouble to their doorstep is a gesture far removed from gratitude. A seemingly minor slip-up, such as receiving an improperly sealed package from a vendor, could escalate quickly, potentially leading to an unwelcome visit from law enforcement. Imagine the distress and disappointment that would follow, especially considering the years of care and support they've provided you.

The wise move? Opt for a P.O. box for receiving your parcels. This ensures your privacy and keeps your home environment secure and respectful. If you're underage or find the process daunting, it's a clear sign to steer clear of deep web markets and related activities. These platforms are intended for mature audiences, with age restrictions in place for good reason. The allure of exploring the hidden corners of the internet and experimenting may seem tempting, but it's a journey fraught with risks, especially for those not fully prepared to navigate its complexities.

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

Whether to sign for a package or mail when requested can be a nuanced decision, shaped by local laws and the specific circumstances surrounding the delivery. In certain areas, signing may be necessary for official matters, while in others, it may not be as critical.

However, in scenarios involving controlled deliveries—situations orchestrated by law enforcement to catch individuals receiving illegal items—choosing not to sign won't necessarily prevent subsequent arrest. Law enforcement's strategy doesn't

hinge solely on obtaining a signature; their focus is on the broader context of illegal activity. Refraining from signing could even raise suspicion.
It's important to note that signing for a package doesn't automatically imply guilt. The legal system requires proof beyond just accepting a delivery. Signing typically serves as confirmation of receipt for the postal service, ensuring they've fulfilled their delivery responsibilities. This process is particularly common for international shipments.
The reluctance to sign, prevalent among some communities, especially those involved in risky activities like darknet transactions, stems from a desire to maintain control and minimize risk. It reflects the anxiety and paranoia associated with receiving potentially compromised packages. Ultimately, once a package is in transit, individuals have limited control over law enforcement's actions.

Using a drop

In the intricate world of managing discrete mailing addresses, utilizing a "drop" presents itself as an unconventional yet resourceful method. This guide outlines the nuanced strategy behind setting up a drop—a location detached from personal ties, used for receiving sensitive correspondences.
While the reliance on drops is not universally recommended due to its complexity and potential risks, those who proceed must do so with creativity and adaptability as their guiding principles. The effectiveness of a drop hinges on its believability as a legitimate address, and here's a streamlined approach to establishing one:

- **Strategically Selecting a Drop Location:** Look for a residential property currently unoccupied (ensuring it's not bank-owned) to serve as your drop. The aim is to create the illusion of habitation—this includes basic yard maintenance and the occasional placement of everyday items outdoors. Regular visits to the property over a period of one to three weeks are crucial. These visits, coupled with subtle interactions or lack thereof, should foster a general awareness among neighbors of someone residing there, without making your identity discernible.
- **Familiarizing the Mail Delivery System:** To integrate the drop into the local postal service's routine, start by sending non-essential mail and packages to the address under the chosen delivery name. This step acquaints the mail carrier with the address's active status. Note the distinction in delivery services (e.g., Amazon's use of UPS versus USPS for standard mail), and adjust your strategy accordingly. Regularly collect and store the mail inside the premises, adopting a cautious approach to its handling.
- **Alternative Methods:** For those without direct access to vacant properties, opening a PO box under another's name or even in your own name in a different state offers a viable alternative. This method simplifies the process, requiring no false identification, and maintains a layer of separation between the box's user and its registered owner.

It's essential to view this guide as a starting point rather than a comprehensive

manual. The intricacies of establishing a drop are vast, with many variables dependent on the specific circumstances of the drop location. Attention to detail and situational adaptability are paramount in navigating this complex terrain effectively.

Is it possible to immediately start using my PO Box after setting it up?

Immediately utilizing your PO Box after its establishment is possible, though exercising a bit of patience is often advised. A prudent approach involves dispatching inconsequential, lawful items initially to ascertain the operational status of your PO Box. It's not uncommon for new users to encounter initial hiccups; instances such as overlooked activation by the postal staff have been noted. Imagine the inconvenience should these teething problems coincide with the delivery of sensitive parcels. Opting for a self-sent test package or placing an order through mainstream online marketplaces like Amazon or eBay serves as a wise preliminary step. Additionally, diversifying the contents of your deliveries, perhaps by exploring /r/freebies on Reddit, can be a strategic move to avoid any unwanted attention towards your PO Box, especially if you aim to maintain a low profile.

Controlled Delivery (CD)

What Does "Controlled Delivery" Mean?

A controlled delivery involves law enforcement allowing a package suspected of containing illegal drugs to be delivered. The goal is to use the acceptance of this package as grounds for conducting a search of the recipient's home. The rationale behind this tactic is that accepting the package can be seen as probable cause, suggesting that the recipient was expecting the package and aware of its contents. It's important to note, however, that not all packages requiring a signature are part of a controlled delivery operation.

How Does One Become Subject to a Controlled Delivery?

Individuals may find themselves targeted for a controlled delivery through various scenarios. Often, this occurs when someone orders a significant quantity of products from overseas. Law enforcement (LE) might detect a surge in packages arriving from the same sender, decide to inspect one, and subsequently begin profiling the recipient. The likelihood of being subjected to a controlled delivery increases with the size of the order, especially if it's from another country. Conversely, domestic shipments containing smaller quantities are less likely to attract attention. In cases where the amount is deemed personal use, the recipient might instead receive a warning letter, commonly referred to as a "love letter," which typically marks the end of the matter. Additionally, law enforcement may initiate monitoring of the individual's mail as part of their investigation.

What Occurs During a Controlled Delivery?

In a controlled delivery, law enforcement (LE) agents will deliver a package suspected of containing illegal substances directly to you, mimicking a standard delivery process. If executed properly, there should be no visible signs that this

delivery is anything but ordinary. Contrary to popular belief, this scenario does not involve a SWAT team forcefully entering your home and engaging in a shootout. Instead, once you accept the package, the officers will reveal themselves, announce their presence, and then instruct you on their next steps, which typically involve asking you to exit your home.

How Much of a Product Triggers a Controlled Delivery?

The threshold for what constitutes enough of a product (such as illegal substances) to warrant a controlled delivery (CD) is influenced by a multitude of factors. These can include your location, criminal history, age, the resources and priorities of your local law enforcement agency, among other considerations. As such, there is no one-size-fits-all answer applicable to everyone, everywhere. It's crucial to exercise good judgment. The term "bulk" is subjective and varies widely; if you're considering ordering large quantities, it's wise to use alternative receiving methods, like a drop location. Ultimately, making informed and cautious decisions is key.

What Happens After You Accept the Package?

Upon accepting the package, law enforcement typically proceeds to search your residence for additional illicit substances or evidence of drug orders. They often search for empty letters and packages that might have return addresses linked to the shipment. It's a misconception that your computer will always be confiscated; however, without any admission from you, it's less likely they'll connect the delivery to a dark net market (DNM). It's crucial to communicate with the police solely through an attorney you've selected and researched in advance. Remember, saying less often means revealing less, so it's advisable to let your legal representation do the talking.

How to Safeguard Against a Potential Controlled Delivery

To minimize the risk of becoming involved in a controlled delivery (CD), there are several indicators you can watch for. Extended delays in shipment beyond the expected delivery time might suggest complications, potentially related to law enforcement scrutiny. Receiving a seizure notice, especially following a significant order, is another red flag. Additionally, if the vendor you've purchased from is apprehended and their outgoing mail is confiscated, this could also increase the likelihood of a CD involving their shipments. Being vigilant about these signs can help you assess and mitigate risks associated with receiving packages under surveillance.

How do you protect yourself?

For optimal operational security, it's crucial to adhere closely to established guidelines. For starters, using your own residence as the delivery address is surprisingly the safest option. It's less likely to raise suspicion if you use your genuine name and address. Regardless of where you direct your shipments – be it an unoccupied property or a post office box – if authorities are determined, they will find a way to link you to the order, potentially endangering the sender as well. Therefore, it's advisable to keep shipments directed to your home under your real

name.
In the event of a controlled delivery (CD) suspicion, the immediate step should be to ensure your environment is clear of any illegal or even questionable items, such as drug paraphernalia. This preemptive measure significantly lowers the risk of legal repercussions, as the absence of incriminating evidence makes it difficult to prove wrongdoing. Particularly if you've been utilizing Tails for online activities, there's no direct trail leading to your recent or past orders. Remember, a CD itself doesn't imply inevitable punishment; concrete proof of your involvement in the order is required for legal action.

Does receiving a controlled delivery mean my address is compromised?

If you experience a controlled delivery (CD), it's highly probable that your address will be under surveillance thereafter. In such a scenario, you have a couple of options. You could either cease ordering from darknet markets (DNMs) entirely or consider having your orders sent to a friend's address. However, using a drop location is not advisable. If authorities discover that you've redirected your activities elsewhere following a CD, they're more likely to take decisive action against you. Should you choose to use a friend's address, ensure it's done with their consent and use their name for the order. This way, if a CD occurs at their location, it won't be directly linked to you, assuming your friend maintains discretion.

Monitored Delivery

Understanding Monitored Deliveries

Monitored delivery stands in contrast to controlled delivery, presenting a less common but strategic approach by law enforcement. This method involves the deliberate delivery of illegal drugs by authorities who then initiate surveillance on the recipient. The objective? To collect evidence over time, potentially spanning months, that supports a broader investigation into the recipient's unlawful activities. This meticulous strategy allows law enforcement to construct robust cases against individuals with otherwise strong operational security.

Real-Life Instances:

- **Community Alert:**
  A cautionary tale shared by T00N highlights the risks involved. A student known to T00N's acquaintance faced arrest by the DEA for distributing substances like Xanax and cocaine. The twist? Law enforcement had intercepted a package destined for him seven months prior but continued the deliveries to amass evidence. A grim reminder of the vigilance needed.
- **A Cautionary Example:**
  In another case, a person experienced the ramifications of monitored deliveries firsthand with the importation of large drug quantities. After receiving a shipment of MDMA, they were trailed from the drop-off point back to their residence, where further surveillance documented their

activities. Despite being found with a significant cache of drugs, including MDMA, LSD, and ketamine, the individual received a relatively lenient sentence. Notably, federal agents overlooked additional substances hidden within their home. Scheduled for release in 2019, this story serves as a stark illustration of the unexpected outcomes in drug enforcement operations.

These examples underscore the serious and unpredictable nature of monitored deliveries, emphasizing the need for awareness and caution.

Safeguarding Yourself from Monitored Deliveries

Protecting oneself from a monitored delivery presents significant challenges, primarily because individuals often remain unaware of ongoing law enforcement activities. Typically, these surveillance tactics target drug distributors rather than individuals purchasing drugs for personal use.

To mitigate risks, you might employ certain strategies to discern whether your mail is under scrutiny, though these methods are not foolproof. Packages might not show signs of tampering, making detection difficult. Reducing the frequency of your orders can also help, potentially leading law enforcement to deduce that there are no forthcoming shipments.

The legality of monitored deliveries varies by country. In the United States, such practices are indeed utilized by law enforcement. Being aware of your local laws and regulations can provide some guidance on what to expect and how to navigate these situations more safely.

Love letter

A “love letter” might sound endearing, but in certain contexts, it’s anything but. This term refers to a notification from postal authorities indicating the seizure of illegal substances or contraband mailed to you. Essentially, it’s their way of saying, “We’ve caught something you shouldn’t have sent or received. We’re letting you off this time, but we’re keeping an eye on you. Don’t let it happen again.”

International and Domestic Seizure Notices: A Closer Look

Internationally, customs agencies, including those in the United States, often issue these “love letter” notices for small quantities of illegal drugs found in mail. The message is clear: you’ve been spared from legal action, but the incident hasn’t gone unnoticed. If you receive such a letter, it’s wise to consider your address compromised for any future illegal shipments.

Interestingly, receiving a fake seizure letter is within the realm of possibility, adding a layer of complexity to this issue.

On the domestic front, the situation differs significantly. It’s rare to receive a formal seizure notice for contraband sent within the same country, particularly in the United States. More commonly, if illegal drugs are discovered in domestic mail, authorities opt for a controlled delivery to apprehend the recipient directly. Therefore, any seizure notice for a domestic shipment of drugs is likely a hoax, except in rare cases involving the interception of cash.

This distinction underscores the seriousness with which postal authorities and law

enforcement agencies treat the interception of illegal goods, emphasizing the risk and consequences associated with such activities.

Harm Reduction

Embarking on the adventure of exploring different substances requires a fundamental understanding of what exactly you're introducing into your system. We're not here to preach a black-and-white message of "Drugs are bad!" Rather, we encourage you to spend a moment perusing the chart below, which outlines potentially hazardous drug interactions. Dive into the available resources to ensure your safety.

Investing in a test kit for any substances you're considering is a wise move. These are readily available on numerous websites, including DanceSafe.org and even Amazon. Not only are these kits straightforward to use, with clear instructions and examples provided, but they're also cost-effective and capable of conducting several tests—potentially lifesaving.

Additionally, there are services available that offer detailed analyses of the contents of your substances. Leveraging these resources can be a crucial step in safeguarding your well-being.

Avoid putting yourself in harm's way by mixing substances without understanding their interactions or skimping on testing. Safety and informed choices should be your top priorities.

Note: To get a better view of the chart mentioned, you can right-click to save the image or select "view image."

Resources

Dedicate a moment to explore the wealth of information provided in these resources. They offer comprehensive insights on various drugs, the science behind their effects, and direct access to advice from experts. Whether you're seeking guidance during a challenging experience or simply curious, everything you need is accessible here.

Guidance on Dosage and Safety

Embarking on the journey with a new substance, especially if your tolerance has diminished, requires informed preparation. Explore Erowid and PsychonautWiki for reliable advice on appropriate dosages.

Additionally, familiarizing yourself with the "Recovery Position" is crucial. This knowledge could be lifesaving, and it only takes a minute to learn. Please make sure to review it.

PsychonautWiki

[Link to PsychonautWiki]

PsychonautWiki stands as a community-curated digital encyclopedia dedicated to the comprehensive exploration of psychonautics, presented through a lens of scientific integrity. Our mission is anchored in several core objectives:

– Thoroughly cataloging the full spectrum of psychonautic theory and practices, ranging from meditation and lucid dreaming to the use of psychoactive substances

and beyond, all from an evidence-based, scholarly standpoint.
– Offering easily accessible educational resources, advocating for safe practices, and contributing to the cultural shift towards accepting the responsible use of psychoactive substances by leveraging both expert knowledge and community contributions.
– Fostering an environment of free thought and individual sovereignty by providing essential information that enables informed decisions regarding the modification of one's physical and mental states.

Erowid

https://www.erowid.org
Erowid serves as a pivotal, member-supported platform dedicated to delivering unbiased, accurate information on psychoactive plants, chemicals, and their associated realms. Our collaborative efforts with experts from academic, medical, and firsthand experiential backgrounds enable us to create, enhance, and expand the reach of valuable resources. Beyond the dissemination of knowledge, we are committed to safeguarding this information as an archival treasure for generations to come, ensuring that insights into psychoactive substances and their impact remain accessible and accurately represented.

National Harm Reduction Coalition

https://harmreduction.org/
The National Harm Reduction Coalition is at the forefront of advocating for individuals who use drugs, dedicating over 25 years to amplifying their voices and experiences. Our mission is to introduce, support, and widen the implementation of evidence-based harm reduction strategies at the community level.
We are instrumental in ensuring safety through initiatives like providing sterile syringes, distributing Naloxone, and offering fentanyl testing services. Discover how we're making a difference and learn more about our efforts!

Tripsit

https://tripsit.me/
At TripSit, our core mission revolves around fostering an environment where open conversations about harm reduction are not just encouraged but integral. We champion the use of harm reduction tools like test kits and provide guidance and support for safer drug use practices. Our community is deeply committed to sharing knowledge on scientific, medical, and philosophical aspects of drug use, alongside offering advice drawn from personal experiences—a treasure trove of insight for those navigating similar paths.
We stand ready to assist or 'tripsit' individuals who find themselves struggling during drug experiences. Our network includes an IRC chat team, offering round-the-clock live support, from providing quick facts to guiding someone through challenging moments. Additionally, our resources include a comprehensive drug-information wiki for immediate knowledge needs and a live radio service to offer

musical solace to our community members.

DanceSafe

https://www.dancesafe.org/

DanceSafe is a nonprofit public health organization dedicated to promoting safety and well-being within the nightlife and electronic music scenes. Established in 1998 by Emanuel Sferios in the San Francisco Bay Area, DanceSafe has expanded nationwide, establishing chapters in various North American cities. Our Initiatives and Services include:

- Creating safe environments for open discussions on health, drug use, and personal safety.
- Distributing free water and electrolytes to combat dehydration and heatstroke.
- Providing complimentary safe sex materials to prevent unintended pregnancies and the transmission of STIs.
- Offering free ear plugs to protect against hearing damage.
- Delivering accurate, impartial information about drugs to help individuals make informed choices.
- Serving as a nonjudgmental first point of contact for individuals facing risky or difficult situations.
- Conducting drug checking services to reduce the risk of overdoses and fatalities.
- Collaborating with event organizers and local partners to prioritize safety measures.

Through these efforts, DanceSafe champions a health-first approach, ensuring that the nightlife and electronic music communities are informed, protected, and supported.

Drugs and Me

https://drugsand.me/en/

Drugs and Me is an educational platform offering accessible, impartial, and thorough resources aimed at minimizing the immediate and enduring risks associated with drug use. Our team consists of scientists, educators, and analysts who bring a wealth of experience to the field of drug education. Motivated by a desire to curb the rising incidents of accidents and fatalities globally due to inadequate drug knowledge, we strive to make a difference by enhancing awareness and understanding.

DrugWise

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

DrugWise is a comprehensive resource dedicated to providing up-to-date drug information, crafting new reports, and offering a wealth of archival materials from DrugScope, including all Druglink articles since 1986. Beyond its focus on drugs,

DrugWise extends its scope internationally, covering issues related to alcohol and tobacco, particularly the debates surrounding e-cigarettes and diverse perspectives on drug policy and practice.
Recognizing the challenge of scattered resources, we've established I-Know, an international knowledge hub designed to consolidate a wide array of information, policy, and practice materials related to drugs, alcohol, and tobacco. Hosted on our server, I-Know aims to develop into a robust library, ensuring these valuable resources remain accessible for those seeking comprehensive and authoritative insights into these critical public health issues.

SaferParty

https://www.saferparty.ch/

Saferparty.ch is a service provided by the social department of the City of Zurich, managed by Saferparty Streetwork. This initiative offers guidance and support to young individuals up to the age of 28 facing crisis situations, with a special emphasis on the prevention of party drug misuse. Through consistent outreach and relationship-building efforts, Saferparty Streetwork engages with youth who might not connect with other available services. Together with those seeking assistance, it crafts personalized solutions aimed at fostering autonomy and responsible decision-making. This service is available to teenagers and young adults on a voluntary, confidential, and free-of-charge basis.
For inquiries related to substance use, specific substances, or information about our drug checking service in Zurich, please feel free to reach out to us. We're here to help and look forward to assisting you.

SocietalActivities

https://www.societalactivities.org/

SocietalActivities.org is a resourceful platform dedicated to offering valuable aids such as complimentary fentanyl test strips and Narcan spray. Our primary mission addresses the challenges posed by pervasive attitudes of selfishness, individualism, and egotism. While recognizing that these traits can be essential and motivating at a personal level, we also understand that, when magnified across society, they contribute significantly to contemporary issues. By providing these tools and fostering a community of care and support, SocietalActivities aims to counteract these societal tendencies and promote a more collective and empathetic approach to solving problems.

Labs

On this page you can find some labs and drug test results. Curious about the precise composition of your substances? This resource is tailored for you. Particularly for those purchasing in large quantities or intending to distribute, it's crucial to invest time in obtaining a laboratory test. This step ensures you're fully informed about the product's contents, helping prevent any unintended harm.

Energy Control International

https://energycontrol-international.org/

Energy Control International is a collective of individuals, united by a shared concern for the challenges associated with drug use, both in recreational environments and within society at large. Our mission transcends the boundaries of personal drug use, focusing instead on the development of Harm Reduction strategies. We aim to mitigate risks and minimize harm through the provision of information, personalized advice, and educational efforts concerning drug consumption.

Our services include a Drug Checking Service, designed to enlighten users about the contents of their substances, enabling us to guide them towards safer consumption practices. We pride ourselves on delivering tailored, scientifically-backed, and judgment-free drug information specifically aimed at users. This initiative, which began in Spain in 1999, expanded in 2014 to encompass an International Drug Testing Service.

Visitors to our website can access comprehensive reports from our International Drug Testing Service, alongside a wealth of significant peer-reviewed scientific publications. Additionally, our contributions to international congresses, scientific gatherings, and the presentation of conference posters are readily available for those seeking in-depth knowledge on the subject.

DrugData

https://www.drugsdata.org/

DrugsData, previously known as EcstasyData, operates as the autonomous, anonymous laboratory testing initiative under the umbrella of the Erowid Center. This program is dedicated to the acquisition, evaluation, management, and dissemination of laboratory test results. These results include both our own findings and those sourced from various analysis projects around the globe. Our aim is to provide comprehensive and reliable data on substances to inform and educate the public.

Wedinos

https://wedinos.org/

Wedinos provides a crucial insight into the emerging concerns surrounding new psychoactive substances (NPS) usage within the UK and Europe. Evidence suggests that individuals engaging with NPS face significant risks, including immediate physical, psychological, and behavioral consequences, alongside an elevated likelihood of encountering the criminal justice system. The long-term effects, although largely undocumented, present an area of concern that this project aims to address. Through comprehensive research and analysis, Wedinos seeks to enhance our understanding of both the immediate and prolonged impacts of NPS use, offering valuable information to inform public health and policy decisions.

Get Your Drugs Tested

https://getyourdrugstested.com/ (Canada)

GetYourDrugsTested offers a groundbreaking service in Canada, enabling individuals to understand precisely what their street drugs contain. As the world's most extensive database of street drug analyses, this initiative is a community-focused service powered by the Medicinal Cannabis Dispensary. Despite being recognized by Vancouver Coastal Health as an Overdose Prevention Site, it operates without government funding, maintaining its independence.

How We Test Your Drugs

Our facility employs a cutting-edge "FTIR Spectrometer," a device capable of identifying and analyzing drug samples within minutes, all without destroying the sample. By directing an infrared laser onto the substance, the spectrometer examines the reflected light spectrum to pinpoint the exact components of the drug.

Additionally, we provide test strips specifically designed to detect even minuscule amounts of fentanyl or benzodiazepines, enhancing our testing capabilities.

We offer our drug testing services nationwide via mail, ensuring accessibility for all. For those in Vancouver, samples can be directly submitted for analysis at our 880 East Hastings location during business hours.

Vancouver Coastal Health

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

Vancouver Coastal Health (VCH) in Canada is dedicated to offering an array of free and confidential harm reduction services designed to support the well-being of our clients. Our harm reduction initiatives include providing materials for safer drug injection (like needles), safer smoking (such as mouthpieces and push sticks), and safer sex (condoms). These services are integral to VCH's broader public health and addictions strategy, which encompasses prevention and treatment efforts aimed at safeguarding individuals and communities. The primary objective of our harm reduction programs is to prevent infections, illnesses, and injuries associated with drug use and sexual behaviors.

Services Provided Include:

- Education on safer drug use and safer sex practices, along with referrals to health, addiction services, and other forms of support.
- Programs that offer education and access to testing and treatment for communicable diseases, in addition to referrals to counseling services.
- Needle exchange programs designed to ensure the safe recovery and disposal of used needles.
- Supervised consumption sites to provide a safe environment for drug use under medical supervision.
- Overdose prevention and response services to reduce the risk of drug-related fatalities.

- Information and guidance on cannabis (marijuana) use.
- Assistance with referrals for individuals seeking drug detox, treatment, or counseling services.

At VCH, our aim is to maintain the safety and health of both individuals and the community at large by mitigating the risks associated with drug use and sexual activities.

Drug Foundation

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

At the Drug Foundation, we provide a wide array of resources and guidance for individuals using drugs, their families, those who support them, and communities affected by alcohol and other substances. Our mission is to collaboratively eradicate the adverse effects of drug use in Aotearoa New Zealand.

Our harm reduction initiatives currently encompass a variety of services: "Did You Know" for parents, "Living Sober," "PotHelp," "DrugHelp," and "Drugs in Bars," along with efforts to broaden the availability of complimentary drug checking. We're also building an Acute Drug Harm Community of Practice for healthcare providers and professionals; collaborating with agencies to set up an early warning system for drug risks; assisting employers, including the NZ Defence Force and Maritime NZ, to mitigate workplace impairment hazards; supporting employment readiness programs; and enhancing the approach schools take towards drug-related issues.

Suicide Hotlines

For anyone finding themselves in a moment of despair, it's crucial to remember that there is hope and assistance readily available. Across the globe, numerous organizations and helplines are dedicated to offering a compassionate ear and professional support during times of crisis.

Below, I will outline a selection of suicide prevention hotlines by country, designed to serve as a beacon of hope for those in need:

United States

National Suicide Prevention Lifeline: 1-800-273-TALK (1-800-273-8255)
Crisis Text Line: Text HOME to 741741

Canada

Canada Suicide Prevention Service: 1-833-456-4566 (In Quebec: 1-866-277-3553)
Crisis Text Line: Text HOME to 686868 in Canada

United Kingdom

Samaritans: 116 123 (free from any phone)
Campaign Against Living Miserably (CALM): For men in the UK who are down or have hit a wall for any reason, who need to talk or find information and support. Call 0800 58 58 58.

Australia

Lifeline: 13 11 14

Suicide Call Back Service: 1300 659 467

New Zealand

Lifeline Aotearoa: 0800 543 354
Suicide Crisis Helpline: 0508 828 865 (0508 TAUTOKO)

Ireland

Samaritans: 116 123
Pieta House: 1800 247 247 or text HELP to 51444

South Africa

The South African Depression and Anxiety Group (SADAG): 0800 567 567
Lifeline
0861 322 322
SMS 31393

India

Snehi: +91 9582208181
Aasra: 91-22-27546669
Please remember, if you or someone you know is in immediate danger, contact your local emergency services right away. There are people who want to help, and it's important to reach out for the support you deserve.

Darknet Markets

Darknet markets refer to online marketplaces that exist on encrypted networks, like Tor or I2P. These platforms primarily act as clandestine bazaars, facilitating the sale and distribution of illicit goods, including narcotics, unauthorized medications, and steroids, among other items.

FAQ

- **If I'm purchasing only legal items from a market, that means I'm not violating any laws, right?**

Regrettably, the situation isn't that straightforward. Even if the items are legal, you're indirectly supporting a criminal enterprise through market fees and circumventing tax laws of your country. However, it appears law enforcement doesn't prioritize this issue, meaning it's unlikely you'll face legal repercussions for buying legal goods through such a market.

- **Is (Random Market) currently unavailable?**

If you're unable to access the website, it's likely due to a site-wide outage, and you're probably not the only one experiencing this issue. To confirm, visit the market's specific subdread to see if others are facing similar problems. If the issue persists for several hours, consider looking through forums for any updates or announcements about the site's status.

- **Is it safe to just browse Darknet Markets (DNMs) without making any purchases, and without using Tails?**

Absolutely not. Should you be caught, or if law enforcement conducts a search of your premises for any reason, evidence of your DNM browsing could be discovered. Convincing a judge of your innocence and law-abiding intentions would then become significantly more challenging, as your plausible deniability

would effectively disappear. Therefore, it's crucial to take the brief time required to boot up Tails, ensuring you're not making yourself an easy target.

- **Can I recover access to my Darknet Market (DNM) account if I've lost it?**

The ability to regain access to your DNM account varies by market and hinges on the details you can share with their support team. Generally, your most effective approach is to register a new account on the market and reach out to support from there. Offer as much proof as you can to establish that you are the legitimate owner of the account in question, such as details of messages sent, orders placed, account creation date, and so on. After providing this information, the next step is to wait and hope for a positive outcome.

- **Why are the prices so high?**

The principles of supply and demand govern pricing. It's possible that the prices you encounter on the street are lower than those you find on the market. For instance, the market prices for cocaine in Colombia, MDMA in the Netherlands, or cannabis in California aren't likely to undercut the street prices you'd find in those locations.

- **Is it legitimate for a vendor to request payment through PayPal, Western Union, or cash in the mail?**

Absolutely not! Such requests are a red flag for potential scams. If a vendor suggests bypassing the escrow system, you should report them to the website's administration immediately.

- **I deposited bitcoins into my account, but blockchain.info indicates they were sent to a different address!**

Many sites employ a built-in bitcoin 'tumbler' mechanism to obscure the final destination of deposited coins. After this process concludes, your account balance should accurately show the deposited amount. It's important to note, however, that this market system doesn't function as a true tumbler because it handles only 'dirty' bitcoins (those associated with drug transactions) and doesn't incorporate 'clean' bitcoins as a genuine tumbler would.

- **Do prices adjust based on changes in the Bitcoin exchange rate?**

The majority of sites anchor their prices to the USD, meaning prices automatically recalibrate in response to Bitcoin value fluctuations. This ensures the displayed USD price remains consistent, regardless of the Bitcoin exchange rate.

- **What are the odds of getting caught?**

While it's impossible to quantify with an exact figure, the risk is generally low if you meticulously follow all the guidelines outlined in the DNM bible.

- **Is it feasible that law enforcement (LE) might set up a new vendor account to entrap buyers?**

The likelihood of this strategy being employed by law enforcement depends on the legal context within your jurisdiction. Generally speaking, yes, it's possible. However, historical patterns suggest that law enforcement tends to prioritize capturing vendors and subsequently taking control of their accounts to identify

customers. Caution is advised if a vendor's behavior suddenly seems suspicious. In cases of doubt, request the vendor to authenticate their identity by signing a message with their PGP key (and ensure you know how to verify such a signed message).
Should a vendor change their PGP key without verifying the new one with the old key, it's wise to avoid transactions with them until they provide such verification.

- **What are the safest items to buy and ship?**

Certain products, like LSD, are simpler to conceal and ship compared to others, such as cannabis. However, the key factor isn't necessarily which items are safer to purchase, but rather what you intend to buy. By adhering to the guidance provided in the DNM bible—particularly the section on 'How to choose a good vendor'—you're likely to significantly reduce the risk of your order not arriving.

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

It's unlikely you'll face immediate issues, but it's crucial to prevent this from happening again. Ensure you disable JavaScript and adjust the security slider to its highest setting each time you use the Tor browser in the future.

Important tips for using markets

- Always encrypt sensitive information, like your address, yourself. Relying on the market's encryption leaves a vulnerability: the market could retain the unencrypted original of your message while sending an encrypted version to the vendor. This illusion of security means both you and the vendor might believe the information was securely encrypted, even though the market has access to the plaintext. Moreover, if law enforcement takes control of the market, they could collect unencrypted data sent through a 'PGP encrypt' checkbox, all while continuing to forward encrypted messages to vendors to avoid raising suspicion. Personal encryption is the only way to ensure true security.
- Implement Two-Factor Authentication (2FA) for an additional layer of security. This method requires you to decrypt a PGP message with your public key every time you log in, beyond just entering your username and password. Utilizing 2FA significantly enhances your credibility when seeking support from the market, such as in instances of lost funds. It makes unauthorized access to your account considerably more difficult, preventing support from dismissing your concerns as a simple case of phishing. To activate 2FA, navigate to your DNM account settings and select the option to enable 2FA. Ensure you've uploaded your public PGP key in the settings if it's not already done. Follow these steps to create a robust PGP key.
- Avoid using markets that necessitate enabling JavaScript. To understand the risks involved, it's crucial to educate yourself on the subject. [Read about why here.]

- Always transfer only the amount of bitcoins you need to the market, ideally right before you're ready to make a purchase. This minimizes the time your funds are in your market wallet, reducing the risk of theft by the market itself. It's risky to leave funds in your market wallet for any length of time, as they could be stolen at any moment.
- It's crucial to keep your activities on Dark Net Markets (DNM) confidential. The importance of discretion in this matter cannot be overstated.
- Always ensure you use unique usernames, passwords, PINs, or PGP key-pairs for each market you participate in. If a malicious individual or even untrustworthy market staff were to access your account on one platform, they could potentially compromise your accounts on other markets, leading to greater losses such as theft of your funds or deletion of your accounts.
- Avoid using usernames or passwords that could reveal your identity. Ensure your username doesn't provide any hints about your real identity, such as including your birth year or any other personal identifiers.
- Steer clear of services like Privnote that promise self-destructing messages. There's no guarantee these services won't retain your messages after they're supposed to have been deleted. Additionally, they require JavaScript, which poses a significant security risk. Instead, use PGP encryption for your messages, just like other market users, and communicate through the market's internal messaging system. Also, it's wise to avoid vendors who rely on Privnote or similar platforms for communication.
- Avoid tracking your package unless it's significantly delayed beyond the expected delivery time. Tracking it won't speed up its arrival and only serves to leave digital traces. For further information, refer to the section on non-arriving packages. If you find it absolutely necessary to check tracking (which ideally should never be the case), avoid using Tor, as it's a known red flag for law enforcement monitoring Dark Net Market (DNM) users. Instead, opt for third-party tracking websites like TrackingEx or PackageMapping, rather than the official site of your mail carrier. Also, do not use your personal WiFi to check the tracking number. Utilize a network not linked to your identity, such as public WiFi at a cafe, or use a VPN set to a server in your country to avoid suspicion.
- Avoid making your purchase decisions based solely on a vendor's market dominance or their advertisement presence on darknet markets or other websites. Frequently, smaller vendors excel by offering superior products and customer service, surpassing larger competitors in quality and experience.
- Struggling to differentiate between a lowercase 'l' and an uppercase 'I' in

a captcha? The trick is, it's almost always a lowercase 'l'.

- If a vendor unexpectedly switches their PGP key without verifying the change with their previous key, exercise caution and avoid engaging with them until they properly authenticate the update.
- When sending messages, whether on Reddit or a darknet market, aim to convey all your information in a single message. It's frustrating for recipients to be greeted with a flood of notifications, only to find out they stem from multiple messages you sent. Moreover, consolidating your communication into one message makes it simpler for the recipient to respond, enhancing the overall exchange.
- Upon placing an order, its initial status is typically listed as "unaccepted" or a similar term. Once the vendor acknowledges and confirms your order, its status updates to "accepted" or "processing," though the precise terminology can differ across various digital marketplaces. Following this, the order's status progresses to "shipped" or "in transit." The final phase of your order is marked as "finalized" or "completed."
- On digital marketplaces, it's not mandatory to encrypt every message you send. Essential information that's sensitive, like addresses or tracking numbers, must be encrypted without exception. However, for routine inquiries about products, encryption isn't necessary. This approach avoids burdening the vendor with the time-consuming task of decrypting every single message.
- Avoid using "SWIM" or any variations of it, which stands for "Somebody Who Is Not Me." This term is ineffective and will not deter law enforcement in any way. Using it only serves to highlight your inexperience. Instead, focus on enhancing your operational security (OpSec), which is significantly more beneficial for protecting your privacy and safety.
- For enhanced security, it's advisable to remove the version string from your PGP public key. This is the line that starts with "Version:" and is found right below the "—–BEGIN PGP PUBLIC KEY BLOCK—–" line. Eliminating this detail is a simple yet effective measure, as it doesn't compromise the key's functionality but prevents unnecessary disclosure of the software version you're utilizing.
- If you're consistently entering the correct captcha but still can't get past it, try restarting your Tor browser and revisiting the marketplace's address to register. If the issue persists and the marketplace offers multiple onion addresses, attempt to use another one. Should the problem continue, adjust your privacy settings by typing about:preferences#privacy in your address bar or navigating through Edit -> Preferences to select "Privacy" from the sidebar. In the privacy menu, locate the "Exceptions..." button near the unchecked "Accept cookies

from sites" option. Enter the marketplace's onion link in the provided field, select "Allow for Session," and save your changes. To avoid repeating this process, you can opt to leave the "Accept cookies from sites" box checked, which is the default setting.

- Avoid using Tor gateways at all costs. Utilizing them means your login details and all other transmitted data are sent unencrypted across the internet until they reach the Tor gateway. This practice not only exposes your activities to your Internet Service Provider (ISP) but also leaves you vulnerable to theft, as the gateway operator could easily steal your bitcoins. Instead, adhere to the guidelines outlined in the DNM bible, following the same precautions as other prudent users.
- Get a scale. Seriously.
- Employ KeePassXC for creating and safeguarding your passwords for marketplace accounts, Electrum, and PGP. This tool is essential for maintaining strong, unique passwords and ensuring they're securely stored.
- When differentiating between "Bitcoin" and "bitcoin," the key lies in the context. Use "Bitcoin" with a capital "B" when referring to the Bitcoin network or the concept as a whole, such as in "I was learning about the Bitcoin protocol today." On the other hand, use "bitcoin" with a lowercase "b" to denote the currency units, for example, "I sent ten bitcoins today." The abbreviations BTC or XBT are also commonly used to refer to the currency. This distinction helps clarify whether you're discussing the technology/platform or the currency itself.

Types of markets

To make an informed decision about which market best suits your needs, it's crucial to familiarize yourself with the various market types and their associated payment methods. The three primary types you'll encounter are:

- Multisig (Multi-signature)
- Escrow
- Direct Deal

Each type operates uniquely, so it's essential to not only identify a market as, say, an escrow market but also to thoroughly review their guidelines. These guidelines are typically accessible on the market's homepage or through their specific subdread. Taking the time to understand these differences will ensure a smoother transaction process.

Multisignature (Multisig) Markets Explained

To simplify our discussion, we'll focus on multisig markets. This ratio signifies the necessary number of keys required for a transaction. Multisig, short for multi-signature, requires several approvals before finalizing a transaction.

Originally introduced to Bitcoin in 2012, multisig technology has led to the development of multisig wallets and specialized multisig markets, such as Hansa,

CGMC, Cannahome, and Versus. These platforms enhance security by necessitating two or more private keys for transaction confirmation.

Why Multisig Enhances Security:

- **Increased Protection:** To execute a transaction, all required keys must be present, making it harder for unauthorized access.
- **Business Operations:** For crypto businesses with multiple partners, multisig wallets offer a secure way to manage funds, fostering decentralized decision-making.
- **Secure Escrow Services:** Multisig wallets can act as neutral third parties in transactions, holding funds until all conditions are met.

Practical Example:

Imagine a buyer and vendor engaged in a transaction, and the market facilitating this exchange suddenly closes or is compromised. The funds remain secure, as the transaction can still be completed with the signatures of the buyer and vendor. This system ensures funds cannot be unilaterally moved; cooperation between at least two parties (buyer and vendor, or market and one of the parties) is essential.

Choosing Multisig:

Opting for multisig whenever available is wise to mitigate risks associated with market closures or scams.

For specific instructions on using multisig on a Darknet Market (DNM), refer to the help section or wiki of the respective market.

Best Practices for Multisig Wallets:

- Always back up your keys and securely store your mnemonic phrase.
- Distribute keys across different locations or devices for added security.
- Remember, all parties must safeguard their private keys diligently. Failing to meet signing requirements renders the funds inaccessible.

By adhering to these guidelines, you can leverage multisig markets for enhanced security and peace of mind in your transactions.

Escrow

In a typical escrow system, the market acts as a neutral third party that holds the funds during a transaction. These are among the most prevalent types of marketplaces you'll encounter. Here, you transfer your cryptocurrency to a wallet controlled by the market. Once you confirm receipt and satisfaction with your order, you instruct the market to release the funds to the vendor.

Key Points to Remember:

- **Automatic Finalization:** Orders may automatically finalize after a certain period to ensure vendors aren't left waiting indefinitely for payment. It's important to manually finalize if you're satisfied with your purchase to avoid unintended completions.
- **Dispute Resolution:** If your order is unsatisfactory (incorrect quantity, not as described, etc.), you can open a dispute. This action prevents automatic finalization, allowing you to seek resolution with the help of market staff and the vendor. It's advisable to contact the vendor directly

with any concerns before initiating a dispute.

Risks Involved:

However, the escrow system is not without its risks, primarily that the market could abscond with the funds. Historical instances include notable marketplaces such as Sheep Market, Empire, Evolution, Abraxas, Nucleus, and Middle Earth Marketplace falling victim to such scenarios.

Direct Deal

Established vendors might participate in direct transaction platforms or be awarded the status of Finalizing Early (FE) in escrow-based markets due to their longstanding reputation, signifying a higher level of trust.

However, current marketplace guidelines typically prohibit vendors from soliciting buyers to finalize early unless they've officially received FE status. Receiving a request from a vendor to finalize early should raise significant concerns; it's a practice you should avoid.

Finalizing early essentially means transferring your payment directly to the vendor at the time of order placement. This is akin to paying a local dealer upfront and waiting for them to return with your purchase, presenting a substantial risk of fraud, particularly for accounts with minimal transaction history. Your credibility as a buyer could be questioned, and in the event of a scam, the chances of recovering your funds are slim.

Although some vendors might offer discounts for orders finalized early, citing immediate payment as a convenience, the potential pitfalls far outweigh the benefits. This practice is especially discouraged with new vendors, where the likelihood of fraud is even greater.

Choosing a Darknet Market

Navigating the selection of a darknet market can feel daunting due to the sheer number of options available, with new ones launching frequently. It's crucial to conduct thorough research on various markets and vendors independently. Relying on queries in forums like /d/DarknetMarkets for recommendations often leads to biased responses from market promoters or potential phishing attempts. A more reliable starting point is the Superlist, which features a compilation of established markets known for their reliability. Dive into this resource to explore different markets and read through user experiences. Additionally, staying informed on updates and user discussions in market-specific forums (subdreads) before placing any orders is wise. This habit helps you stay informed about any changes in policies and increases your protection against potential exit scams. Remember, each market has its unique procedure for handling orders, so it's advisable to familiarize yourself with the specific user guides provided on their platforms.

Choosing a vendor

The process of selecting a vendor from whom to purchase your desired product is a critical decision that warrants careful consideration to prevent future complications. This choice could be the deciding factor between experiencing a

loss of money without receiving the product, and completing a successful, hassle-free transaction. Take your time to make an informed decision, as it significantly impacts the outcome of your purchase.

Tips

As a newcomer to the marketplace, it's advisable to choose vendors with an established reputation to minimize risks and ensure you're dealing with someone experienced. Here are some key points to consider when looking for a trustworthy vendor:

1. **Vendor Profile and Product Description:** Ensure the vendor's profile and product descriptions are detailed, informative, and free from poor grammar. This reflects their professionalism and attention to detail.
2. **Vendor Feedback:** Opt for vendors with a strong positive feedback history. Ideally, choose those with at least 50 positive reviews and fewer than three negative ones to gauge their reliability.
3. **Product-Specific Feedback:** Be wary of products with disproportionately negative reviews compared to the vendor's other offerings. This could indicate issues with that specific item.
4. **Operational Security (OpSec) Practices:** Avoid vendors who discourage secure practices, such as not encrypting your address with PGP. Good OpSec is crucial for safety.
5. **Vendor Terms and Policies:** Read the vendor's profile, listing descriptions, and terms carefully. Make sure you're comfortable with their policies, including their stance on refunds for new buyers.
6. **Originality of Product Descriptions:** Be cautious of vendors who plagiarize product descriptions from other websites. Original content suggests a more trustworthy vendor.
7. **Vendor Responsiveness:** A reliable vendor should be able to answer questions about their products, shipping methods, etc., indicating their knowledge and commitment to customer service.
8. **Authenticity of Product Photos:** Look for photos that show the actual product with identifiable tags, rather than stock images. Photos should not compromise operational security by revealing unnecessary details.
9. **Recency of Reviews:** Check the dates of the latest reviews. A pattern of old or suddenly negative reviews could suggest problems, such as a potential exit scam.
10. **Presence on Other Markets:** Investigate the vendor's reputation across different markets. High volumes of orders and positive feedback with little to no presence elsewhere could be a red flag for scams.
11. **Review Authenticity:** Be on the lookout for manipulated feedback, such as multiple reviews from the same day or for implausibly low amounts, which could indicate dishonesty.
12. **Exaggerated Advertising:** Steer clear of vendors who make overblown

claims about their products. Honesty and realism in product descriptions are signs of a reputable vendor.

13. **Product Variety:** A vendor selling a wide array of unrelated products might prioritize profit over operational security, increasing risk.
14. **Feedback and Dispute Policies:** A vendor should be open to resolving issues before buyers leave negative feedback or initiate disputes. A policy against neutral or negative feedback without attempting resolution is a major concern.
15. **Listing Views and Sales:** Disproportionate views to sales ratios, especially for new listings, can indicate feedback manipulation. Exercise caution and avoid if unsure.
16. **Pricing and Product Listings:** Be wary of vendors offering bulk products at significantly lower prices than the market rate, as this could be a scam.

When a Vendor Doesn't Accept Your Order

There are occasions when vendors might refuse orders without offering an explanation. This could be due to several reasons:

1. **Item Availability:** Sometimes, vendors fail to update the "items left in stock" feature, or the marketplace lacks this function altogether. As a result, they might cancel the order if they're out of stock.
2. **Bitcoin Value Changes:** Significant drops in Bitcoin value can affect transactions. If you've transferred funds into escrow and the Bitcoin value falls, the vendor ends up receiving less than the original price set for the product. This practice is worth noting; if a vendor consistently cancels orders during Bitcoin's low phases but accepts them when its value spikes (thereby earning more), it may be wise to reconsider future purchases from them.
3. **Buyer Feedback:** Vendors often prefer engaging with buyers who have established feedback and a transaction history. This preference stems from the belief that transactions with experienced buyers are more likely to proceed smoothly and that the risk of dealing with undercover law enforcement officers (LEOs) is minimized. New accounts or those without feedback might be seen as higher risk, as undercover LEOs typically need to make several purchases before targeting a specific vendor.

Tips for Being an Effective Buyer

Being a considerate buyer is as crucial as choosing a reliable seller. Here are several guidelines to ensure transactions proceed smoothly:

1. **Order Responsibly:** Avoid making purchases under the influence. Shopping while sober prevents errors.
2. **Read Thoroughly:** Always fully review the seller's information before placing an order. They may have specific prerequisites or instructions, which can answer most of your queries.
3. **Maintain Politeness:** Courtesy towards the seller and marketplace staff

often leads to better outcomes than expected.

4. **Timely Disputes:** Don't delay disputes until the last moment. Market timings can vary unexpectedly, so initiate disputes well before the automatic completion deadline. Always attempt to resolve issues with the seller before disputing.
5. **Dispute Etiquette:** Stay calm and respectful during disputes. Present your situation clearly, based on facts, without making assumptions. Suggest a fair resolution and be open to compromise.
6. **Communicate Clearly:** Use proper grammar and encryption for sensitive information. Keeping messages concise and clear is appreciated.
7. **Prompt Follow-Ups:** Check in soon after your purchase to address any potential queries from the seller, continuing until the order is confirmed as shipped.
8. **Responsible Feedback:** Only finalize the transaction after receiving your order. Reserve feedback until after evaluating the product, as updates to feedback might not be possible later.
9. **Minimal Communication:** Keep interactions brief. Sellers value their time highly.
10. **Patience is Key:** Understand that delivery times can vary. A typical domestic delivery window is 7 days. This process is not instantaneous like mainstream online shopping.
11. **Tracking Requests:** Only ask for tracking information if there's a significant delay. Check with the seller for any updates first.
12. **Encryption Practices:** Avoid double encryption. Correctly encrypt your address once and refrain from using market's encryption if unnecessary.
13. **PGP Keys:** Your public PGP key need not be included in every message if it's already linked to your marketplace account. Update it as needed.
14. **Honest Feedback**: Leave genuine feedback upon assessing your order.
15. **Realistic Orders**: Don't exaggerate your buying capacity to secure discounts. Honest communication and building a positive purchase history can lead to better deals.
16. **Special Requests**: If you have agreed on specific details with the seller, include that information with your order to ensure clarity.
17. **Error Resolution**: Should you receive incorrect items, inform the seller. This helps them recognize the mistake without obligating you to return the item or make additional payments.

Getting a lawyer

If you get in legal trouble.

Should you find yourself entangled in legal difficulties, it's imperative to understand that this advice is predominantly tailored for those in the United States. Legal norms can vary significantly across borders. For instance, in the UK,

choosing to remain silent could potentially work against you. Therefore, it's crucial to conduct thorough research on the legal practices pertinent to your own country.
In the event that you're confronted by law enforcement under grave circumstances, such as being involved in a controlled delivery, it's essential to refrain from making any statements. Silence is your best defense. Even if you have an exceptional attorney just a phone call away, a simple slip-up in your conversation with the police can lead to severe repercussions, including extensive prison sentences, regardless of whether the self-incrimination was intentional or accidental. To illustrate the importance of how to interact with law enforcement, here's a useful video, along with additional advice from a lawyer who occasionally contributes to Reddit.
Moreover, it's advisable not to refute any allegations. If you haven't been formally arrested but find yourself detained, there are only two phrases you should consider uttering: "Am I free to go?" and a variation of "I need a lawyer immediately," coupled with an invocation of your right to remain silent.
It's also wise to avoid issuing any declarations, as inaccuracies can lead to further charges. Law enforcement may employ intimidation tactics or offer seemingly favorable deals to compel you to speak. It's best to leave any negotiations to the lawyer you have requested.

Selecting and Preparing for Legal Representation

Prioritizing the search for a competent lawyer is an indispensable step that must be taken before you engage in any activities that could potentially lead to legal issues. This preparatory measure is essential because, should you find yourself facing legal challenges, you won't have the luxury of time to vet legal representation thoroughly.
The moment legal difficulties arise, law enforcement officials will likely attempt to engage you in conversations aimed at eliciting admissions of guilt for as many offenses as possible. They are known to deploy various strategies to this end. A proactive defense against such tactics is to secure a lawyer in advance. Should you encounter legal troubles, your best move is to insist on communicating solely through your attorney, thereby sidestepping any traps that may lead to self-incrimination.
It's advisable to research and select two law firms that specialize in drug-related cases and boast a track record of success. Once you've identified two reputable firms, jot down their contact details and office locations on multiple pieces of paper. This precaution is crucial because, in the event of a legal search, your electronic devices could be confiscated. Place these notes in several accessible locations, such as your wallet, desk, and phone case, for easy retrieval when needed.
In the unfortunate event that you're caught up in legal issues, having these numbers at your disposal allows you to promptly secure representation. Should the first firm be unavailable, you have a backup ready. Additionally, it's wise to set aside funds to cover legal fees, ensuring you're financially prepared to engage a lawyer's services.

Another crucial aspect is familiarizing yourself with the specific laws your activities may infringe upon. Understanding these laws can help you mitigate potential penalties by avoiding common legal pitfalls. For example, the presence of firearms in conjunction with drug offenses can significantly escalate penalties in many jurisdictions.

Remember, if you're ever interrogated by law enforcement, your stance should be clear: you only discuss matters in the presence of your lawyer. Do not let intimidation tactics sway you. There's a reason why the adage goes, "No one ever regretted speaking to their lawyer first before talking to the police."

Making a purchase

Completing a Purchase: A Step-by-Step Guide

Ensuring you have your PGP, cryptocurrency, and marketplace account ready is the first step. Now, make sure to back up this crucial data to prevent any loss of access to your accounts and funds.

Essential Tips for a Smooth Transaction

Purchasing on the marketplace can be an exciting process, but there are several key considerations to ensure a successful and safe transaction:

- **For Beginners:** It's advisable for newcomers to start with domestic orders. This provides a simpler introduction to how the process works.
- **Research:** Conduct thorough research on both the marketplace and the seller. This step cannot be overstated in its importance.
- **Product Knowledge:** Make an informed decision about the product you're planning to purchase. Understanding the substances and respecting your body is crucial. Utilize reputable resources like Erowid for dosage guidelines, user experiences, legal status, and other valuable information.
- **Financial Preparation:** Know the exact amount required for the transaction (including the cost of the product, shipping, and any additional fees) and have the cryptocurrency ready. Given the volatile nature of Bitcoin (BTC), consider sending a bit extra to cover any unexpected fluctuations in value. Any surplus can be withdrawn to your personal wallet after the order is finalized.
- **Address Accuracy:** Carefully input your shipping address, adhering to the vendor's specifications or the standard format for your country. Missteps here can lead to legal complications and dissatisfaction from the seller. Save your correctly formatted address in a secure .txt file for future orders, and always verify if the vendor requires a different format.
- **PGP Encryption:** Encrypt your shipping address with PGP and include it in the designated order or buyer notes section of the marketplace.
- **Corrections:** Should you err in providing your address, notify the vendor promptly to rectify the mistake.
- **Payment Security:** Opting to keep funds in escrow or using Multi-

Signature transactions can protect against vendor exit scams.
- **PGP Key:** If you've already added your public PGP key to your profile settings, there's no need to include it in direct messages to the vendor.
- **Realistic Expectations:** If an offer seems too good to be true, it likely is. Approach such deals with caution.
- **Shipping Misconceptions:** Understand that "overnight shipping" rarely means the item will arrive the next day. Adjust your expectations accordingly to avoid disappointment.

Providing Feedback

Providing feedback and assigning ratings to a vendor is crucial, rivaling the importance of secure transactions such as escrow or multi-signature protocols. Your feedback serves as a crucial communication tool for the vendor and potential future customers, helping to shape the vendor's business practices. Approaching the feedback process with seriousness is essential, as it is a key mechanism for ensuring accountability and maintaining the quality of products available in the marketplace. The collective feedback and ratings from customers play a critical role in the vendor selection process. Consider the following key aspects when evaluating a vendor:

- **Communication:** While minimal communication might be necessary, the emphasis should be on the timeliness and professionalism of the vendor's responses.
- **Efficiency:** Evaluate how quickly the vendor processes and ships orders. Note that delivery times can vary due to external factors beyond the vendor's control, such as shipping services, holidays, and weather conditions.
- **Packaging:** Proper vacuum sealing is crucial for maintaining product integrity. Additionally, packaging should offer sufficient stealth and protection against scent and weather damage, especially if the package is compromised during transit.
- **Product Weight:** The quantity received should match what was purchased. Acknowledge both instances where the quantity exceeds expectations (heavy packs) and when it falls short (light packs).
- **Product Purity:** The product should meet the advertised quality and purity standards. Ensure the product's specifications are clear before leaving any feedback or rating.

Feedback and ratings not only impact the vendor's business but are also invaluable to the broader community. Your contributions remain as long as the vendor's shop is active, providing anonymous guidance to other users. To ensure your feedback is constructive, consider these tips:

- **Timeliness:** Leave feedback only after receiving and inspecting your order, coinciding with the completion of your transaction.
- **Honesty:** Provide truthful feedback to set accurate expectations for

future customers.
- **Context:** Understand the unique nature of transactions on the darknet compared to mainstream platforms like Amazon. Consider the significant impact of ratings on a vendor's business, and strive to be fair and reasonable.
- **Resolution:** Before leaving negative feedback or a less-than-perfect rating, attempt to resolve any issues with the vendor. A courteous approach may lead to a satisfactory resolution, allowing for positive feedback.

Handling Threats or Blackmail from a Vendor

Encountering threats or blackmail from a vendor can be alarming. Occasionally, vendors might escalate situations unreasonably, including threats to disclose your personal information (doxxing) or alert law enforcement. If you find yourself in this predicament, it's crucial to maintain your composure and take strategic steps to protect yourself. Moreover, promptly reporting the vendor to the marketplace administration is essential. When communicating with the market staff, ensure your message is clear, polite, and devoid of panic or insults. This approach maximizes your chances of resolving the issue favorably and potentially getting the vendor banned.

If you've adhered to the principles of being a conscientious buyer, maintaining polite and respectful communication, you'll likely be in a more advantageous position. The market staff will be able to discern your reasonable demeanor, contrasting with the vendor's irrational behavior.

Threats of involving law enforcement are generally empty, as executing them would compromise the vendor's operational security and be unduly burdensome just to target one buyer. These threats are often intended to intimidate you into compliance.

Nevertheless, as a precaution, ensure your residence is free of any illegal or suspicious items. In the unlikely scenario of a law enforcement visit, this preparation helps maintain your innocence. The possibility of the vendor physically confronting you is minimal; such threats are typically bluffs by individuals hiding behind the anonymity of the internet. It's also wise to pause any new purchases until the situation is fully resolved.

You have the option to publicly call out the vendor on platforms like /d/ DarknetMarkets, provided you also share evidence of their misconduct. This step should be taken with caution, ensuring you do not compromise your own privacy or safety.

Operational Security in Real Life (IRL OpSec)

This section focuses on enhancing operational security (OpSec) in aspects of your life that aren't directly linked to Darknet Markets (DNMs). It covers practices such as reselling, which might be relevant if you're engaging in activities that your acquaintances wouldn't typically support or understand, like setting up secure communication channels just for basic interactions.

The Cardinal Rule: Silence is Golden

The most critical principle in maintaining operational security is absolute discretion about your sources and methods. You should never disclose the origin of your products to anyone, under any circumstances. The pressure to share your secrets, even with close friends, must be resisted to safeguard your operations and personal security.

Remember, once information is shared, it cannot be unspoken. If even a single person is privy to your activities, there's no telling how far that information might spread. Invariably, when someone is cornered by law enforcement, they might divulge everything they know to lighten their own legal burdens. This could lead directly to your doorstep, potentially costing you not just your privacy but also significant legal expenses.

Real-world examples abound of individuals facing legal consequences because someone else failed to maintain secrecy:

1. An investigation into 18-year-old Ryan Andrew Backer followed after authorities were tipped off about LSD shipments from the Netherlands to him.
2. The arrest of a university student for ordering and reselling LSD originated from a suspicious package received from Hawaii, leading to police intervention and legal action.

When questioned about your sources, a vague response citing an unspecified "guy" without further details is prudent. Persistent inquiries should prompt you to reconsider the nature of your relationship with the questioner. Anyone who cannot respect your privacy is a potential risk.

Communication Strategies

Expect confusion or resistance when suggesting the use of PGP encrypted emails to friends or customers. Adapting your communication methods without compromising evidence is crucial.

- **Securing Communications:** Familiarize yourself with and follow security guidelines for iPhone or Android devices to minimize prosecutable evidence. Encourage the use of encrypted messaging apps like Telegram or Signal among your contacts, ensuring features like automatic message destruction (e.g., after 24 hours) are utilized. Advocate for full disk encryption on devices with a strong passphrase.
- **Avoid Cloud Backups:** Disable iCloud or Google Cloud backups for messages and photos, as law enforcement can easily access these with a subpoena.

Adhering to these principles not only enhances your operational security but also significantly reduces the risk of legal repercussions stemming from your activities or associations.

Alternative Communication Strategies

Typically, the internal messaging system of the marketplace suffices for buyer-seller interactions. Nonetheless, under circumstances such as the marketplace

experiencing downtime, the need for alternative methods of communication may arise to maintain contact with vendors. The subsequent sections will focus on how to employ these alternative strategies effectively, ensuring your operational security (OpSec) remains uncompromised.

Email

It's important to remember that email services, particularly those hosted on .onion domains and operated anonymously, can unexpectedly cease operations. This has occurred frequently in the past and is likely to continue. To mitigate risks, regularly back up essential emails and avoid linking critical accounts, such as those used for two-factor authentication (2FA) on significant Bitcoin trading platforms, to these email addresses.

For secure email communication, consider the following guidelines:

- **Select a Reputable Email Provider:** Opt for a provider with a strong reputation for security and privacy. Research on platforms like Dread can help identify services that accommodate Tor users and are known for their resistance to government inquiries.
- **Javascript Disabled:** Choose an email service that functions fully without the need for Javascript, enhancing your security.
- **Encrypt Your Communications:** Utilize Pretty Good Privacy (PGP) encryption for all outgoing emails and confirm that your correspondents do the same. This step is crucial for maintaining the confidentiality of your messages.
- **Be Cautious with Email Subjects:** Avoid divulging sensitive information in the subject line. Even with PGP encryption, the subject remains unencrypted and could reveal too much. Instead of specific details like "about the $4k drug deal we made," use neutral placeholders such as "subject" to maintain privacy.

Jabber / XMPP

XMPP Overview

XMPP (Extensible Messaging and Presence Protocol) is a versatile communication protocol that facilitates instant messaging between two or more participants across networks, akin to services like Skype or Facebook Messenger. Originally called Jabber, this protocol is sometimes still referred to by its original name.

By following the guidelines provided, you can enable real-time, end-to-end encrypted messaging at no cost.

OMEMO Encryption

Developed by Andreas Straub, OMEMO is an advanced XMPP extension designed for secure messaging across multiple devices. Utilizing the Double Ratchet Algorithm, OMEMO ensures that messages are encrypted end-to-end, supporting synchronization across several clients, even when some are not online. The acronym "OMEMO" stands for "OMEMO Multi-End Message and Object Encryption," highlighting its capability for secure multi-device communication. As

an open standard, it leverages both the Double Ratchet Algorithm and the Personal Eventing Protocol (PEP, XEP-0163) to offer features like future and forward secrecy, deniability, and the ability to deliver messages offline. Compared to OTR (Off-the-Record Messaging), OMEMO provides additional benefits such as group chat encryption, message queuing for offline users, file sharing, and both verifiability and deniability, albeit with a minor increase in message size.

OTR (Off-the-Record Messaging)

Although OTR and the messaging client Pidgin are included in some security-focused software bundles like Tails, their technology is becoming outdated. Transitioning to OMEMO is highly recommended for enhanced security features. Pidgin is a versatile, open-source messaging client that supports various messaging protocols, enabling users to connect to different messaging services like Facebook, Google Talk, and AIM from a single platform. Pidgin is renowned for its Off-the-Record (OTR) plugin, which provides end-to-end encryption for secure conversations. To use this feature, both parties must have the OTR plugin installed, though it is not necessary for both to use Pidgin. The OTR plugin employs Perfect Forward Secrecy to prevent third parties from intercepting messages, though it cannot prevent a chat partner from logging conversations.

Setup Gajim+OMEMO

This guide is your go-to resource for mastering communication via Gajim and OMEMO, the preferred method for interacting with XMPP clients. For those with an existing XMPP account from applications like Pidgin, we'll walk you through the seamless transition to Gajim and introduce you to the essentials of utilizing OMEMO. Remember, encrypted conversations are only possible if both parties have OMEMO installed; otherwise, your messages will be unencrypted. Encourage those without OMEMO to install it for secure communication.

Important: Gajim does not support OTR by default.

Initial Setup

Before diving into Gajim on Tails, ensure you've activated persistent storage and enabled the Additional Software option, along with setting up a root password upon startup.

Installation Process

Follow these steps to install Gajim:

1. Navigate to Applications -> System Tools -> Synaptic Package Manager.
2. In the Package Manager, use the search function on the right to find "gajim-omemo."
3. Select "gajim-omemo" for installation and confirm your choice.
4. After clicking "Apply," confirm again in the new window and set Tails to install Gajim upon each startup.

Creating Your XMPP Account

New to XMPP? Here's how to create your account and set up OMEMO:

- Choose a service provider; we recommend calyxinstitute for this guide,

but feel free to select another.
- Launch Gajim and on the welcome screen, choose “Sign Up.”
- Enter “jabber.calyxinstitute.org,” enable advanced settings, and proceed to sign up with these specifications:
  - – Proxy: Tor
  - – Hostname: jabber.calyxinstitute.org
  - – Port: 5222
  - – Connection Security: StartTLS
- Create your username and password, and you’re ready to go with Gajim+OMEMO!

Chatting with Gajim+OMEMO

Initiating a chat is straightforward. After adding a contact and vice versa, you can start your conversation. Look for the lock icon in the chat box to enable OMEMO and ensure to verify the OMEMO fingerprints for secure communication.

Transferring Your XMPP Account to Gajim

To migrate your existing XMPP account to Gajim and use OMEMO:

- Install Gajim as outlined above.
- On the welcome screen, input your account details, enable advanced settings, and log in with:
  - Proxy: Tor
  - Hostname: (Your current XMPP host)
  - Port: 5222
  - Connection Security: StartTLS
- Once logged in, access your OMEMO fingerprint by pressing Ctrl+E, selecting the settings wheel on the OMEMO plugin, and there you have it!

Congratulations! You’re all set to enjoy secure communication with Gajim+OMEMO.

Setup Pidgin+OTR

In this tutorial, we’ll use The Calyx Institute as our example for setting up a Jabber (XMPP) account. The Calyx Institute is known for its public jabber servers, transparent data retention policy, and commitment to privacy. You can find more information about them [here](#).

While we recommend The Calyx Institute for its privacy features, you’re free to choose another provider. For alternatives, check out [this list](#). Note that settings may vary depending on your choice.

Setting Up Pidgin with the OTR Plugin

1. 1. **Launching Pidgin**: Navigate through Applications (top left) -> Internet -> Pidgin Internet Messenger. Two windows will open.
2. 2. **Activating OTR Plugin**:
   - – In the “Buddy List” window, go to Tools -> Plugins.
   - – Scroll down to find “Off-the-Record Messaging” and ensure it’s checked.

- – Select it and click “Configure Plugin”.
- – Enable the following options:
  - – “Enable private messaging”
  - – “Don’t log OTR conversations”
  - – “Automatically initiate private messaging”
- – Close both the configuration and plugin overview windows.

Registering an XMPP Account

To communicate via XMPP, you’ll need an account. XMPP servers have varying policies on data logging, but those listed in our services are privacy-conscious. If using Tor (via Tails or Whonix), your privacy is further enhanced. Note that some servers might require you to register through their website.

1. **Account Creation:**
   - In the “Buddy List” window, select Accounts -> Manage Accounts.
   - Click “Add” and input the following:
     - Protocol: XMPP
     - Username: YourDesiredName
     - Domain: jabber.calyxinstitute.org (or another server from the list)
     - Resource: Leave this blank.
     - Password: Choose a strong, unique password.
     - Ensure “Create this new account on the server” is checked.
2. **Advanced Settings:**
   - Set Connection Security to “Require Encryption”.
   - Connect Port: 5222
   - Connect server: jabber.calyxinstitute.org
   - Leave File transfer proxies and BOSH URL blank.
   - Opt for a hidden service server if possible.
3. **Finalizing Setup:**
   - Click “Add”, then log in with your new credentials when prompted.
   - Accept any certificates if necessary.
   - Enable your new account in the “Accounts” window to go online.

Upon successful setup, you’ll receive a welcome message with further information, such as The Calyx Institute’s Twitter account and encouragement to donate if you find their services useful.

This guide aims to help you securely set up and use XMPP with a focus on privacy and security. Whether for personal or professional communication, following these steps will ensure a safer online chatting experience.

Using pidgin+OTR (XMPP)

Starting a conversation with someone

Once you’ve set up your Jabber account, adding a new contact involves a few steps. First, navigate to Buddies > Add Buddy. If you find that the “Add Buddy” option is greyed out, try closing and reopening all Pidgin windows.

Next, type in the username provided by your contact, which might look something

like username909@jabber.calyxinstitute.org. You have the option to assign a nickname to this contact, which will be displayed in your chat window for easier recognition, instead of the longer username. To finalize adding them, simply click on “Add”.

The person you’re trying to add will be notified to authorize your request the next time they’re online. They’ll see your username and must click “Authorize” to proceed. A follow-up dialog allows them to set a nickname for you as well.

Once they’ve authorized you and are online, their name will appear in your “Buddies” list. You might also notice a small notification at the bottom of your “Buddy List” window indicating they want to add you. Make sure to click on authorize.

Now, to start chatting, double-click their name in your buddy list. To ensure privacy, click on the red “Not private” button at the bottom right corner and select “Start private conversation”. You’ll see a few system messages indicating the initiation of a secure chat.

And there you have it – you’re all set for a secure chat session!

Authenticating your buddy

When engaging in a secure chat, you might notice an “unverified” status at the bottom right of your chat window, indicating that the person you’re conversing with could potentially be someone else, possibly even a malicious actor. This situation arises if you’re unsure whether the communication channel through which you received their XMPP username was secure.

If the XMPP username was shared over a channel you trust, like an encrypted message, you might choose to bypass further verification. However, if there’s any doubt—say, the username came via an unsecured message on a Darknet Market (DNM), which could have been compromised by law enforcement or other entities—it’s crucial to authenticate the identity of your chat partner.

To do so, click on the “Unverified” label located at the bottom right and select “Authenticate Buddy”. Here, you will be prompted to enter a question and a secret answer. A practical approach could be using a question like “check your email account” with a secret answer that’s a unique combination of characters, such as “Rw!M{t”. Before proceeding to authenticate, share this secret answer with your buddy through a secure method, such as an encrypted email using their PGP key, ensuring the communication remains between you two.

After sending the secret answer securely, proceed by clicking the “Authenticate” button. This action initiates a waiting period for the authentication process to complete. Your chat partner will be prompted to answer the question you set. Successful entry of the correct answer will change the status in your authentication window to “Authentication successful”, which you can then close by clicking “OK”.

This process not only confirms the establishment of a secure chat connection but also verifies you are indeed communicating with the intended individual. Your chat partner may also initiate a similar authentication process, allowing both parties to be verified.

Upon successful authentication, the status will change to a green “Private”, indicating a secure and verified communication channel.

Services

Here’s a list of other renowned services you might consider exploring. Be sure to verify their server names and port numbers in their configurations.

- 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

Miscellaneous information

While you might not use the guides in this section immediately, it’s worthwhile to familiarize yourself with their contents. This will enable you to reference information from them should the need arise. We plan to enrich this section with more useful information over time.

Javascript

JavaScript Warnings

If you’re using JavaScript, you’ve likely encountered warnings on various websites by now. While JavaScript itself isn’t inherently harmful, it can be exploited in certain scenarios to compromise your anonymity.

This is a key reason we advocate for keeping your darknet and clearnet activities entirely separate. Some sites can use JavaScript to uncover your real IP address, even when using Tor.

Disabling JavaScript

Important: This adjustment must be made every time you restart Tails!

1. Upon launching Tor, click on the dice icon located in the upper right-hand corner.
2. Select “Advanced Security Settings.” A window similar to this will appear:
3. Choose “Safest.”

Please Note: You might still receive messages from websites indicating that JavaScript is enabled. This occurs because it’s being blocked by NoScript, which might not catch everything. For enhanced security, after setting the security level to “Safest,” follow these steps:

1. Type `about:config` in the address bar.

2. Click “Accept the Risk and Continue.”
3. In the search bar, type “java.”
4. Near the top of the list, you’ll find an option labeled `javascript.enabled`. Double-click it to change its value to false.

And that’s it—you’re all set!

Removing exif data from images

At some point, you might need to capture a photo of a product you’ve purchased, possibly for a review or because you’re in the middle of a dispute.

Understanding EXIF Data

EXIF, or Exchangeable Image File Format, is a standard that allows information to be stored within an image file. When you snap a photo with your smartphone or camera, it embeds details ranging from the device used to precise GPS locations. It’s crucial to strip this EXIF data from your image before uploading it anywhere.
Important Reminder: Never rely on a website or service to eliminate the EXIF data for you. There’s always a risk they could retain a copy of the original image.
Fortunately, Tails offers an efficient tool to help you remove this data safely:

1. Right-click the image file from which you want to remove the data.
2. Select “Remove Meta Data” from the context menu.
3. A new file will be generated, purged of all EXIF data, ready for safer sharing.

Secure Image Uploading Guide

Uploading images can inadvertently disclose a wealth of information, potentially compromising your anonymity despite adhering to all other digital security measures outlined in guides like the DNM Bible. The distinction between maintaining your freedom and facing legal consequences can be as simple as following the guidelines in this chapter.
Consider what basic forensic photo/video analysis software can accomplish, and then imagine the capabilities of advanced forensic tools that law enforcement agencies can access with substantial funding.

Taking Photos Safely

Even if you implement every precaution recommended in this chapter, it’s still feasible to trace the image back to your camera through specific data unique to your device, which is much more challenging to conceal. Hence, it’s strongly advised to use either a disposable camera or a device that has never been used to upload images online.
To transfer images from your camera or smartphone to Tails, insert the SD card into your computer or connect your mobile phone with a USB cable after booting into Tails.

Removing Digital Traces

To minimize traces in the images you intend to upload (though not a guarantee against all forensic techniques), follow these steps:

1. Right-click the image, hover over “Open With,” and choose “GNU Image Manipulation Program (GIMP)” from the context menu.

    - For easier navigation, enable Single-Window Mode by selecting “Window” at the top and choosing “Single-Window Mode.”
2. Use the “Crop Tool” from the toolbox to eliminate background elements that might identify you. After selecting the desired area, press Enter.
3. Add noise to the image to obscure any sensor-specific characteristics that could be used for identification. Navigate through “Filters” > “Noise” > “HSV Noise.” The default settings usually suffice, but you can adjust the noise level for added paranoia while ensuring the image remains comprehensible.
4. To save the edited image, click “File” > “Export As...” and save it to your Persistence folder. Deselect all optional metadata entries, such as “Save resolution,” to ensure no identifiable information is stored.

Note: This process also eliminates EXIF data, which includes details that could de-anonymize you, such as the GPS coordinates where the photo was taken. With these steps, such information is no longer a concern, offering an added layer of anonymity to your online image uploads.

OpenBazaar

This section provides insights into OpenBazaar, a more secure and decentralized alternative to traditional darknet markets. Although using OpenBazaar is optional, it’s highly recommended to consider this platform, especially if a vendor promotes their OpenBazaar store in their profile on a conventional market.

Introduction to OpenBazaar

OpenBazaar (abbreviated as OB) is an open-source initiative aimed at creating a protocol for conducting e-commerce transactions within a completely decentralized marketplace. Initially supporting Bitcoin, there are plans to expand its cryptocurrency support in the future.

Essentially, OpenBazaar operates similarly to the darknet markets you’re familiar with but stands out by its decentralized nature—eliminating the possibility of a single point of failure through server seizure. This model gives vendors full control over their stores, meaning law enforcement would need to directly target a vendor to disrupt their operations. Even in such cases, only the affected vendor would be taken down, allowing the rest of the marketplace to continue operating normally.

However, it’s critical to acknowledge that, like any system, OpenBazaar isn’t immune to potential bugs or vulnerabilities that could jeopardize its stability or the anonymity of its users. Therefore, setting up OpenBazaar correctly and adhering to best practices outlined in the DNM bible is vital. Skipping steps or looking for shortcuts could put your safety and future at significant risk. Committing to thoroughness in your setup and operations can safeguard your interests in the long term.

Setting Up OpenBazaar on Whonix

To install OpenBazaar (OB) on Whonix, you’ll need to carry out a series of steps on the Whonix Workstation. Begin by launching the Konsole application; you can do this by double-clicking the “Konsole” icon on your Workstation desktop. Once

open, enter the following command to update your system. You can copy and paste this command into the Konsole by right-clicking within the window and selecting “Paste”:

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

This command ensures all your installed software is updated to the latest version. During this process, you’ll likely be prompted to enter the password you created during the Whonix setup—make sure you have it ready.

Then open the Tor Browser which is also linked on your desktop and visit the OB download page. Within the download section, look specifically for the Linux options and find the one labeled “32-bit (deb)”. Click on this link to proceed.

When prompted with a dialog box asking where to save the file, initiate the save process by clicking on the “<” symbol located between the “Save in folder:” label and the “Browser > Downloads” path. After that, click on “user” found within the new file path that appears between “> home >” and “> .tb > tor-browser > Browser > Downloads”. Navigate to the “Desktop” folder by double-clicking on it and conclude by clicking the “Save” button to download the file directly to your desktop for easier access.

This guide aims to clarify the saving process for your files, emphasizing the importance of storing them in the correct directory. Ensure you save your file in the standard user directory rather than the Tor browser directory. Despite their similar structures, saving in the Tor browser directory could lead to confusion and difficulty in locating the file later.

Upon completing your download, which is indicated by the download icon next to the address bar in your Tor browser, navigate back to your desktop. There, verify the presence of only one file with the OB label. If two files appear, one might be named something like “openbazaar2_2.0.18_i386.deb.part,” indicating the download is still in progress. Wait until this partial file disappears, signifying the completion of your download.

Next, right-click on the final downloaded file, select “Properties,” then go to the “Permissions” tab, and tick the “Is executable” checkbox before clicking “OK.”

Note: At the time this was written, OpenBazaar didn’t offer a method to verify the integrity of the downloaded file (e.g., through a signature file or hash), posing a potential security risk. Though the file’s transmission is encrypted, an attacker with access to the download server could potentially replace it with a harmful version.

You’re nearly there! Begin by launching the Konsole application, which can be done by double-clicking the “Konsole” icon. Once open, execute the following command to start the installation of OpenBazaar. This can be done by copying the command below, then right-clicking in the Konsole window and selecting “Paste”:

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

After entering the command, you'll be prompted to input your password. Following this, you may notice error messages related to missing software required for OpenBazaar (referred to as dependencies). There's no need to worry—these errors indicate what needs to be addressed for a successful installation.
To automatically install the necessary software and resolve these dependencies, ensuring your OpenBazaar installation completes without issue, enter the next command:
"`
sudo apt-get -f install
"`
When prompted with "Do you want to continue? [Y/n]," press ENTER to affirm and proceed. Allow the command to run its course, which will finalize the setup process for you.

Congratulations! You've successfully installed OpenBazaar. To launch it, navigate to the Application Launcher, identifiable by the small "K" icon located at the bottom left corner of your screen, reminiscent of the Start Menu in Windows. Once there, type "open" in the search bar. You should see an entry labeled "OpenBazaar"—click on it to proceed.
Upon opening OpenBazaar, a dialogue may appear after some initial loading. It's important here not to check the box labeled "Use Tor." Given that Whonix is already routing all your internet traffic through Tor, this layer is unnecessary. Simply click on the "Save" button and patiently wait until you are brought to a screen featuring a "Get started >" button. Clicking this moves you forward to the next step.
You will then be asked to provide some personal information. For your privacy and security, avoid using your real name. Opt for a nondescript username, such as "MichaelTheMan"—especially if your name isn't Michael, to avoid any direct identification. It's also wise to skip including details like your birth year or any information that could compromise your anonymity. You may select your preferred currency but leave the other options untouched to maintain operational security. Remember, details like your country can be disclosed to vendors when you share your PGP encrypted address, and choosing an avatar might risk leaking digital traces that could lead back to you.
Finally, after filling in your details, proceed to the next step by clicking "Next." Take a moment to review the Terms of Service before agreeing to them. This ensures you are informed about the platform's rules and your responsibilities as a user.

Customizing the settings

To complete the setup of your OpenBazaar (OB) profile, you'll need to tweak a few settings. Start by navigating to the "Home" tab and clicking the "Customize" button. From here, move to the "General" tab on the left side. Here, you'll find an option labeled "Display Mature Content." Change this setting to "Yes" and confirm by clicking the "Save" button.
Next, head over to the "Store" tab. Since you're not planning to sell items, for

enhanced security, turn the “Store” option to “Off.” Don’t forget to hit the “Save” button at the top right to apply your changes.
The following step involves the “Shipping Addresses” tab. It’s crucial not to input your real address for safety reasons. Instead, create a placeholder using your OB username as the “Name” and select either the default country or your actual location for the “Country” field. Leave all other fields blank. Vendors will receive your genuine shipping details through a PGP encrypted message included in your order notes, allowing you to maintain privacy while providing necessary information for order processing. Setting your country is relatively low risk and can assist vendors in managing their orders more effectively, such as by avoiding orders from countries they do not ship to.
After setting up your dummy address, click the “Save” button. Your OB setup is now complete, and you’re all set to explore the marketplace with confidence, free from the concern of encountering a seizure notice.
Finding a Vendor and Using OB Store Links:
If you’ve already identified a vendor, accessing their OB store is straightforward. Look for a link that starts with “ob://” followed by a sequence of letters and numbers, which may end with “/store.” Copy and paste this link into the address bar at the top of your OB interface, similar to how you would in a standard browser like Tor.
Note:
Exercise caution when dealing with vendors on OB. There’s no absolute assurance of legitimacy, and the risk of encountering law enforcement or sellers with manipulated feedback exists. Thoroughly vet any vendor prior to making a purchase.
Tips:
Create a desktop shortcut for OpenBazaar for quick access. Simply go to the Start Menu, search for “open,” then right-click on OpenBazaar and select “Add to Desktop.” This shortcut streamlines the process of launching OB, making your experience smoother.

I2P

What is i2p?

I2P, short for The Invisible Internet Project, is a network technology similar to Tor, designed to offer a private layer over the internet. It serves as a robust alternative, particularly addressing some vulnerabilities in Tor that have made it susceptible to Distributed Denial of Service (DDoS) attacks against its services. Increasingly, various online marketplaces are adopting I2P to circumvent these issues, highlighting its growing relevance in the pursuit of digital privacy and security.
At its core, I2P establishes a secure, encrypted peer-to-peer network, effectively obscuring both the users and servers from each other. It operates entirely within its network, ensuring that all traffic is confined to I2P and never directly interacts with the broader internet. This isolation is achieved through encrypted, one-way tunnels between users, rendering the traffic’s origin and destination anonymous.
One of I2P’s defining characteristics is its near-complete decentralization. Upon

joining the network, users connect with peers by creating exploratory tunnels, which are initially facilitated by trusted reseeding servers. This method not only secures your initial entry into the network but also enhances connectivity and speed over time as your network contribution grows.
It's crucial to note that I2P is primarily intended for accessing hidden services within its network, as it doesn't officially support exiting traffic to the regular internet—a process known as outproxying. This design choice underscores I2P's commitment to privacy, suggesting users opt for Tor Browser for general internet browsing needs. While I2P offers significant privacy advantages by keeping traffic within its network, it's important to recognize and navigate its limitations carefully, ensuring a thorough understanding and adherence to provided setup instructions for optimal security.

How Secure is I2P?

In the I2P network, each node plays a role in routing packets for others, requiring your IP address to be visible for connection setup. Although it's apparent that your device is using I2P, your specific actions remain private. Whether you're exploring eepSites, sharing files, conducting research, or simply donating bandwidth, your activities are concealed. However, it's crucial to remember that I2P does not hide your identity on the traditional internet by itself. For comprehensive protection, I2P should be complemented with additional privacy measures, which we'll discuss in subsequent sections.

How can I run I2P?

- **Android:** Beginner Level (Least secure and least recommended)
- **Linux (Ubuntu):** Intermediate Level (Moderately secure and beginner-friendly)
- **Tails:** Note: Incompatible with Tails version 5 and above
- **Whonix on Qubes:** Expert Level (Highly secure, offering maximum privacy)

Utilizing mobile devices introduces significant operational security (opsec) risks. This guide advises against mobile use for I2P activities. Its inclusion here aims to assist those already using I2P on mobile to enhance their security. However, it's important to understand that mobile devices are generally inadequate for robust opsec.

How to install I2P on Tails?

Installing I2P on Tails requires a thoughtful approach, given the emphasis on privacy and security inherent in both tools. Here's a step-by-step guide to set you on the right path:

1. **Start Tails:** Boot up your Tails system. Remember, Tails is designed to run from a USB stick or DVD, ensuring your privacy by not leaving traces.
2. **Configure Persistence (Optional):** If you want your I2P installation and configuration to persist across sessions, you'll need to enable persistent storage in Tails. This can be done from the Tails Greeter when you start up. Go to Applications > Tails > Configure persistent volume.

3. **Enable Unsafe Browser (Temporarily):** Since Tails is configured for maximum security, you'll need to temporarily enable the Unsafe Browser to download I2P, as it might not be directly accessible through the Tor Browser. To do this, go to Applications > Tails > Tails Greeter settings > Additional Settings > Unsafe Browser.
4. **Download I2P:** Use the Unsafe Browser to go to the official I2P download page and download the I2P installation package for Linux. Make sure to verify the integrity of the download using signatures or checksums provided on the site.
5. **Install I2P:** After downloading, you'll need to install I2P. This might require opening a terminal and navigating to the directory where you downloaded the file. Typically, the command will be something along the lines of `dpkg -i i2p*.deb` or following the specific installation instructions for Linux on the I2P website.
6. **Configure I2P to Start Manually:** Tails does not save software installations between sessions for security reasons. If you have enabled persistence, you can configure I2P to start manually so you can control its use. This involves editing some configuration files or creating scripts that run at startup, depending on your preference and security needs.
7. **Start I2P and Configure Your Browser:** Once installed, start I2P and configure your browser to use I2P. This usually involves setting up a proxy. Instructions can be found in the I2P documentation.
8. **Disable Unsafe Browser:** After you've finished setting up I2P, make sure to disable the Unsafe Browser to maintain the security integrity of your Tails session.
9. **Explore I2P Safely:** Now that I2P is installed and configured, you can explore the I2P network with an emphasis on privacy and security.

Remember, while Tails and I2P are powerful tools for maintaining privacy online, their effectiveness depends on proper configuration and usage. Always stay updated on best practices and potential vulnerabilities.

For the most current and detailed information, including any changes to the installation process after my last update in April 2023, please refer to the official Tails and I2P documentation.

Important

For those wishing to return to standard web browsing via Tor after using I2P, it's crucial to methodically reverse each modification you've made. Then, deactivate the i2pd service by executing `sudo service i2pd stop` in your terminal (or `restart` if you intend to explore additional I2P sites). The Tor Browser Bundle (TBB) isn't set up to seamlessly switch between I2P, Tor, and clearnet browsing, so it's necessary to revert all changes and restart your browser each time you switch your browsing target. While this process may seem cumbersome, it's a vital step for ensuring your online security.

How to install I2P on Android?

Running I2P on Android devices is feasible, but it's particularly advised for users with Graphene OS or those without access to alternative setup options.
Prerequisites:

1. **Install F-Droid App Store:** Begin by installing the F-Droid app store on your Android device.
2. **Install InvZible Pro from F-Droid:** This app routes your traffic through Tor, ensures DNS queries are encrypted via DNSCrypt, and enables access to I2P sites (eepSites) using Purple I2P.
3. **Install Fennec F-Droid from F-Droid:** This hardened web browser is optimized for navigating through I2P sites (eepSites).

Setup Instructions:

1. **Initiate InvZible Pro**: After installing, launch InvZible Pro. Complete the initial setup by providing the necessary permissions and disabling battery optimizations. Do not start the service yet.
2. **Configure Fennec F-Droid**: Open Fennec F-Droid and type `about:config` in the address bar to access the advanced settings.
    - Disable JavaScript by searching for `javascript.enabled` and setting it to false.
    - Set up the proxy by searching for `network.proxy.http` and changing it to 127.0.0.1.
    - Configure the proxy port by finding `network.proxy.http_port` and setting it to 4444.
    - Ensure DNS queries are not proxied by setting `network.proxy.socks_remote_dns` to false.
    - Adjust HTTPS settings by setting `dom.security.https_first_pbm` and `dom.security.https_only_mode` to false.
        - **Note**: Some settings might revert to their defaults upon restarting the app. It's recommended to use private browsing mode to mitigate this.
3. **Start Browsing**: Return to InvZible Pro and click "Start" to begin browsing I2P sites securely. When finished, simply click "Stop" to end the session.

Remember, these settings ensure a more secure browsing experience on I2P with Android, but always be mindful of the inherent security limitations of mobile devices.

How to install I2P on Ubuntu?

To install I2P on Ubuntu, you will need to follow a few steps to ensure the process is smooth and successful. Here's a concise, step-by-step guide tailored for Ubuntu users:

1. **Open Your Terminal:** Begin by opening the Terminal on your Ubuntu

system. You can do this by pressing `Ctrl+Alt+T` on your keyboard.
2. **Add the I2P Repository:** Before you can install I2P, you need to add its repository to your system. This ensures you get the latest version directly from the source. Execute the following command:
   ```
   sudo apt-add-repository ppa:i2p-maintainers/i2p
   ```
   This command adds the official I2P package repository to your list of sources.
3. **Update Your Package List:** After adding the repository, update your package list to include the new source. You can do this by running:
   ```
   sudo apt-get update
   ```
   This command refreshes your system's package list, incorporating the newly added I2P repository.
4. **Install I2P:** Now that your package list is updated, you can proceed to install I2P. Execute the following command to start the installation:
   ```
   sudo apt-get install i2p
   ```
   This command installs I2P along with any necessary dependencies.
5. **Start I2P:** With I2P installed, you need to start the service. Use this command:
   ```
   sudo service i2p start
   ```
   This initiates the I2P service on your system.
6. **Enable I2P to Start on Boot:** To ensure I2P starts every time you boot your computer, enable it with the following command:
   ```
   sudo systemctl enable i2p
   ```
   This command sets I2P to automatically start with your system.
7. **Access I2P Console:** Finally, to access the I2P console and start navigating the I2P network, open your web browser and go to http://localhost:7657. This URL is the default homepage for the I2P router console, from where you can manage your I2P settings and view your I2P network status.

By following these steps carefully, you can install I2P on your Ubuntu system, offering you a gateway to a secure and anonymous internet layer designed for privacy-focused communication. Remember, navigating any privacy-focused

network requires caution and a good understanding of online security practices.

Advanced Setup for Whonix on Qubes

Compatibility and Prerequisites

- **Qubes OS Version:** 4.1 and newer
- **Whonix Version:** 16 and newer
- **Initial Step:** Ensure Qubes OS is installed with Whonix templates.

Preparing Your Whonix Workstation

1. **Persistence Configuration**: It's crucial to enable appropriate persistence options on your Whonix workstation to prevent data loss upon VM restarts.
2. **Command Execution**: All commands listed below should be executed in the terminal of your Whonix workstation.

Adding the I2P Signing Key

- **For Whonix-Workstation Users (anon-whonix)**: Run the following command to download the I2P signing key:
  ```
  scurl-download –proxy http://127.0.0.1:8082 –tlsv1.2 https://geti2p.net/_static/i2p-archive-keyring.gpg
  ```
- **Verification**: Display the key's fingerprint with the following command and verify it against the information on the Whonix wiki regarding I2P:
  ```
  gpg –keyid-format long –import –import-options show-only –with-fingerprint i2p-archive-keyring.gpg
  ```
  The fingerprint should match the provided example. After verification, copy the signing key to your APT keyring directory:
  ```
  sudo cp i2p-archive-keyring.gpg /usr/share/keyrings/i2p-archive-keyring.gpg
  ```

Setting Up the I2P Repository

- **Repository Addition:** Add the I2P APT repository by executing:
  ```
  echo "deb [signed-by=/usr/share/keyrings/i2p-archive-keyring.gpg] tor+https://deb.i2p2.de/ bullseye main" | sudo tee /etc/apt/sources.list.d/i2p.list
  ```

Installing I2P Packages

- **Installation Commands:** Update your package lists and install I2P without additional recommended packages:
  ```
  ```

```
sudo apt update && sudo apt full-upgrade
sudo apt install –no-install-recommends i2p i2p-keyring
```

Configuring I2P

1. **Automatic Startup:** Configure the I2P service to start with the system. When prompted, leave the default settings and choose 'Yes'.
2. **Adjusting the Local Worker Connection Address:** To avoid conflicts with the Whonix Tor Proxy, edit the connection address as shown below. This step is noted to have issues with the latest versions of I2P/Whonix:
   ```
   sudoedit /var/lib/i2p/i2p-config/clients.config.d/00-net.i2p.router.web.RouterConsoleRunner-clients.config
   ```
   Change `127.0.0.1` to `127.0.0.2`.

Maintaining Configuration Across Reboots

- **Startup Script Creation:** To ensure your configuration persists, create a startup script as follows:
  ```
  sudo nano /start.sh
  ```
  Insert this bash script into the newly created file:
  ```
  sed -i 's/127.0.0.1/127.0.0.2/' /var/lib/i2p/i2p-config/clients.config.d/00-net.i2p.router.web.RouterConsoleRunner-clients.config
  systemctl restart i2p
  ```
  Make the script executable:
  ```
  sudo chmod +x /start.sh
  ```
  Note: Place this script at the root of your Whonix template.

Execution and Additional Steps

- Upon starting your anon-whonix qube, open the Xfce Terminal and execute `sudo /start.sh`. This may also be set as a default startup option, though it may not always work effectively.
- **I2P Service Activation:** Enable I2P on anon-whonix startup and manage template shutdowns and qube restarts accordingly.
  ```
  sudo systemctl enable i2p
  sudo systemctl start i2p
  ```

Configuring Tor Browser for I2P Access

- Navigate to `about:config` in Tor Browser and adjust settings to enable I2P connections. Note: These changes may affect browser fingerprinting; use the modified settings only for I2P activities.
- Verify I2P functionality by accessing the I2P Router Console and monitoring connection stability.

Important Consideration: While I2P can operate over Tor, this setup isn't officially supported or recommended by I2P developers due to potential connectivity issues and the inherent design of I2P not being tailored for use over Tor. This method primarily serves to obscure your IP address from the I2P network.

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.

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

- Tor Project
- GnuPG
- Whonix
- Tails

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