

# Tails for Anarchists



**Series: Defensive**

This version of the zine was last edited on 2024-04-26. Visit  
[anarsec.guide](https://anarsec.guide) to see whether it has been updated since.

The dagger symbol † on a word means that there is a glossary entry for  
it. Ai ferri corti.

# Contents

TAILS: The Amnesic & Incognito Live System .....	5
The Threat Model Concept .....	8
I) The Basics of Using Tails .....	8
Prerequisites .....	9
Installation .....	10
Bootling from your Tails USB .....	10
Using the Tails Desktop .....	13
Optional: Create and Configure Persistent Storage .....	15
Upgrading the Tails USB .....	18
II) Going Further: Several Tips and Explanations .....	19
Tor .....	19
Included Software .....	31
Password Manager (KeePassXC) .....	32
Really delete data from a USB .....	34
How to create an encrypted USB .....	35
Encrypting a file with a password or public key .....	37
Adding administration rights .....	37
Installing additional software .....	38
Remember to make backups! .....	38
Privacy screen .....	38
III) Troubleshooting Issues .....	39
Best Practices .....	41
Appendix: Recommendations .....	41
Your Phone .....	42
Your Computer .....	42
Encrypted Messaging .....	43
Storing Electronic Devices .....	43
Appendix: Glossary .....	44
Command Line Interface (CLI) .....	44
Correlation Attack .....	44
Exploit .....	45
HTTPS .....	45

LUKS .....	45
Man-in-the-middle attack .....	45
Open-source .....	46
Operating system (OS) .....	46
Phishing .....	46
Physical attacks .....	47
Remote attacks .....	47
Sandboxing .....	47
Threat model .....	48
Tor network .....	48



Tails is an operating system<sup>†</sup> that makes anonymous computer use accessible to everyone. Tails is designed<sup>1</sup> to leave no trace of your activity on your computer unless you explicitly configure it to save specific data. It accomplishes this by running from a DVD or USB, independent of the operating system installed on the computer. Tails comes with several built-in applications<sup>2</sup> preconfigured with security in mind, and all anarchists should know how to use it for secure communication, research, editing, and publishing sensitive content.

The documentation on the Tails website<sup>3</sup> is excellent and easy to follow. This tutorial summarizes the most relevant documentation and additionally includes configuration and usage advice specific to an anarchist threat model<sup>†</sup>. Our Tails Best Practices<sup>4</sup> article goes into more detail, but we recommend that you familiarize yourself with the basics of Tails before reading it.

# TAILS: The Amnesic & Incognito Live System

Tails is an operating system. An operating system is the set of programs that run the various components (hard drive, screen, processor, memory, etc...) of the computer and allow it to function.

You have probably heard of “Windows” or “macOS”, the two most common operating systems. There are other operating systems — maybe you have heard of Linux? Linux refers to a family of operating systems that branches off into several sub-families, or different versions of Linux, one of which is called Debian. In the Debian sub-family we find Ubuntu and Tails. Tails is a distribution (version) of Linux with several distinguishing features:

---

<sup>1</sup>[tails.net/about/index.en.html](https://tails.net/about/index.en.html)

<sup>2</sup>[tails.net/doc/about/features/index.en.html](https://tails.net/doc/about/features/index.en.html)

<sup>3</sup>[tails.net/doc/index.en.html](https://tails.net/doc/index.en.html)

<sup>4</sup>[anarsec.guide/posts/tails-best](https://anarsec.guide/posts/tails-best)

- ***Live System***

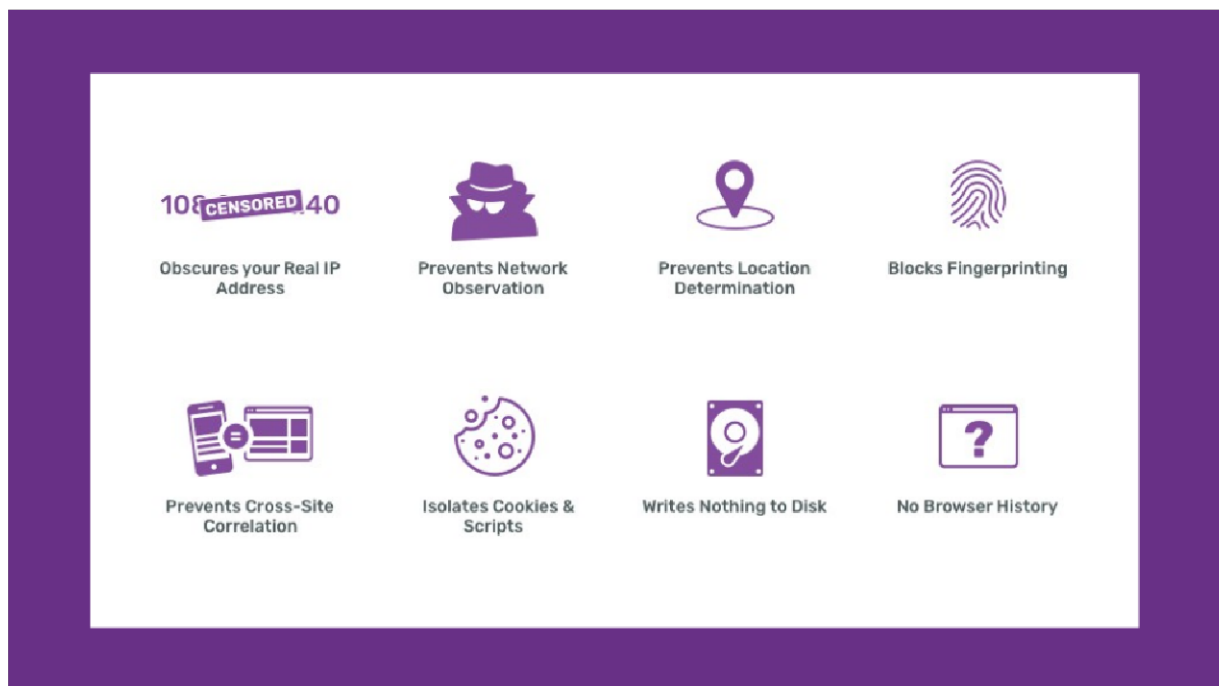
- Tails is a so-called live system. While other operating systems run from your computer's hard drive, Tails is installed on an external device such as a USB (or even an SD card or DVD). When you start your computer with the Tails device plugged in, your computer runs off of that device instead, leaving your hard drive untouched. You can even use Tails on a computer without a hard drive.

- ***Amnesia***

- Tails is designed to leave no data on the computer you are using; it writes nothing to the hard drive, and runs only in RAM (memory), which is automatically erased after shutdown. The Tails live system itself (usually running on a USB) is also left untouched. The only way to save information is to move it to another USB partition before shutting down (see below). The purpose of this is to avoid leaving forensic traces that someone with physical access to your computer or your Tails USB could later read. Things like Internet search history, “recently edited” documents, etc. are all erased.

- ***Incognito***

- Tails is also a system that allows you to be incognito, or anonymous. It hides the elements that could reveal your identity, location, etc. Tails uses the Tor anonymity network<sup>†</sup> to protect your anonymity online by forcing all default software to connect to the Internet through Tor. If an application tries to connect to the Internet directly, Tails will automatically block the connection. Tails also changes the “MAC address” of your network hardware, which can be used to uniquely identify your laptop.



- **Security**

- Tails was designed with security in mind. A minimal, functional, and verified environment is already installed (with everything needed for basic word processing, image editing, encryption, etc.).

Today's digital security is not necessarily tomorrow's. **Protecting personal data requires regular updates.** Digital tools are unreliable if they are never updated, and to have lasting confidence in these tools, it is good to know that teams are actively maintaining them and that they have a good reputation. It is important to understand the spirit of Tails: everything is designed with security in mind. However, in software, there is no such thing as a perfect tool; there are always limits. Also, **the way you use Tails can create security problems.**

Tails is free and open-source<sup>†</sup> software. Anyone can view, download and modify the source code (the recipe)... It is absolutely necessary to make sure that the version of Tails you have is genuine. Don't neglect the verification steps during installation, which are well explained on the Tails website.

Tails allows non-experts to benefit from digital security and anonymity without a steep learning curve. Using Tor is central to digital anonymity, and Tails helps us make as few mistakes as possible

when using Tor and some other tools. Using Tails takes very little effort to make everyday digital behavior more secure, even if it seems “inconvenient” at times. The “convenient” alternative, on the other hand, means an increased risk of repression — not only for you, but also for those you communicate with.

This tutorial is divided into several sections. The first covers the basics for getting started with Tails. The second section covers tips for using the software included in Tails, as well as what you need to know about how Tor works. The third section is about troubleshooting any problems that you might encounter with your Tails USB, so do not give up at the first problem — most of the time the solution is simple!

## The Threat Model Concept

Tails is not magic and has many limitations. The Internet and computers are hostile territory designed to steal your data. Tails will not protect you from human error, compromised hardware, compromised firmware, being hacked, or certain other types of attacks. There is no such thing as perfect security on the Internet, which is why building a threat model<sup>†</sup> is so important.

Building a threat model is simply a matter of asking yourself certain questions. Who am I defending against? What are their capabilities? What would be the consequences if they had access to that data? And then, based on the particular situation, assess how you can protect yourself.

It makes no sense to say “this tool is secure”. Security always depends on the threat model and it takes place on multiple levels (network, hardware, software, etc.). For more information on this topic, see the Threat Library<sup>5</sup>.

## I) The Basics of Using Tails

---

<sup>5</sup>[notrace.how/threat-library/](https://notrace.how/threat-library/)

# Prerequisites

## *Select a USB/DVD:*

Tails will only work with USBs that are at least 8GB, DVDs, or SD cards. Any data on the USB will be completely erased during installation, so save it somewhere else before, and if you don't want any trace of what was there before, use a new USB.

The Tails Best Practices<sup>6</sup> article recommends using a USB with a write-protect switch (an unmodifiable disk). When locked, the switch prevents the contents of the USB from being changed at all. This prevents a compromised Tails session from compromising your Tails USB. The write-protect switch must be turned off during installation. If you are unable to obtain such a USB, you can run Tails from a SD card, DVD-R/DVD+R, or always boot with the toram option (described in the article).

## *Select a laptop:*

Although it is possible to use Tails on a desktop computer, it is not recommended because it is only possible to detect physical tampering<sup>7</sup> on a laptop. See Tails Best Practices<sup>8</sup> for more information on obtaining a laptop.

Some laptop and USB models will not work with Tails, or some features will not work. To see if your model has any known issues, see the Tails known issues page<sup>9</sup>.

If Tails is too slow, make sure the USB is 3.0 or higher and that you are using a USB 3.0 port on the laptop. If Tails freezes frequently, you can add more RAM to your computer. 8GB should be sufficient.

---

<sup>6</sup>[anarsec.guide/posts/tails-best/#using-a-write-protect-switch](https://anarsec.guide/posts/tails-best/#using-a-write-protect-switch)

<sup>7</sup>[anarsec.guide/posts/tamper/#tamper-evident-laptop-screws](https://anarsec.guide/posts/tamper/#tamper-evident-laptop-screws)

<sup>8</sup>[anarsec.guide/posts/tails-best/#reducing-risks-when-using-untrusted-computers](https://anarsec.guide/posts/tails-best/#reducing-risks-when-using-untrusted-computers)

<sup>9</sup>[tails.net/support/known\\_issues/](https://tails.net/support/known_issues/)

# Installation

To install Tails on a USB, you need a “source” and a USB (8GB or larger).

There are two solutions for the “source”.

## ***Solution 1: Install by download (preferred)***

Follow the Tails installation instructions<sup>10</sup> it is important to follow the entire tutorial. It is possible for an attacker to intercept and modify the data on its way to you (this is called a man-in-the-middle attack<sup>†</sup>), so do not skip the verification steps. As discussed in Tails Best Practices<sup>11</sup>, the GnuPG installation method<sup>12</sup> is preferable because it more thoroughly verifies the integrity of the download.

## ***Solution 2: Install from another Tails USB***

This requires knowing a Tails user you trust. A very simple software called the Tails Installer allows you to “clone” an existing Tails USB to a new one in a few minutes; see the documentation for cloning from a PC<sup>13</sup> or Mac<sup>14</sup>. Any Persistent Storage data won’t be transferred. The downside of this method is that it may spread a compromised installation.

# Booting from your Tails USB

Once you have a Tails USB, follow the Tails instructions for booting Tails on a Mac or PC<sup>15</sup>. The Tails USB must be inserted before turning

---

<sup>10</sup>[tails.net/install/index.en.html](https://tails.net/install/index.en.html)

<sup>11</sup>[anarsec.guide/posts/tails-best/#reducing-risks-when-using-untrusted-computers](https://anarsec.guide/posts/tails-best/#reducing-risks-when-using-untrusted-computers)

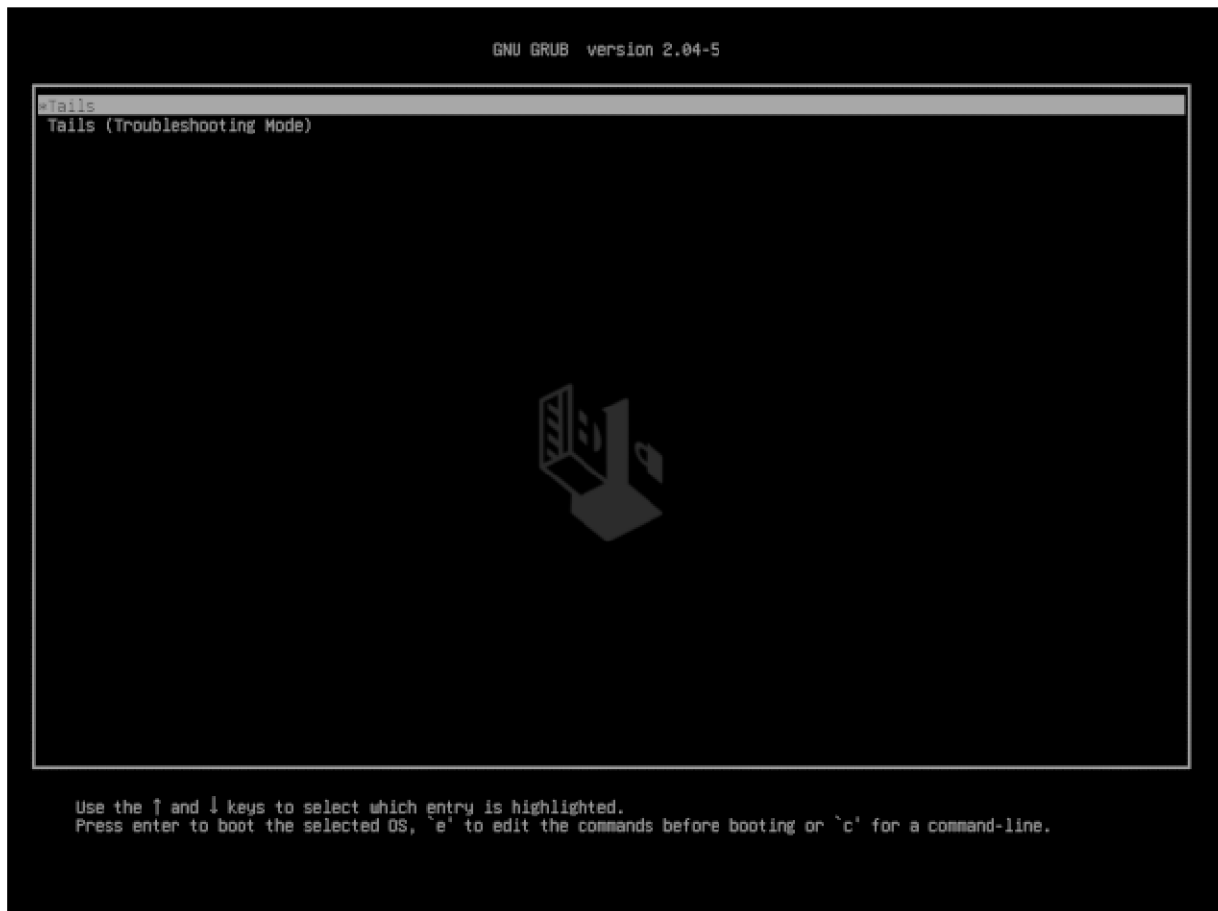
<sup>12</sup>[tails.net/install/expert/index.en.html](https://tails.net/install/expert/index.en.html)

<sup>13</sup>[tails.net/install/clone/pc/index.en.html](https://tails.net/install/clone/pc/index.en.html)

<sup>14</sup>[tails.net/install/clone/mac/index.en.html](https://tails.net/install/clone/mac/index.en.html)

<sup>15</sup>[tails.net/doc/first\\_steps/start/index.en.html](https://tails.net/doc/first_steps/start/index.en.html)

on your laptop. The Boot Loader screen will appear and Tails will start automatically after several seconds.



After about 30 seconds of loading, the Welcome Screen<sup>16</sup> will appear.

---

<sup>16</sup>[tails.net/doc/first\\_steps/welcome\\_screen/index.en.html](https://tails.net/doc/first_steps/welcome_screen/index.en.html)



On the Welcome Screen, select your language and keyboard layout in the **Language & Region** section. For Mac users, there is a keyboard layout for Macintosh. Under “Additional Settings” you will find a + button, click it and more configuration options will appear:

- Administration Password
  - Set this if you need administration rights. This is necessary, for example, to install additional software that you want to use during your Tails session. In the following dialog you can enter any password (and you have to remember it!). It will only be valid for this one Tails session. Restart the Tails session without an administration password as soon as you are done the activity that required it.
- MAC Address Spoofing
  - We recommend that you never disable this. It is enabled by default.
- Network Connection
  - “Disable all networking” allows you to disable all software network adapters at startup. If you intend to have an ‘offline’ Tails

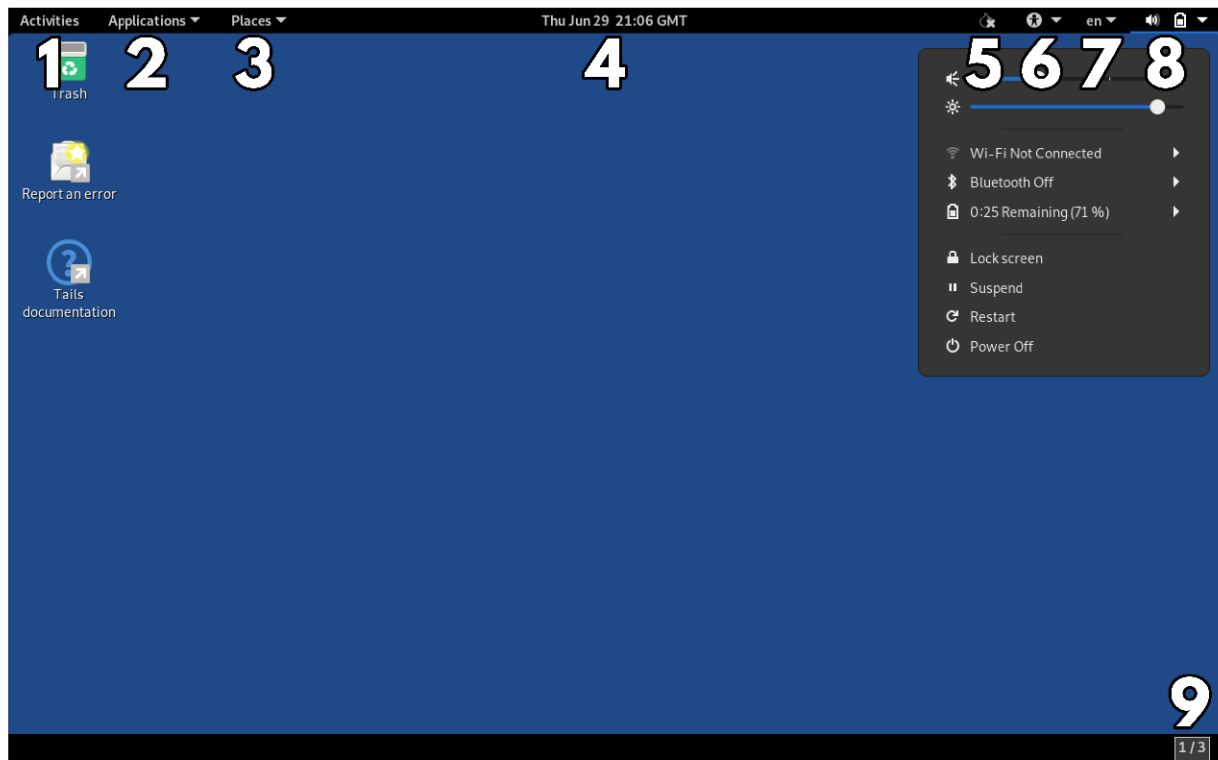


session, it makes sense to do this before Tails starts its networking functionality.

- Unsafe Browser
  - The Unsafe Browser is enabled by default and doesn't use Tor. An attacker could exploit<sup>†</sup> a vulnerability in another application in Tails to launch an invisible Unsafe Browser and reveal your real IP address. This is possible even if you're not using the Unsafe Browser. For example, an attacker could exploit a vulnerability in Thunderbird by sending you a phishing<sup>†</sup> email that launches an invisible Unsafe Browser that visits a website and reveals your IP address. Such an attack is very unlikely, but it could be carried out by a strong attacker, such as a government or a hacking company. For this reason, we **recommend that you disable Unsafe Browser for each session**. Leave Unsafe Browser enabled only when you need to go through a "captive portal" to connect to the Internet (when you have to click a box or log in to connect to the internet, common in Internet cafes, public Wi-Fi, etc.).

If you have Persistent Storage enabled, the passphrase to unlock it will appear in this window. If you haven't enabled Persistent Storage, no data will be stored on your Tails USB beyond this session. Click **Start Tails**. After 15 to 30 seconds, the Tails desktop will appear.

## Using the Tails Desktop



Tails is a simple operating system.

1. The Activities menu. Allows you to see an overview of your windows and applications. It also allows you to search for applications, files, and folders. You can also access Activities by sending your mouse to the top left corner of your screen or by pressing the Command/Windows (⌘) key.
2. The Applications menu. Lists available applications (software), organized by category.
3. The Places menu. Shortcuts to various folders and storage devices, which can also be accessed through the Files browser (**Applications** → **Accessories** → **Files**).
4. Date and time. Once connected to the Internet, all Tails systems around the world share the same time<sup>17</sup>.
5. The Tor status indicator. Tells you if you are connected to the Tor network. If there is an X over the onion icon, you are not connected. You can open the Onion Circuits application from here. Check your Tor connection by visiting [check.torproject.org](https://check.torproject.org) in the Tor Browser.

6. The “Universal Access” button. This menu allows you to enable accessibility software such as the screen reader, visual keyboard, and large text display.
7. Choice of keyboard layouts. An icon showing the current keyboard layout (in the example above, en for an English layout). Clicking it provides options for other layouts selected at the Welcome Screen.
8. The System menu. From here, you can access the volume and screen brightness, the Wi-Fi and Ethernet connection, the battery status, and the restart and shutdown buttons.
9. The Workspaces icon. This button toggles between multiple views of the desktop (called “workspaces”), which can help reduce visual clutter on a small screen.

If your laptop is equipped with Wi-Fi, but there is no Wi-Fi option in the system menu, see the troubleshooting documentation<sup>18</sup>. Once you connect to Wi-Fi, a Tor Connection assistant will appear to help you connect to the Tor network. Select **Connect to Tor automatically**, unless you are in a country where you need to hide that you’re using Tor (in which case you’ll need to configure a bridge<sup>19</sup>).

## Optional: Create and Configure Persistent Storage

Tails is amnesiac by default. It will forget everything you have done as soon as you end the session. This isn’t always what you want — for example, you may want to install additional software without needing to re-install it each time you start up. Tails has a feature called Persistent Storage, which allows you to save data between sessions. This is explicitly less secure, but necessary for some activities.

The principle behind Persistent Storage is to create a second storage area (called a partition) on your Tails USB that is encrypted. This new

---

<sup>17</sup>[tails.net/doc/first\\_steps/desktop/time/index.en.html](https://tails.net/doc/first_steps/desktop/time/index.en.html)

<sup>18</sup>[tails.net/doc/anonymous\\_internet/no-wifi/index.en.html](https://tails.net/doc/anonymous_internet/no-wifi/index.en.html)

<sup>19</sup>[tails.net/doc/anonymous\\_internet/tor/index.en.html#hiding](https://tails.net/doc/anonymous_internet/tor/index.en.html#hiding)

partition allows you to make some data persistent — that is, to keep it between Tails sessions. It's very easy to enable Persistent Storage. To create the Persistent Storage<sup>20</sup>, choose **Applications → Tails → Persistent Storage**.

A window will pop up asking you to enter a passphrase; see Tails Best Practices<sup>21</sup> for information on passphrase strength. You'll then configure<sup>22</sup> what you want to keep in Persistent Storage. Persistent Storage can be enabled for several types of data:

### **Personal Documents:**

- **Persistent Folder:** Data such as your personal files, documents, or images you're working on.

### **System Settings:**

- **Welcome Screen:** Settings from the Welcome Screen: language, keyboard, and additional settings.
- **Printers:** Printer configuration<sup>23</sup>.

### **Network:**

- **Network Connections:** The passwords for Wi-Fi networks can be saved so you don't have to enter them every time.
- **Tor Bridge:** If Tor Bridge is enabled (for users in countries that censor Tor), the last Tor Bridge you used will be remembered.

### **Applications:**

- **Tor Browser Bookmarks:** Tor Browser bookmarks.
- **Electrum Bitcoin Wallet:** The bitcoin wallet and settings.
- **Thunderbird Email Client:** The Thunderbird email inbox, feeds, and OpenPGP keys.
- **GnuPG:** The OpenPGP keys you create or import into GnuPG and Kleopatra.

---

<sup>20</sup>[tails.net/doc/persistent\\_storage/create/index.en.html](https://tails.net/doc/persistent_storage/create/index.en.html)

<sup>21</sup>[anarsec.guide/posts/tails-best/#passwords](https://anarsec.guide/posts/tails-best/#passwords)

<sup>22</sup>[tails.net/doc/persistent\\_storage/configure/index.en.html](https://tails.net/doc/persistent_storage/configure/index.en.html)

<sup>23</sup>[tails.net/doc/sensitive\\_documents/printing\\_and\\_scanning/index.en.html](https://tails.net/doc/sensitive_documents/printing_and_scanning/index.en.html)

- **Pidgin:** The account files of this chat application (using the XMPP protocol).
- **SSH Client:** All files related to SSH, a protocol used to connect to servers.

### Advanced Settings:

- **Additional Software:** If this feature is enabled, a list of additional software of your choice will be automatically installed each time you start Tails. These software packages are stored in Persistent Storage. They are automatically updated when you connect to the Internet. Be careful what you install<sup>24</sup>.
- **Dotfiles:** In Tails and Linux in general, the names of configuration files often start with a dot, so they are sometimes called “dotfiles”. These can be saved in the Persistent Storage. Be careful what configuration settings you change, as changing the defaults can break your anonymity.

To use Persistent Storage, you must unlock it on the Welcome Screen. If you want to change the passphrase, see the documentation<sup>25</sup>. If you ever forget your passphrase, it’s impossible to recover it; you’ll have to delete<sup>26</sup> the Persistent Storage and start over.

In Tails Best Practices<sup>27</sup>, we recommend against using Persistent Storage in most cases; most Persistent Storage features do not work well with USBs that have a write-protect switch, any files stored on a Tails USB will leave forensic traces on it, and storing personal data on the Tails USB also prevents it from being compartmentalized when Persistent Storage is unlocked. Any files that need to be persistent can be stored on a second LUKS-encrypted USB<sup>28</sup> instead.

---

<sup>24</sup>[tails.net/doc/persistent\\_storage/additional\\_software/index.en.html#warning](https://tails.net/doc/persistent_storage/additional_software/index.en.html#warning)

<sup>25</sup>[tails.net/doc/persistent\\_storage/passphrase/index.en.html](https://tails.net/doc/persistent_storage/passphrase/index.en.html)

<sup>26</sup>[tails.net/doc/persistent\\_storage/delete/index.en.html](https://tails.net/doc/persistent_storage/delete/index.en.html)

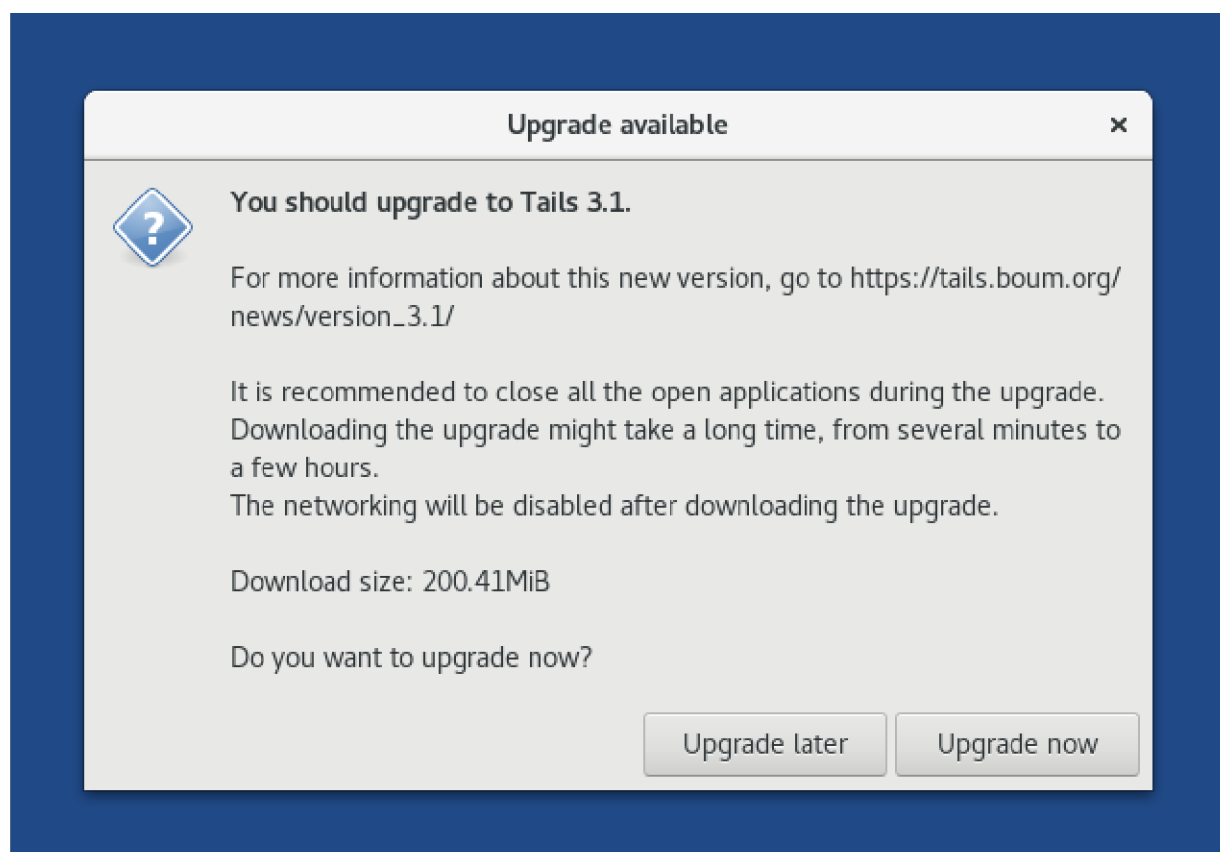
<sup>27</sup>[anarsec.guide/posts/tails-best/#using-a-write-protect-switch](https://anarsec.guide/posts/tails-best/#using-a-write-protect-switch)

<sup>28</sup>[anarsec.guide/posts/tails/#how-to-create-an-encrypted-usb](https://anarsec.guide/posts/tails/#how-to-create-an-encrypted-usb)

# Upgrading the Tails USB

In order for Tails to remain secure, the operating system must be continually developed and any security vulnerabilities must be addressed through upgrades. It is important to always use the latest version (Tails is updated approximately every month), as security vulnerabilities are regularly discovered in the programs used by Tails, which in the worst case could lead to your identity, IP address, etc. being exposed. A Tails upgrade will fix these vulnerabilities and usually improve other features as well.

Every time you start Tails, right after you connect to the Tor network, the Tails Upgrader checks to see if you have the latest version of Tails. There are two types of upgrades.



## *The automatic upgrade*

When an automatic upgrade<sup>29</sup> is available, a window will appear with information about the upgrade, and you will need to click **Upgrade now**. Wait a while for it to complete, then click ‘Apply upgrade’ and your internet will be interrupted for a moment. Wait until you see the Restart Tails window. If the upgrade fails (for example, because you shut down before it was finished), your Persistent Storage will not be affected, but you may not be able to restart your Tails USB. If you are using a USB with a write-protect switch, you will need to unlock it for the dedicated session in which you are performing the upgrade.

### *The manual upgrade*

Sometimes the upgrade window will tell you that you need to do a manual upgrade. This type of upgrade is only used for major upgrades (which happen approximately every two years) or if there is a problem with automatic upgrades. See the documentation for manual upgrades<sup>30</sup>.

## II) Going Further: Several Tips and Explanations

### **Tor**

#### *What is Tor?*

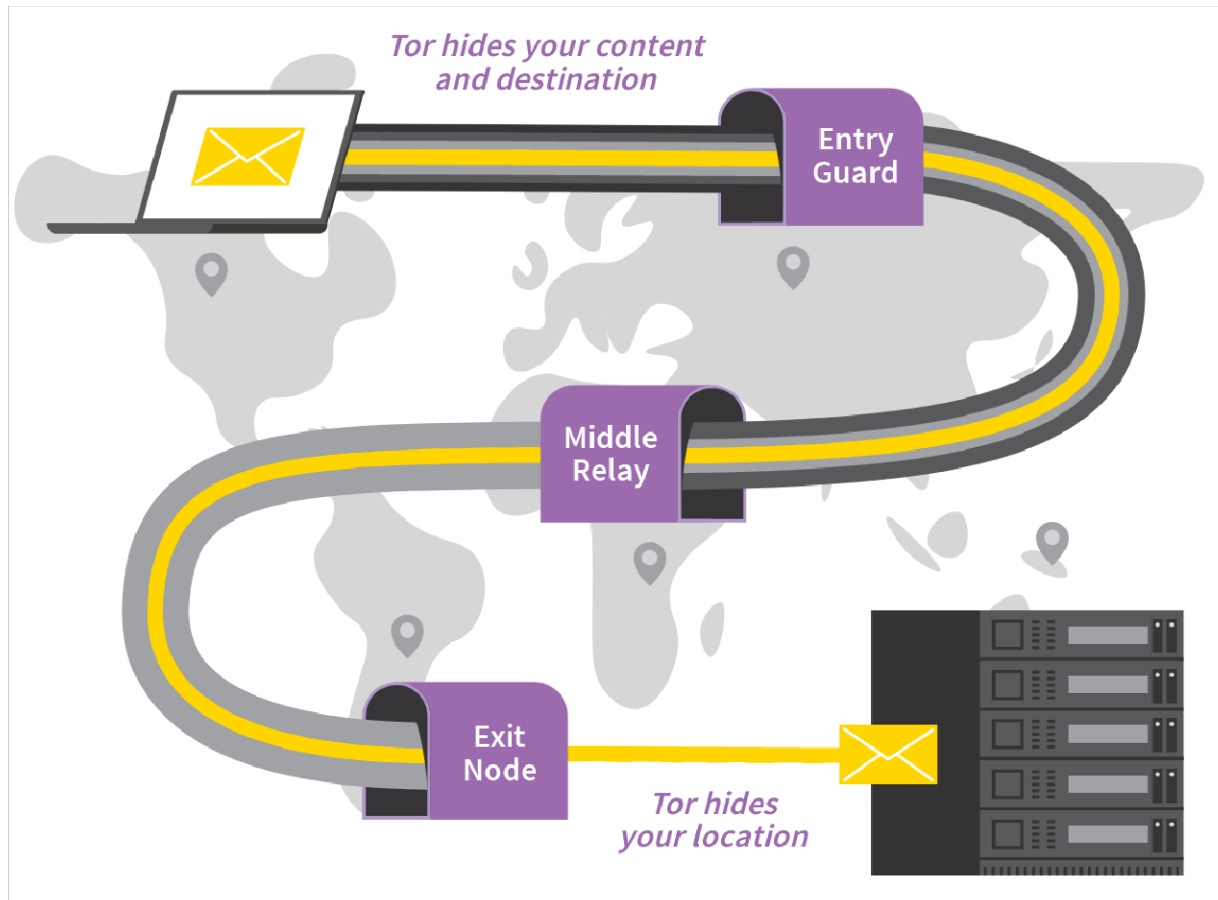
Tor<sup>†</sup>, which stands for The Onion Router, is the best way to be anonymous on the Internet. Tor is open-source software connected to a public network of thousands of relays (servers). Instead of connecting directly to a location on the Internet, Tor takes a detour through three intermediate relays. The Tor Browser uses the Tor

---

<sup>29</sup>[tails.net/doc/upgrade/index.en.html](https://tails.net/doc/upgrade/index.en.html)

<sup>30</sup>[tails.net/upgrade/tails/index.en.html](https://tails.net/upgrade/tails/index.en.html)

network, but other applications can as well if they are configured properly. All default applications included in Tails use Tor if they need to connect to the Internet.



Internet traffic, including the IP address of the final destination, is encrypted in layers like an onion. Each hop along the three relays removes one layer of encryption. Each relay only knows the relay before it and the relay after it (the exit relay knows that it came from the middle relay and that it goes to such-and-such a website, but not the entry relay).



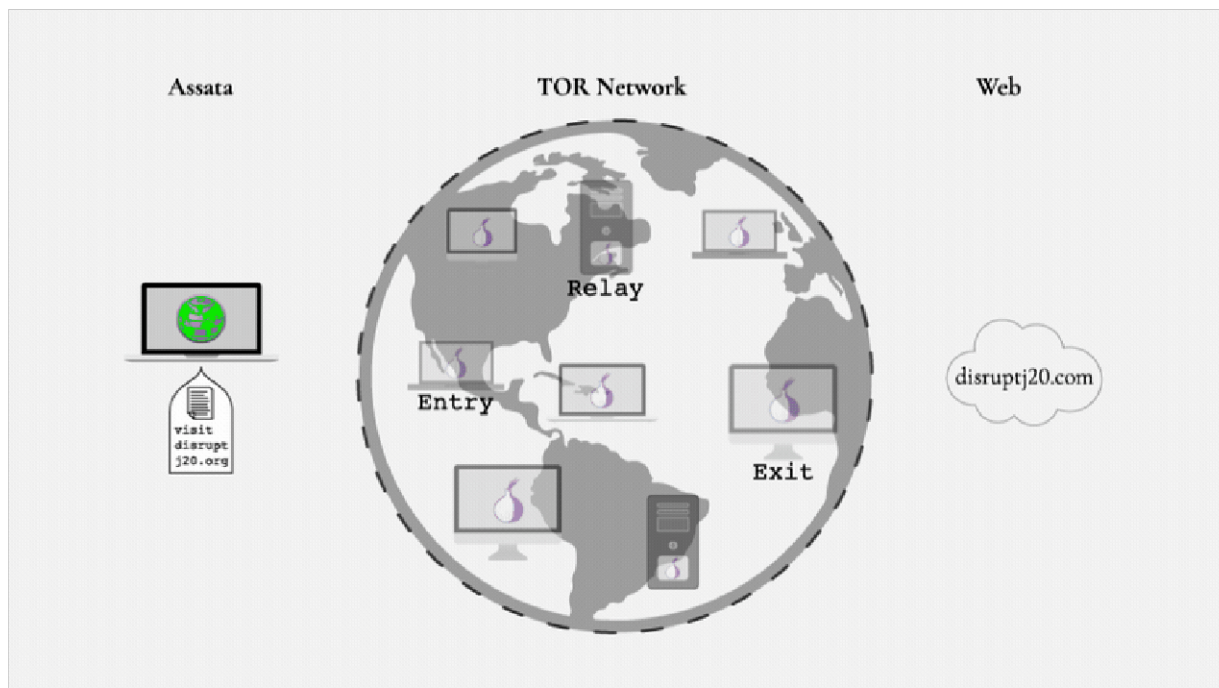


Figure 1: See *anarsec.guide* for the animation.

This means that any intermediaries between you and the entry relay know that you're using Tor, but they don't know what site you're going to. Any intermediaries after the exit relay know that someone in the world is going to that site, but they don't know who it is. The site's web server sees you coming from the IP address of the exit relay.


Tor has several limitations. For example, if someone with the technical and legal means believes you're connecting from a particular Wi-Fi connection to visit a particular site, they can try to match your Wi-Fi connection with what the website activity (a "correlation attack"). However, to our knowledge, this type of attack has never been used by itself to incriminate someone in court. For sensitive activities, use Internet connections that are not tied to your identity to protect yourself in case Tor fails.

## ***What is HTTPS?***

Virtually all websites today use HTTPS<sup>†</sup> — the S stands for "secure" (e.g., <https://www.anarsec.guide>). If you try to visit a website without `https://` in the Tor Browser, you will receive a warning before proceeding. If you see `http://` instead of `https://` in

front of a website's address, it means that all intermediaries after the exit relay of the Tor network know what you are exchanging with the website (including your credentials). HTTPS means that the digital record of what you do on the site you are visiting is protected by an encryption key that belongs to the site. Intermediaries after the exit relay will know that you are visiting `riseup.net`, for example, but they will not have access to your emails and passwords, nor will they know if you are checking your emails or reading a random page on the site. A small padlock appears to the left of the site address when you are using HTTPS.

If there's a yellow warning on the padlock, it means that some elements on the page you're viewing are not encrypted (they use HTTP), which could reveal the exact page or allow intermediaries to partially modify the page. By default, the Tor Browser uses HTTPS-Only Mode to prevent users from visiting HTTP sites.



HTTPS-Only Mode Alert

Secure Connection Not Available

You've enabled HTTPS-Only Mode for enhanced security, and a HTTPS version of `neverssl.com` is not available.

[Learn More...](#)

**What could be causing this?**

- Most likely, the website simply does not support HTTPS.
- It's also possible that an attacker is involved. If you decide to visit the website, you should not enter any sensitive information like passwords, emails, or credit card details.

If you continue, HTTPS-Only Mode will be turned off temporarily for this site.

Continue to HTTP Site

Go Back

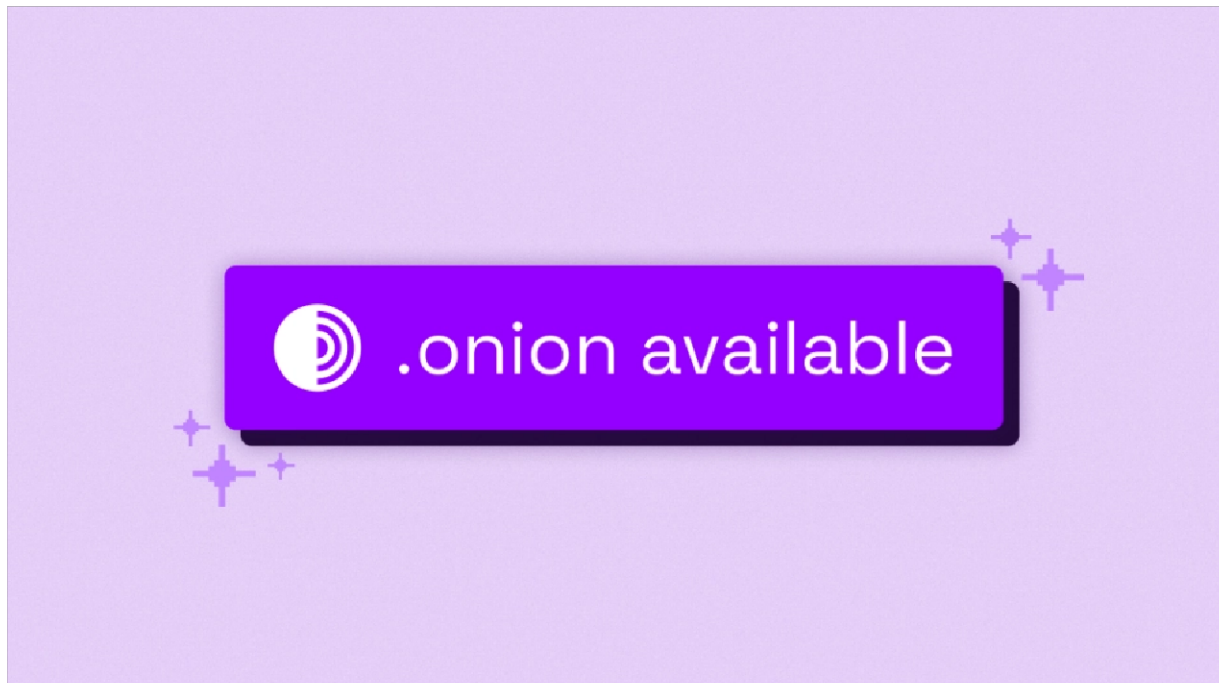
HTTPS is essential both to limit your web fingerprint and to prevent an intermediary from modifying the data you exchange with websites. If the intermediary cannot decrypt the data, they cannot modify it. For an overview of HTTP / HTTPS connections with and without Tor, and

what information is visible to various third parties, see the EFF's interactive graphic<sup>31</sup>.

In short, don't visit websites that aren't using HTTPS.

## ***Onion Services: what is .onion?***

Have you ever seen a strange website address with 56 random characters ending in .onion? This is called an onion service, and the only way to visit a website using such an address is to use the Tor Browser. The “deepweb” and “darkweb” are terms that have been popularized in the media to describe these onion services.



Anyone can set up an .onion site. But why would they want to? Well, the server location is anonymized, so authorities cannot find out where the site is hosted in order to shut it down. When you send data to an .onion site, you enter the site's three Tor relays after the standard Tor circuit. So we have 6 Tor relays between us and the site; we know the first 3 relays, the site knows the last 3, and each Tor node only knows the relay before and after. Unlike a normal HTTPS website, it's all Tor encrypted from end to end.

---

<sup>31</sup>[eff.org/pages/tor-and-https](https://eff.org/pages/tor-and-https)

This means that both the client (your laptop) and the server (where the site lives) remain anonymous, whereas with a normal website, only the client is anonymous. In addition to being more anonymous for the server, it is also more anonymous for the client: you never leave the Tor network, so it is not possible to intercept you after the exit relay.

The .onion site address is long because it includes the site's certificate. HTTPS is unnecessary; security depends on knowing the site's .onion address.

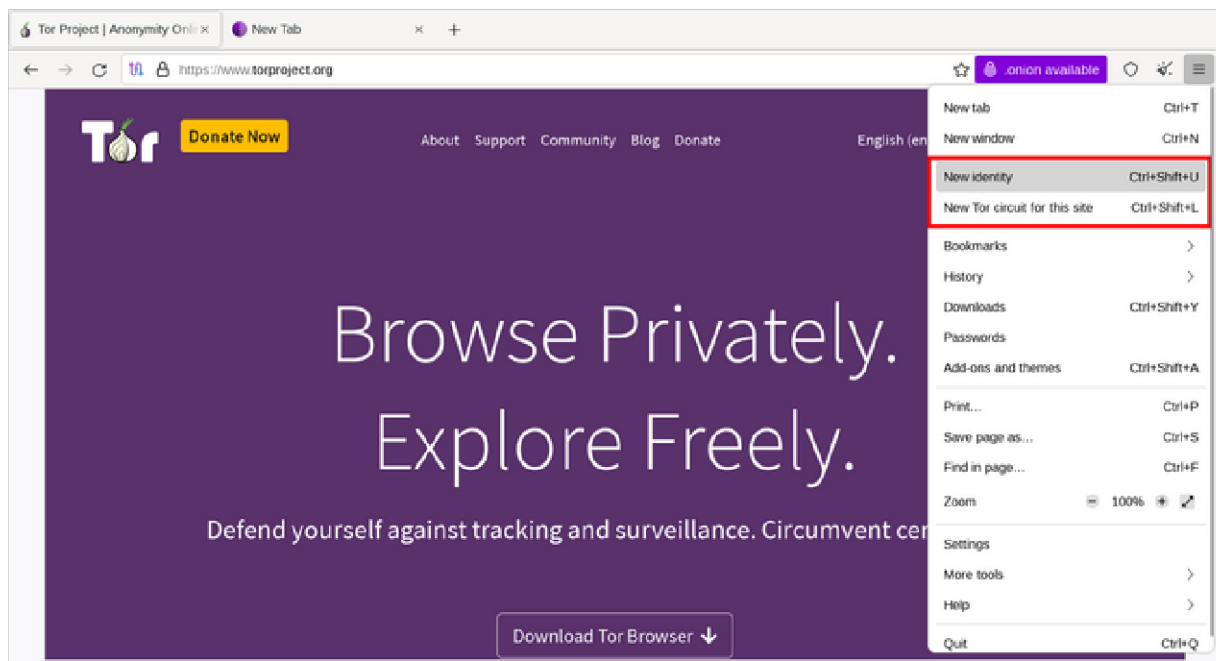
Some sites offer both a classic URL and an .onion address. In this case, if the site has been configured to do so, an indication of “.onion available” should appear next to the URL. If not, sometimes the site will list the .onion address somewhere on its page. To find out the addresses of sites that are only available as .onion, you will need to either find them by word of mouth, or through websites that list other .onion sites, such as this GitHub page<sup>32</sup>.

## ***Sites that block Tor***

Some sites block users who visit through the Tor network, or otherwise make it inconvenient to visit the site. Some sites may force you to complete CAPTCHAs or provide additional personal information (ID, phone number...) before continuing, or they may block Tor altogether.

---

<sup>32</sup>[github.com/alecmuffett/real-world-onion-sites](https://github.com/alecmuffett/real-world-onion-sites)



The site may only block certain Tor relays. In this case, you can change the Tor exit node being used for this site: click the ☒ → **“New Tor circuit for this site”** button. The Tor circuit (path) will change for the current tab, including other open tabs or windows from the same website. You may need to do this several times in a row if you’re unlucky enough to encounter multiple banned relays.

Since all Tor relays are public, it is also possible that the site is blocking the entire Tor network. In this case, you can try using a proxy to access the site, such as <https://hide.me/en/proxy> (but only if you don’t have to enter personal information like login credentials). You can also check if the page you want to access has been saved to the Wayback Machine: [web.archive.org](https://web.archive.org).

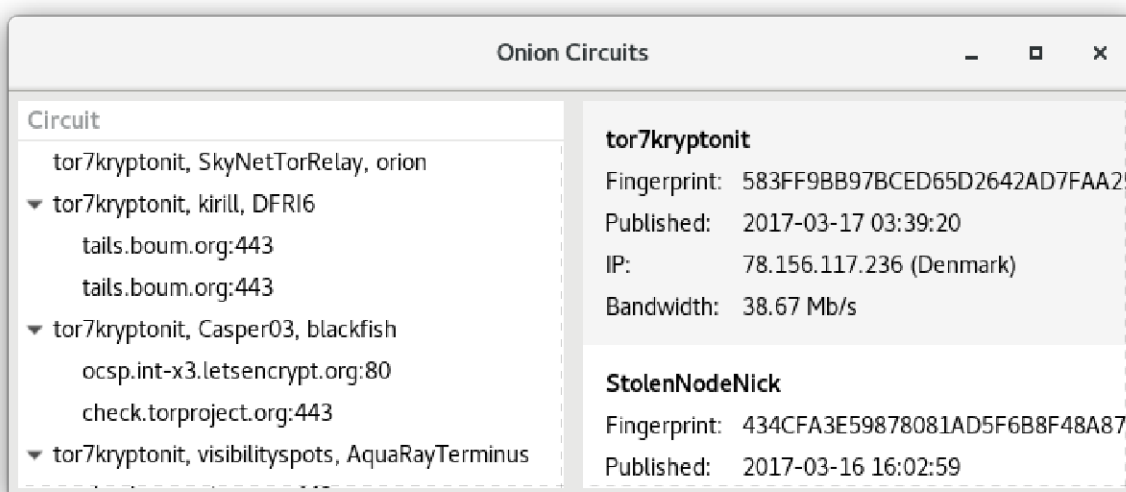
## ***Cleanly Separate Anonymous Identities***

It is not recommended to perform different Internet tasks that should not be associated with each other during the same Tails session. You must separate different (contextual) identities carefully! For example, it is dangerous to check your personal email and publish an anonymous text during the same session. In other words, you should not be identifiable and anonymous on the Tor network at the same time. You also shouldn’t use the Tor network under both pseudonym A and



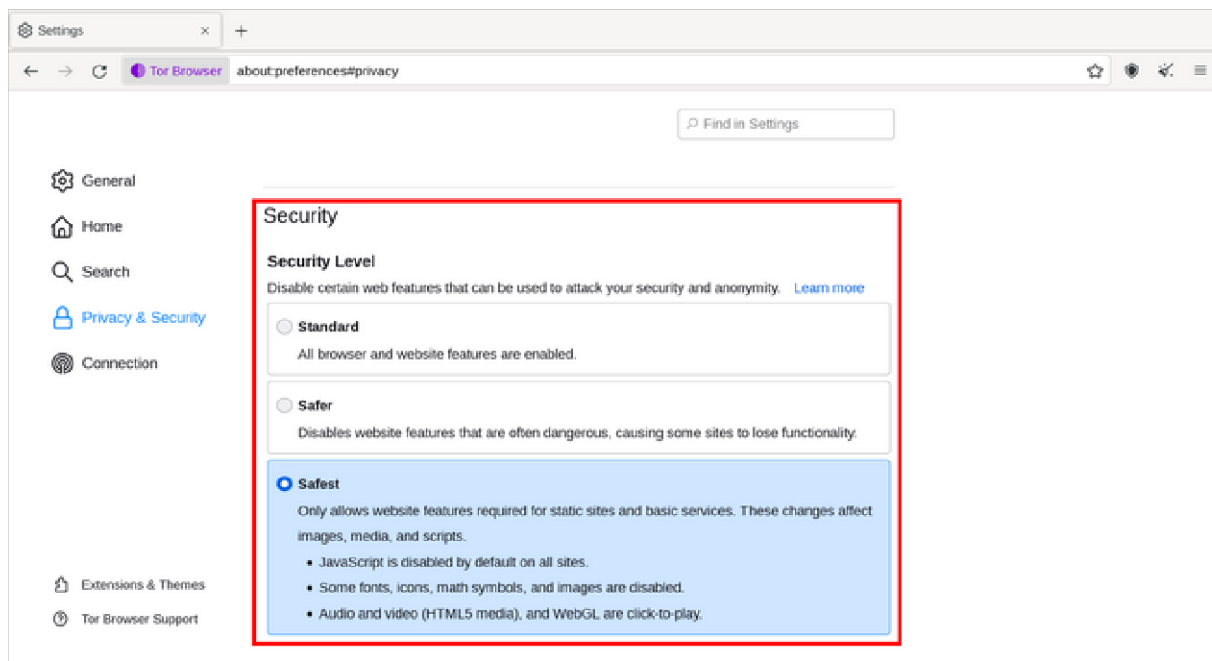
pseudonym B in the same session, as these pseudonyms could be connected through a monitored or compromised Tor exit relay. Shut down and restart Tails between Internet activities under different identities!

The Tor Browser's 'New Identity' feature is not sufficient to completely separate contextual identities in Tails, since it does not reestablish connections outside the Tor Browser, and you keep the same Tor entry node. Restarting Tails is a better solution.



The Onion Circuits application shows which Tor circuit a server connection (website or otherwise) is using. Sometimes it can be useful to make sure that the exit relay is not located in a certain country, to be further away from the easiest access for investigating authorities. In the example above, the connection to [check.torproject.org](https://check.torproject.org) goes through the relays `tor7kryptonit`, `Casper03`, and the exit node `blackfish`. Clicking on a circuit will display technical details about its relays in the right pane. The Tor Browser's 'New Identity' feature is useful for changing this exit relay without restarting the Tails session, which can be repeated until you have an exit relay you are happy with. We do not recommend using 'New Identity' to switch between identities, but only if you want to change the exit node within the same identity's activities.

## ***Tor Browser security settings***



Like any software, the Tor Browser has vulnerabilities that can be exploited — various police agencies have Tor Browser exploits for serious cases. To mitigate this, it's important to keep Tails up to date, and you should increase the Tor Browser's security settings: click the shield icon, and then click **Settings....** By default, it's set to Standard, which maintains a browsing experience comparable to a regular browser. **We strongly recommend that you set it to the most restrictive setting before you start browsing: Safest.** The vast majority of exploits against Tor Browser will not work with the Safest setting.

The layout of some pages may be changed, and some types of content may be disabled (SVG images, click-to-play videos, etc.). For example, [anarsec.guide](#) has two things that will be broken in Safest mode because they rely on Javascript: dark mode and the article's table of contents. Some sites will not work at all with these restrictions; if you have reason to trust them, you can view them with a less restrictive setting on a site-by-site basis. Remember that both "Standard" and "Safer" settings allow scripts to work, which can break your anonymity<sup>33</sup> in a worst-case scenario.

---

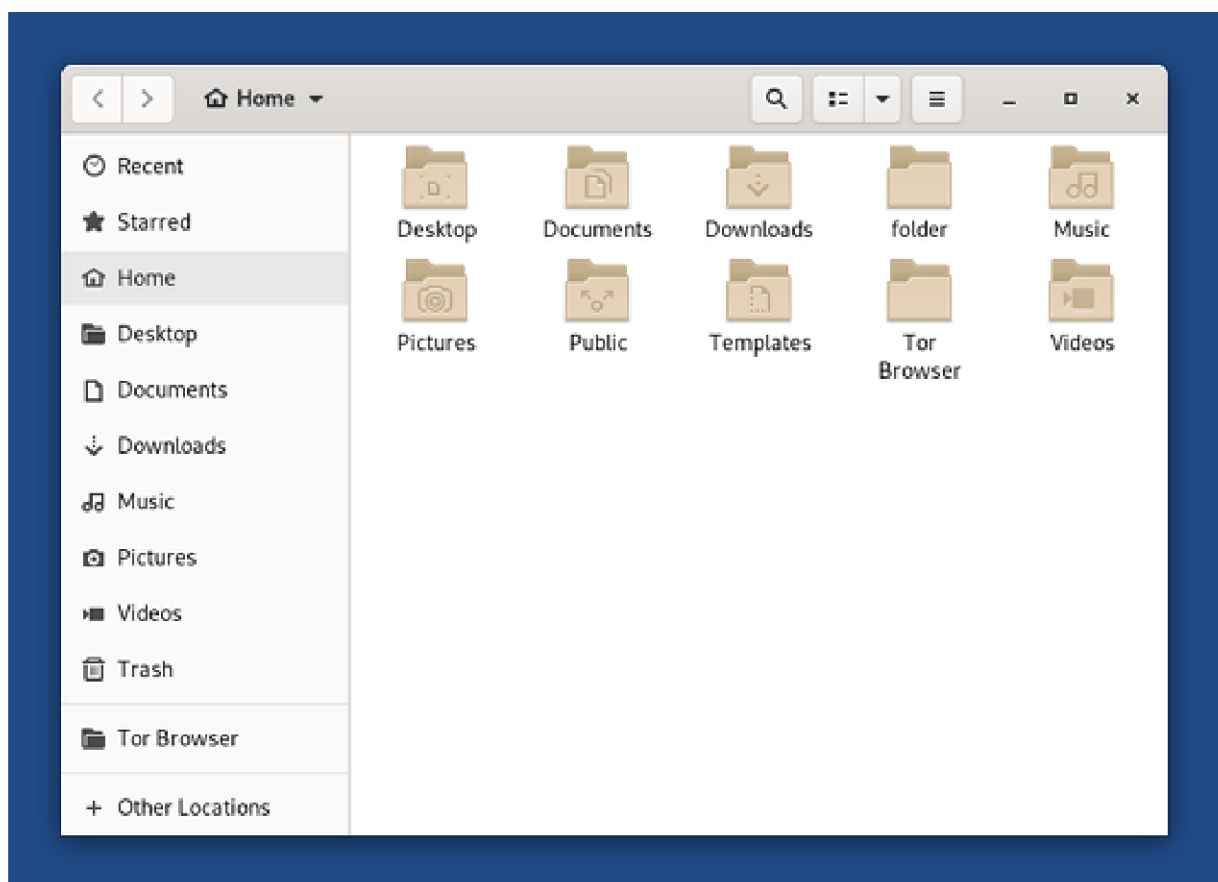
<sup>33</sup>[arstechnica.com/information-technology/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/](https://arstechnica.com/information-technology/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/)

## *Downloading/uploading and the Tor Browser folder*

The Tor Browser on Tails is kept in a “sandbox”<sup>†</sup> to prevent it from snooping on all your files if a malicious site compromised it. This means there are special considerations when uploading or downloading files using the Tor Browser.

### Downloading

When you download something using the Tor Browser, it is stored in the Tor Browser folder (/home/amnesia/Tor Browser/), which is inside the sandbox. If you want to do anything with the file, you should move it out of the Tor Browser folder. You can use the file manager (**Applications** → **Accessories** → **Files**) to do this.



### Uploading

Similarly, if you want to upload something using the Tor Browser (for example, to include a file in a blog post), you will first need to move or

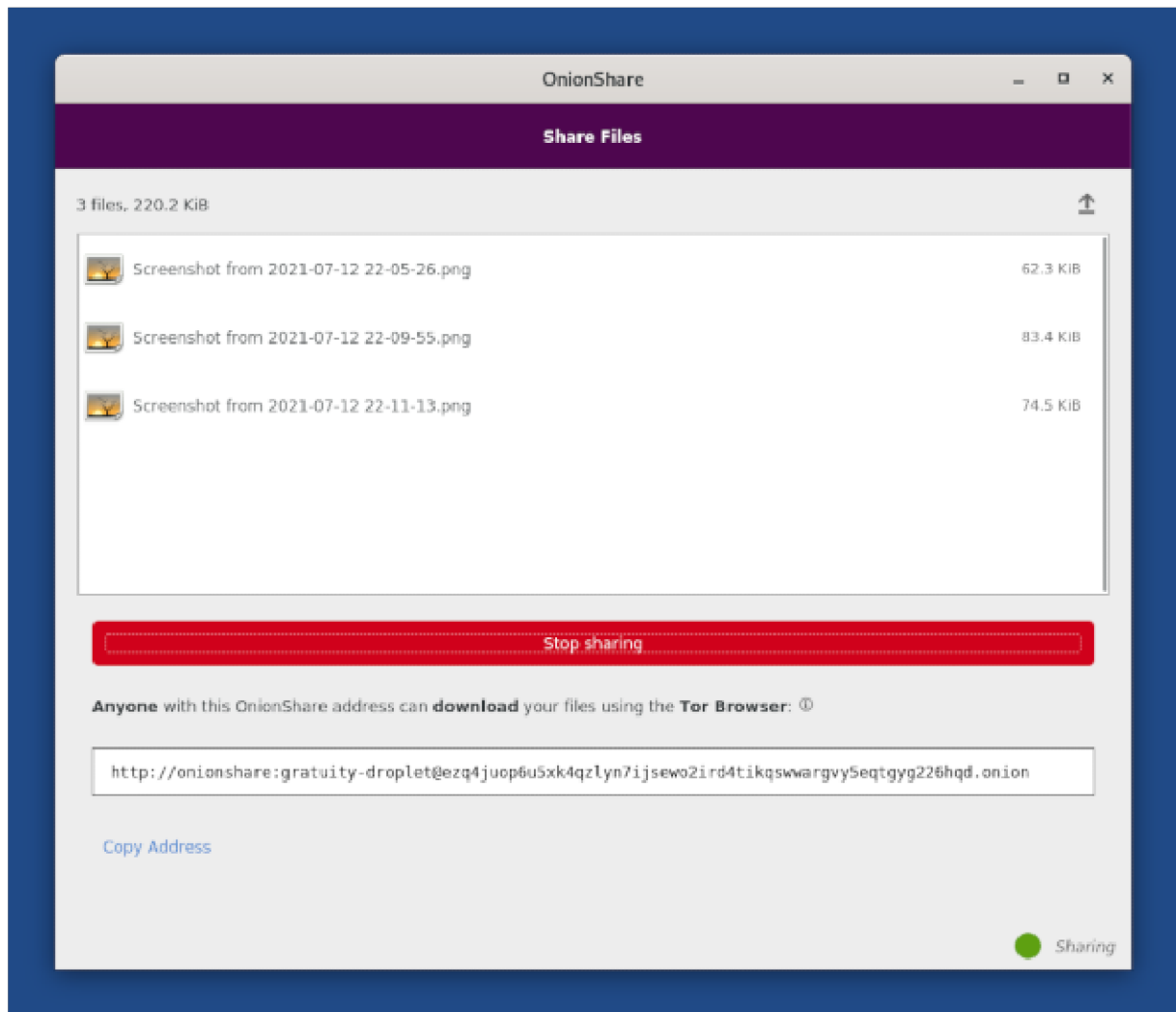


copy the file to the Tor Browser folder. Then it will be available when you select the file to upload in the Tor Browser.

## **RAM**

Be aware that if you are downloading or otherwise working with very large files, your RAM (memory) may fill up. This is because your entire Tails session is running in RAM (unless you have set up Persistent Storage, which uses the USB). If the RAM fills up, Tails will slow down or crash. You can mitigate this by closing unneeded applications and deleting other files you have downloaded. In the worst case, you may need to temporarily enable Persistent Storage to download or upload large files via the persistent Tor Browser folder, which uses the USB instead of RAM.

## ***Share Files with Onionshare***



It is possible to send a document through an .onion link thanks to OnionShare<sup>34</sup> (**Applications** → **Internet** → **OnionShare**). By default, OnionShare stops the hidden service after the files have been downloaded once. If you want to offer the files for multiple downloads, you need to go to the settings and uncheck “Stop sharing after first download”. As soon as you close OnionShare, disconnect from the Internet, or shut down Tails, the files will no longer be accessible. This is a great way to share files because it doesn’t require you to plug a USB into someone else’s computer, which we don’t recommend<sup>35</sup>. The

---

<sup>34</sup>[tails.net/doc/anonymous\\_internet/onionshare/index.en.html](https://tails.net/doc/anonymous_internet/onionshare/index.en.html)

<sup>35</sup>[anarsec.guide/posts/tails-best/#reducing-risks-when-using-untrusted-computers](https://anarsec.guide/posts/tails-best/#reducing-risks-when-using-untrusted-computers)

long .onion address can be shared through another channel (such as a Riseup Pad<sup>36</sup> you create that is easier to type).

## ***Make Correlation Attacks More Difficult***

When you request a web page through a web browser, the site's server sends it to you in small "packets" that have a specific size and timing (among other characteristics). When using the Tor Browser, the sequence of packets can also be analyzed to look for patterns that can be matched to those of websites. To learn more, see "1.3.3. Passive Application-Layer Traffic Patterns"<sup>37</sup>. Tor plans to mitigate this issue in the future<sup>38</sup>.

To make this "correlation attack"<sup>†</sup> more difficult, disable JavaScript by using Tor Browser on the **Safest** setting.

Additionally, doing multiple things at once with your Tor client<sup>39</sup> is recommended by the Tor team.

## **Included Software**

Tails comes with many applications<sup>40</sup> by default. The documentation gives an overview of Internet applications<sup>41</sup>, applications for encryption and privacy<sup>42</sup>, and applications for working with sensitive documents<sup>43</sup>. In the rest of this section, we will only highlight common use cases relevant to anarchists, but read the documentation for more information.

---

<sup>36</sup>[pad.riseup.net/](https://pad.riseup.net/)

<sup>37</sup>[spec.torproject.org/proposals/344-protocol-info-leaks.html](https://spec.torproject.org/proposals/344-protocol-info-leaks.html)

<sup>38</sup>[gitlab.torproject.org/tpo/team/-/wikis/Sponsor-112](https://gitlab.torproject.org/tpo/team/-/wikis/Sponsor-112)

<sup>39</sup>[blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations/](https://blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations/)

<sup>40</sup>[tails.net/doc/about/features/index.en.html](https://tails.net/doc/about/features/index.en.html)

<sup>41</sup>[tails.net/doc/anonymous\\_internet/index.en.html](https://tails.net/doc/anonymous_internet/index.en.html)

<sup>42</sup>[tails.net/doc/encryption\\_and\\_privacy/index.en.html](https://tails.net/doc/encryption_and_privacy/index.en.html)

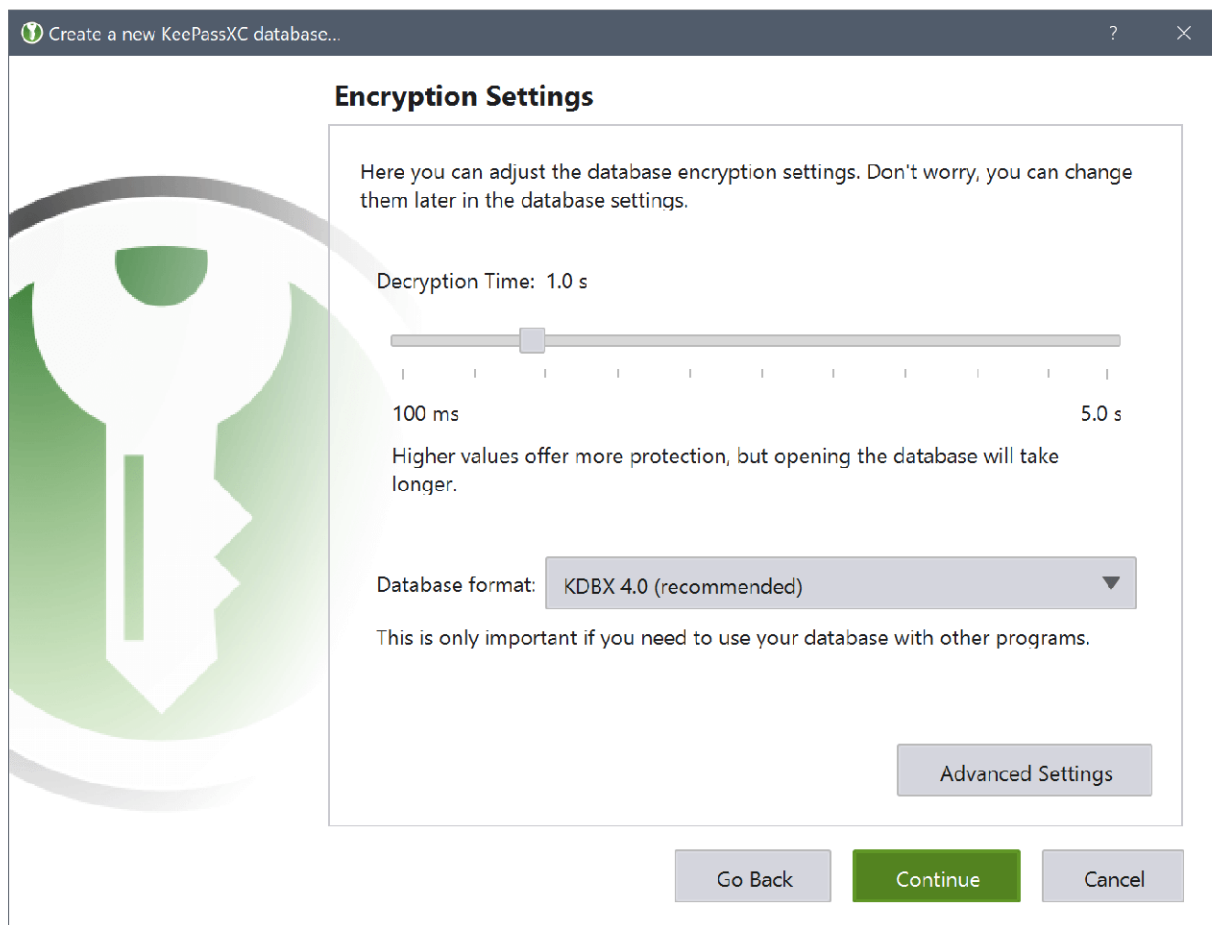
<sup>43</sup>[tails.net/doc/sensitive\\_documents/index.en.html](https://tails.net/doc/sensitive_documents/index.en.html)

# Password Manager (KeePassXC)

When you need to know a lot of passwords, it can be nice to have a secure way to store them (i.e. not a piece of paper next to your computer). KeePassXC is a password manager included in Tails (**Applications** → **Favorites** → **KeePassXC**) that allows you to store your passwords in a file and protect them with a single master password.

We recommend that you compartmentalize your passwords — have a different KeePassXC file for each separate project. They can share the same Master Password — the point of compartmentalization is that only one project's passwords are unlocked at any given time. If the Tails session is compromised, the adversary won't get all of your passwords in one fell swoop, just the ones that are currently unlocked.

In the terminology used by KeePassXC, a *password* is a random sequence of characters (letters, numbers, and other symbols), while a *passphrase* is a random sequence of words.



When you create a new KeePassXC database<sup>44</sup>, increase the decryption time in the **Encryption settings** window from the default to the maximum (5 seconds). Then choose a strong passphrase<sup>45</sup> and save your KeePassXC file. We recommend that you click the small dice icon in the password field to generate a random passphrase of 7-10 words.

This KeePassXC database file will contain all your passwords/passphrases and must persist between sessions on your Persistent Storage or on a separate LUKS-encrypted USB as described in Tails Best Practices<sup>46</sup>. As soon as you close KeePassXC or don't use it for a few minutes, it will lock. Make sure you do not forget your KeePassXC passphrase.

---

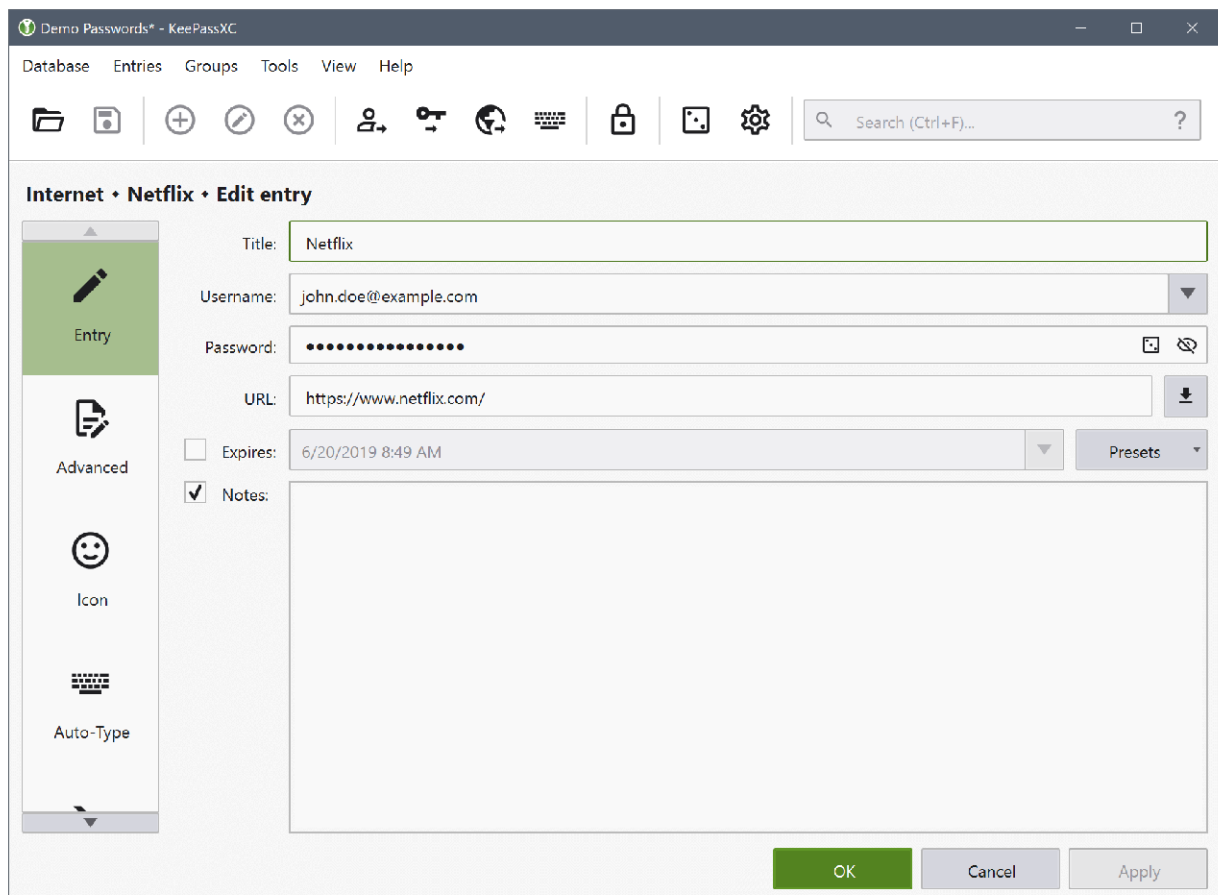
<sup>44</sup>[tails.net/doc/encryption\\_and\\_privacy/manage\\_passwords/index.en.html#index1h1](https://tails.net/doc/encryption_and_privacy/manage_passwords/index.en.html#index1h1)

<sup>45</sup>[anarsec.guide/posts/tails-best/#passwords](https://anarsec.guide/posts/tails-best/#passwords)

<sup>46</sup>[anarsec.guide/posts/tails-best/#using-a-write-protect-switch](https://anarsec.guide/posts/tails-best/#using-a-write-protect-switch)

After creating the database itself, you should see an empty “Root” folder. If you’d like to organize your passwords into different groups, right-click this folder and select “New Group...”.

You can now add your first entry. Click **Entries** → **New Entry**, or click the “plus” icon. Enter the title of the account, your username for the account, and your password. Click the “dice” icon to generate a random password or passphrase for the entry.



To copy a password from the database, select the entry and press CTRL + C. To copy a username, select the entry and press CTRL + B.

## Really delete data from a USB

Clicking “Permanently delete” or sending files to the “trash” does not delete data... and it can be very easy to recover it. When you “delete” a file, you are simply telling the operating system that you are no longer interested in the contents of that file. It then deletes its entry in the

index of existing files. It can then reuse the space that the data occupied to write something else.

However, it can take weeks or years before that space is actually used for new files, at which point the old data actually disappears. In the meantime, if you look directly at what is written to the drive, you can find the contents of the files. This is a fairly simple process, automated by many software programs that allow you to “recover” or “restore” data. You can’t really delete data, but you can overwrite data, which is a partial solution.

There are two types of storage: magnetic (HDD) and flash (SSD, NVMe, USB, memory cards, etc.). The only way to erase a file on either is to reformat the entire drive<sup>47</sup> and select **Overwrite existing data with zeros**.

However, traces of the previously written data may still remain. If you have sensitive documents that you really want to erase, it is best to physically destroy the USB after reformatting it. Fortunately, USBs are cheap and easy to steal. Be sure to reformat the drive before destroying it; destroying a drive is often a partial solution. Data can still be recovered from disk fragments, and burning a drive requires temperatures higher than a normal fire (e.g. thermite) to be effective.

For flash memory drives (USBs, SSDs, SD cards, etc.), use pliers to break the circuit board out of the plastic casing. Use a high-quality house-hold blender to shred the memory chips, including the circuit board, into pieces that are ideally less than two millimeters in size. This blender should not be used for food afterwards, because cleaning it will not adequately remove toxic traces.


## How to create an encrypted USB

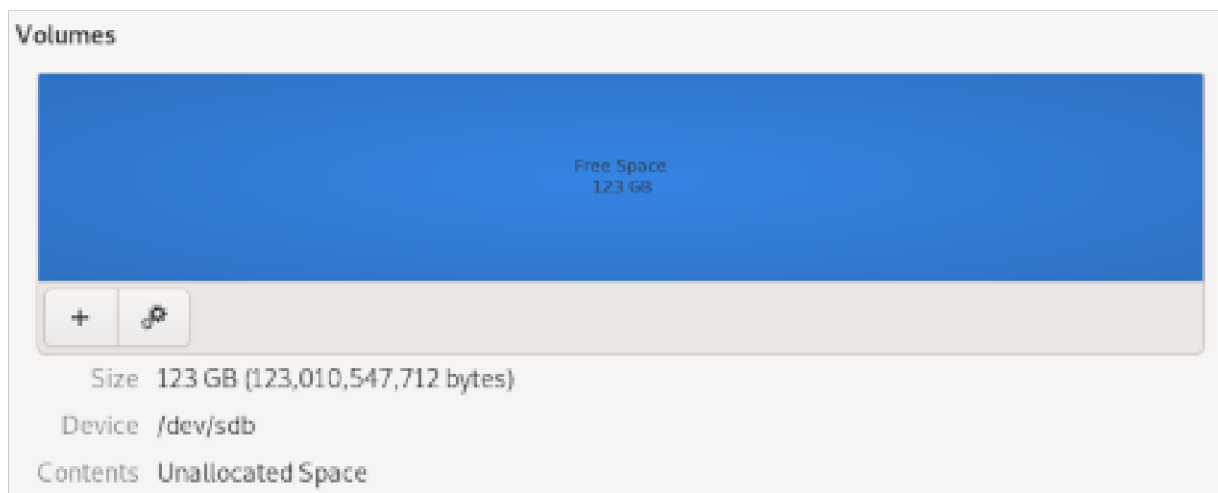
Store data only on encrypted drives. This is necessary if you want to use a separate LUKS USB instead of Persistent Storage on the Tails

---

<sup>47</sup>[anarsec.guide/posts/tails/#how-to-create-an-encrypted-usb](https://anarsec.guide/posts/tails/#how-to-create-an-encrypted-usb)

USB as advised in Tails Best Practices<sup>48</sup>. LUKS<sup>†</sup> is the Linux encryption standard. To encrypt a new USB, go to **Applications → Utilities → Disks**.

- When you insert the USB, a new “device” should appear in the list. Select it and make sure that the description (brand, name, size) matches your device. Be careful not to make a mistake!
- Format it by clicking  → **Format the disk**.
  - In the Erase drop-down list, select **Overwrite existing data with zeroes**. Note that this is not enough to remove all traces of sensitive documents stored on the USB.
  - In the Partitioning drop-down list, select **Compatible with all systems and devices (MBR/DOS)**.
  - Then click **Format...**



- Now you need to add the encrypted partition.
  - Click on the “+” button
  - Select the size of your partition (all free space)
  - For “Type” select **internal disk to be used with Linux systems only (Ext4)** check **Password protected volume (LUKS)**
  - Enter a strong passphrase<sup>49</sup>

If you insert an encrypted USB, you will be prompted to enter the passphrase. Before removing the drive after you are finished working

---

<sup>48</sup>[anarsec.guide/posts/tails-best/#using-a-write-protect-switch](https://anarsec.guide/posts/tails-best/#using-a-write-protect-switch)

<sup>49</sup>[anarsec.guide/posts/tails-best/#passwords](https://anarsec.guide/posts/tails-best/#passwords)



with it, you must right-click it in **Places** → **Computer** and select Eject.

## Encrypting a file with a password or public key

In Tails, you can use the Kleopatra application to encrypt a file<sup>50</sup> with a password or public PGP key. This creates a .pgp file. If you want to encrypt a file, do so in RAM before saving it to a LUKS USB. Once the unencrypted version of a file is saved on a USB, the USB must be reformatted to remove it.

For the same reason, before decrypting a file first copy it to a Tails folder that's only in RAM (e.g. **Places** → **Documents**).

## Adding administration rights

Tails requires an administration password (also called a “root” password) to perform system administration tasks. For example:

- Installing additional software
- Accessing the computer's internal hard drives
- Running commands<sup>†</sup> in the root terminal
- Accessing certain privileges, such as when you see a window that asks for administration authentication

By default, the administration password is disabled for added security. This can prevent an attacker with physical<sup>†</sup> or remote<sup>†</sup> access to your Tails system from gaining administration privileges. If you set an administration password for your session, you are creating another vector to potentially bypass Tails security.

To set an administration password, you must select an administration password on the Welcome Screen when you start Tails. This password is only valid for the duration of the session.

---

<sup>50</sup>[tails.net/doc/encryption\\_and\\_privacy/kleopatra/index.en.html#index1h1](https://tails.net/doc/encryption_and_privacy/kleopatra/index.en.html#index1h1)

# Installing additional software

If you install new software, it's up to you to make sure it's secure. Tails forces all software to connect to the internet through Tor, so you will need to configure this for applications that use the Internet<sup>51</sup>. The software used in Tails is audited for security, but this may not be the case for what you install. Before installing new software, it's best to make sure that Tails doesn't already have software that does the job you want it to do. If you want additional software to persist beyond a single session, you need to enable "Additional Software" in the Persistent Storage configuration<sup>52</sup>.

For more information, see the documentation on installing additional software<sup>53</sup>.

## Remember to make backups!

A Tails USB is easily lost, and USBs have a much shorter lifespan than hard drives (especially the cheap ones). If you have important data on it, remember to back it up regularly. If you use a second LUKS-encrypted USB, this is as simple as using the File Manager to copy files to a backup LUKS-encrypted USB.

If you use Persistent Storage, see the documentation for backing it up<sup>54</sup>.

## Privacy screen

A privacy screen<sup>55</sup> can be added to your laptop screen to prevent people (or hidden cameras) from seeing the content unless they are positioned directly in front of it.

---

<sup>51</sup>[tails.net/doc/persistent\\_storage/additional\\_software/index.en.html#index5h2](https://tails.net/doc/persistent_storage/additional_software/index.en.html#index5h2)

<sup>52</sup>[tails.net/doc/persistent\\_storage/configure/index.en.html](https://tails.net/doc/persistent_storage/configure/index.en.html)

<sup>53</sup>[tails.net/doc/persistent\\_storage/additional\\_software/index.en.html#index3h1](https://tails.net/doc/persistent_storage/additional_software/index.en.html#index3h1)

<sup>54</sup>[tails.net/doc/persistent\\_storage/backup/index.en.html](https://tails.net/doc/persistent_storage/backup/index.en.html)

<sup>55</sup>[en.wikipedia.org/wiki/Monitor\\_filter](https://en.wikipedia.org/wiki/Monitor_filter)

## III) Troubleshooting Issues

### *The computer tries to boot the USB but it doesn't work*

Check the error messages you get (for example, if you have an old 32-bit computer, it won't work with Tails). If it says Error starting GDM with your graphics card, the issue is with the graphics card; check the documentation for Known issues with graphics cards<sup>56</sup>. You can also check the list of known issues<sup>57</sup> on the Tails site for your computer model.

If the Tails Boot Loader page appears, try booting into Tails troubleshooting mode.

### *My Tails USB won't start anymore! (and it did start before on the same computer)*

After an upgrade or otherwise, Tails no longer starts on your computer. You have three options:

- 1) See if the Tails news page<sup>58</sup> mentions any problems with the upgrade.
- 2) Perform a manual upgrade<sup>59</sup>, which may be necessary if the computer was turned off before an automatic upgrade was complete.
- 3) If the first two solutions don't work, the USB is too old, of poor quality, or has been broken. If you need to recover data from Persistent Storage, plug that USB into a Tails session using another USB. It will appear as a normal USB that you will need to unlock with your password. If you can't access your data on another Tails USB that has Persistent Storage enabled, your USB may be dead.

### *I can't connect to a public Wi-Fi network with an authentication page (a captive portal)*

---

<sup>56</sup>[tails.net/support/known\\_issues/graphics/index.en.html](https://tails.net/support/known_issues/graphics/index.en.html)

<sup>57</sup>[tails.net/support/known\\_issues/index.en.html](https://tails.net/support/known_issues/index.en.html)

<sup>58</sup>[tails.net/news/index.en.html](https://tails.net/news/index.en.html)

<sup>59</sup>[anarsec.guide/posts/tails/#the-manual-upgrade](https://anarsec.guide/posts/tails/#the-manual-upgrade)

If you need to connect to Wi-Fi using a captive portal, you must enable Unsafe Browser in the Welcome Screen. Connect to Wi-Fi, and then open **Applications → Internet → Unsafe Browser**. You enter the URL of a site that isn't sketchy (e.g. wikipedia.org) to access the authentication page. Once you've completed the captive portal page, wait until Tor is ready, and then close the unsafe browser.

### ***What if I run out of space on a USB?***

If you run out of space on a USB drive, or if you see less data than you actually have on your USB, check "Show hidden files" in the file browser. There you will see new files named .something. The file .Trash-10xx is taking up space (and if you right-click on it and select "Move to Trash" it will be removed completely). Don't change any other hidden files.

### ***A file always opens in read-only mode or does not open at all?***

In some programs, this is normal if the same file is already open. If this isn't the case, use the same trick as in the paragraph above. You enable Show hidden files. There will be a .lock file with the same name as the file you have a problem with. Delete this file, which indicates that it is already open elsewhere. If that's not the issue, you need to change the permission rights of the file.

### ***I can't install Tails on a USB***

Make sure your USB is not known to have issues<sup>60</sup> with Tails. Format<sup>61</sup> the entire USB and try the installation again.

### ***Is an application slowing down Tails? The screen is glitching?***

Try pressing the Windows key, or the Cmd key for Mac, which will open the window with all your running applications, from where you can exit them. If that doesn't work, you'll need to force a shutdown by holding down the power button.

---

<sup>60</sup>[tails.net/support/known\\_issues/index.en.html#problematic-usb-sticks](https://tails.net/support/known_issues/index.en.html#problematic-usb-sticks)

<sup>61</sup>[anarsec.guide/posts/tails/#how-to-create-an-encrypted-usb](https://anarsec.guide/posts/tails/#how-to-create-an-encrypted-usb)

### *Add a printer*

You go to **Applications** → **System Tools** → **Settings** → **Devices** → **Printers** → “+” → **Add a printer**. Some printer models may not work with Tails (or may be difficult to set up).

### *Unable to install new software*

Sometimes the Synaptic Package Manager will refuse to install software. In this case, use a root terminal (which requires an administration password): install with the command `apt update && apt install [package_name]`

## Best Practices

Tails Best Practices<sup>62</sup> are important to establish before using Tails for highly sensitive activities like claiming an action<sup>63</sup>. To avoid overwhelming yourself, start by learning how to use Tails in basic ways, such as reading anarchist websites or writing texts. See the Tails tag<sup>64</sup> for tutorials on topics like removing identifying metadata from files<sup>65</sup>.

*This article draws from TuTORiel Tails<sup>66</sup> (in French), and Capulcu #1<sup>67</sup> (in German).*

## Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance<sup>68</sup> for

---

<sup>62</sup>[anarsec.guide/posts/tails-best](https://anarsec.guide/posts/tails-best)

<sup>63</sup>[notrace.how/resources/#how-submit](https://notrace.how/resources/#how-submit)

<sup>64</sup>[anarsec.guide/tags/tails/](https://anarsec.guide/tags/tails/)

<sup>65</sup>[anarsec.guide/posts/metadata/](https://anarsec.guide/posts/metadata/)

<sup>66</sup>[infokiosques.net/spip.php?article1726](https://infokiosques.net/spip.php?article1726)

<sup>67</sup>[capulcu.blackblogs.org/neue-texte/bandi/](https://capulcu.blackblogs.org/neue-texte/bandi/)

<sup>68</sup>[notrace.how/threat-library/techniques/targeted-digital-surveillance.html](https://notrace.how/threat-library/techniques/targeted-digital-surveillance.html)

the purposes of incrimination<sup>69</sup> and network mapping<sup>70</sup>. Our goal is to obscure the State’s visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France<sup>71</sup>: “So let’s be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which “private or confidential words are spoken” and must remain so, even if it’s switched off, we become a potential state informer...”

You may also be interested in the Threat Library’s “Digital Best Practices”<sup>72</sup>.

## Your Phone

**Operating system†:** **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists<sup>73</sup>. If you decide to have a phone, treat it like an “encrypted landline” and leave it at home when you are out of the house. See Kill the Cop in Your Pocket<sup>74</sup>.

## Your Computer

**Operating system†:** **Tails** is unparalleled for sensitive computer use (writing and sending communiques,

---

<sup>69</sup>[notrace.how/threat-library/tactics/incrimination.html](https://notrace.how/threat-library/tactics/incrimination.html)

<sup>70</sup>[notrace.how/threat-library/techniques/network-mapping.html](https://notrace.how/threat-library/techniques/network-mapping.html)

<sup>71</sup>[actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/](https://actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/)

<sup>72</sup>[notrace.how/threat-library/mitigations/digital-best-practices.html](https://notrace.how/threat-library/mitigations/digital-best-practices.html)

<sup>73</sup>[anarsec.guide/posts/grapheneos/](https://anarsec.guide/posts/grapheneos/)

<sup>74</sup>[anarsec.guide/posts/nophones/](https://anarsec.guide/posts/nophones/)

moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network<sup>†</sup>. See Tails for Anarchists<sup>75</sup> and Tails Best Practices<sup>76</sup>.

**Operating system<sup>†</sup>:** Qubes OS has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials<sup>77</sup>. Qubes OS can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists<sup>78</sup>.

See When to Use Tails vs. Qubes OS<sup>79</sup>. We do not offer “harm reduction” advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

## Encrypted Messaging

See Encrypted Messaging for Anarchists<sup>80</sup>

## Storing Electronic Devices

See Make Your Electronics Tamper-Evident<sup>81</sup>.

---

<sup>75</sup>[anarsec.guide/posts/tails/](https://anarsec.guide/posts/tails/)

<sup>76</sup>[anarsec.guide/posts/tails-best/](https://anarsec.guide/posts/tails-best/)

<sup>77</sup>[anarsec.guide/posts/linux](https://anarsec.guide/posts/linux)

<sup>78</sup>[anarsec.guide/posts/qubes/](https://anarsec.guide/posts/qubes/)

<sup>79</sup>[anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os](https://anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os)

<sup>80</sup>[anarsec.guide/posts/e2ee/](https://anarsec.guide/posts/e2ee/)

<sup>81</sup>[anarsec.guide/posts/tamper/](https://anarsec.guide/posts/tamper/)

# Appendix: Glossary

## Command Line Interface (CLI)

The “command line” is an all-text alternative to the graphical “point and click” tool that most of us are more familiar with; the Command Line Interface (CLI) allows us to do some things that a Graphical User Interface (GUI) does not. Often, either a GUI or a CLI would work, and which you use is a matter of preference. For example, in Tails<sup>†</sup>, you can verify the checksum<sup>82</sup> of a file using either a GUI (the GtkHash program) or a CLI command (sha256sum).

For more information, see Linux Essentials<sup>83</sup>. The Tech Learning Collective’s “Foundations: Linux Journey” course on the command line<sup>84</sup> is our recommended introduction to using the CLI/terminal.

## Correlation Attack

An end-to-end correlation attack is a theoretical way that a global adversary could break the anonymity of the Tor network<sup>†</sup>. For more information, see Protecting against determined, skilled attackers<sup>85</sup> and Make Correlation Attacks More Difficult<sup>86</sup>. For research papers on the subject, see Thirteen Years of Tor Attacks<sup>87</sup> and the design proposal on information leaks in Tor<sup>88</sup>.

---

<sup>82</sup>[anarsec.guide/glossary](https://anarsec.guide/glossary)

<sup>83</sup>[anarsec.guide/posts/linux/#the-command-line-interface](https://anarsec.guide/posts/linux/#the-command-line-interface)

<sup>84</sup>[techlearningcollective.com/foundations/linux-journey/the-shell](https://techlearningcollective.com/foundations/linux-journey/the-shell)

<sup>85</sup>[anarsec.guide/posts/tails-best/#2-protecting-against-determined-skilled-attackers](https://anarsec.guide/posts/tails-best/#2-protecting-against-determined-skilled-attackers)

<sup>86</sup>[anarsec.guide/posts/tails/#make-correlation-attacks-more-difficult](https://anarsec.guide/posts/tails/#make-correlation-attacks-more-difficult)

<sup>87</sup>[github.com/Attacks-on-Tor/Attacks-on-Tor#correlation-attacks](https://github.com/Attacks-on-Tor/Attacks-on-Tor#correlation-attacks)

<sup>88</sup>[spec.torproject.org/proposals/344-protocol-info-leaks.html](https://spec.torproject.org/proposals/344-protocol-info-leaks.html)



# Exploit

An exploit is designed to take advantage of a vulnerability<sup>82</sup>. Even worse (or better, depending on whether you are the attacker or the target) are zero-day exploits<sup>82</sup>.

# HTTPS

The “S” in HTTPS stands for “secure”; which means that your Internet connection is encrypted using the Transport Layer Security (TLS)<sup>89</sup> protocol. This involves the website generating a certificate using public-key cryptography<sup>82</sup> that can be used to verify its authenticity — that you are actually connecting to the web server you intended, and that this connection is encrypted.

For more information, see our explanation<sup>90</sup> or Defend Dissent: Protecting Your Communications<sup>91</sup>.

# LUKS

The Linux Unified Key Setup (LUKS)<sup>92</sup> is a platform-independent specification for disk encryption. It is the standard used in Tails<sup>†</sup>, Qubes OS<sup>†</sup>, Ubuntu, etc. LUKS encryption is only effective when the device is powered off. LUKS should use Argon2id<sup>49</sup> to make it less vulnerable to brute-force attacks.

# Man-in-the-middle attack

An example of a man-in-the-middle attack is when Alice communicates with Bob over the Internet, Eve (eavesdropper) joins the

---

<sup>89</sup>[youtube.com/watch?v=0TLDTodL7Lc&listen=false](https://youtube.com/watch?v=0TLDTodL7Lc&listen=false)

<sup>90</sup>[anarsec.guide/posts/tails/#what-is-https](https://anarsec.guide/posts/tails/#what-is-https)

<sup>91</sup>[open.oregonstate.edu/defenddissent/chapter/protecting-your-communications/](https://open.oregonstate.edu/defenddissent/chapter/protecting-your-communications/)

<sup>92</sup>[gitlab.com/cryptsetup/cryptsetup](https://gitlab.com/cryptsetup/cryptsetup)

<sup>49</sup>[anarsec.guide/posts/tails-best/#passwords](https://anarsec.guide/posts/tails-best/#passwords)

conversation “in the middle” and becomes the man-in-the-middle. Eve can modify, insert, replay, or read messages at will. Protective measures include encryption (confidentiality) and checking the authenticity and integrity of all messages. However, you must also make sure that you are communicating with the expected party. You must verify that you have the real public key of the recipient. For example, this is what you do when you verify a contract’s “Safety Number” in the Signal encrypted messaging app.

For a more detailed look, see *Defend Dissent: The Man in the Middle*<sup>93</sup> and the Whonix documentation<sup>94</sup>.

## Open-source

The only software we can trust because the “source code” that it is written in is “open” for anyone to examine.

## Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android, and iOS. Linux and some versions of Android are the only open-source options on this list.

## Phishing

Phishing is a technique of social engineering<sup>82</sup>. Attackers send SMS messages, emails, chat messages, etc. to their targets to get their personal information. The attackers can then try to impersonate their victims. It can also be used to get the victim to download malware<sup>82</sup> onto a system, which can be used as a starting point for hacking. Spear phishing<sup>82</sup> is a more sophisticated form of phishing. For more information, see the Kicksecure documentation<sup>95</sup>.

---

<sup>93</sup>[open.oregonstate.edu/defenddissent/chapter/the-man-in-the-middle/](https://open.oregonstate.edu/defenddissent/chapter/the-man-in-the-middle/)

<sup>94</sup>[whonix.org/wiki/Warning#Man-in-the-middle\\_Attacks](https://whonix.org/wiki/Warning#Man-in-the-middle_Attacks)

<sup>95</sup>[kicksecure.com/wiki/Social\\_Engineering](https://kicksecure.com/wiki/Social_Engineering)

# Physical attacks

A physical attack is a situation where an adversary first gains physical access to your device through loss, theft, or confiscation. For example, your phone may be confiscated when you cross a border or are arrested. This is in contrast to a remote attack<sup>†</sup>.

For more information, see Making Your Electronics Tamper-Evident<sup>96</sup>, the Threat Library<sup>97</sup>, the KickSecure documentation<sup>98</sup>, and Defend Dissent: Protecting Your Devices<sup>99</sup>.

# Remote attacks

By remote attack, we mean that an adversary would access the data on your phone or laptop through an Internet or data connection. There are companies that develop and sell the ability to infect your device (usually focusing on smartphones) with malware<sup>82</sup> that would allow their customer (your adversary, be it a corporate or state agent) to remotely access some or all of your information. This is in contrast to a physical attack<sup>†</sup>.

For a more detailed look, see Defend Dissent: Protecting Your Devices<sup>100</sup>.

# Sandboxing

Sandboxing is the software-based isolation of applications to mitigate system failures or vulnerabilities. For example, if an attacker hacks an application that is “sandboxed”, the attacker must escape the sandbox to hack the entire system. Virtualization<sup>82</sup> is the most powerful implementation of sandboxing.

---

<sup>96</sup>[anarsec.guide/posts/tamper](https://anarsec.guide/posts/tamper)

<sup>97</sup>[notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html](https://notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html)

<sup>98</sup>[kicksecure.com/wiki/Protection\\_Against\\_Physical\\_Attacks](https://kicksecure.com/wiki/Protection_Against_Physical_Attacks)

<sup>99</sup>[open.oregonstate.edu/defenddissent/chapter/protecting-your-devices/](https://open.oregonstate.edu/defenddissent/chapter/protecting-your-devices/)

<sup>100</sup>[open.oregonstate.edu/defenddissent/chapter/protecting-your-devices/](https://open.oregonstate.edu/defenddissent/chapter/protecting-your-devices/)

# Threat model

Threat modeling is a family of activities for improving security by identifying a set of adversaries, security goals<sup>82</sup>, and vulnerabilities<sup>82</sup>, and then defining countermeasures to prevent or mitigate the effects of threats to the system. A threat is a potential or actual undesirable event that can be malicious (such as a DDoS attack<sup>82</sup>) or accidental (such as a hard drive failure). Threat modeling is the deliberate activity of identifying and assessing threats and vulnerabilities.

For more information, see the No Trace Project Threat Library<sup>101</sup>, Defend Dissent: Digital Threats to Social Movements<sup>102</sup> and Defending against Surveillance and Suppression<sup>103</sup>.

# Tor network

Tor<sup>104</sup> (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet connection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor “the King of high secure, low latency Internet anonymity” with “no contenders for the throne in waiting”. The Tor network can be accessed through the Tor Browser on any operating system. The Tails<sup>†</sup> operating system

---

<sup>101</sup>[notrace.how/threat-library/](https://notrace.how/threat-library/)

<sup>102</sup>[open.oregonstate.edu/defenddissent/chapter/digital-threats/](https://open.oregonstate.edu/defenddissent/chapter/digital-threats/)

<sup>103</sup>[open.oregonstate.edu/defenddissent/chapter/surveillance-and-suppression/](https://open.oregonstate.edu/defenddissent/chapter/surveillance-and-suppression/)

<sup>104</sup>[torproject.org/](https://torproject.org/)

forces every program to use the Tor network when accessing the Internet.

For more information, see [Tails for Anarchists](#)<sup>105</sup> and [Privacy Guides](#)<sup>106</sup>. To understand the limitations of Tor, see the [Whonix documentation](#)<sup>107</sup>.

---

<sup>105</sup>[anarsec.guide/posts/tails/#tor](https://anarsec.guide/posts/tails/#tor)

<sup>106</sup>[privacyguides.org/en/advanced/tor-overview/](https://privacyguides.org/en/advanced/tor-overview/)

<sup>107</sup>[whonix.org/wiki/Warning](https://whonix.org/wiki/Warning)



AnarSec is a resource designed to help anarchists navigate the hostile terrain of technology — defensive guides for digital security and anonymity, as well as offensive guides for hacking. All guides are available in booklet format for printing and will be kept up to date.

## **Defensive**

### ***Tails***

- Tails for Anarchists
- Tails Best Practices

### ***Qubes OS***

- Qubes OS for Anarchists

### ***Phones***

- Kill the Cop in Your Pocket
- GrapheneOS for Anarchists

### ***General***

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

## **Offensive**

*Coming soon*

Tails is an operating system that makes anonymous computer use accessible to everyone. Tails is designed to leave no trace of your activity on your computer unless you explicitly configure it to save specific data. It accomplishes this by running from a DVD or USB, independent of the operating system installed on the computer. Tails comes with several built-in applications preconfigured with security in mind, and all anarchists should know how to use it for secure communication, research, editing, and publishing sensitive content.

