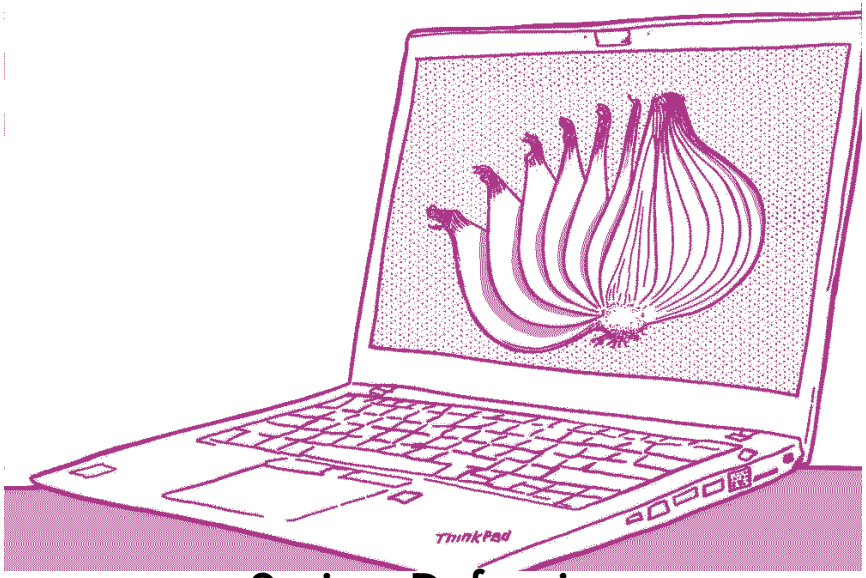
Tails Best Practices

All anarchists should know how to use Tails — this text describes some additional precautions you can take that are relevant to an anarchist threat model. Not all anarchist threat models are the same, and only you can decide which mitigations are worth putting into practice for your activities, but we aim to provide advice that is appropriate for high-risk activities like claiming an action. If you are new to Tails, start with Tails for Anarchists.



Series: Defensive

This version of the zine was last edited on 2024-11-25. Visit 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.

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

Contents

mentation[149].

[149] whonix.org/wiki/Warning

event that can be malicious (such as a DDoS attack[116]) 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[143], Defend Dissent: Digital Threats to Social Movements[144] and Defending against Surveillance and Suppression[145].

Tor network

Tor[146] (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† operating system forces every program to use the Tor network when accessing the Internet.

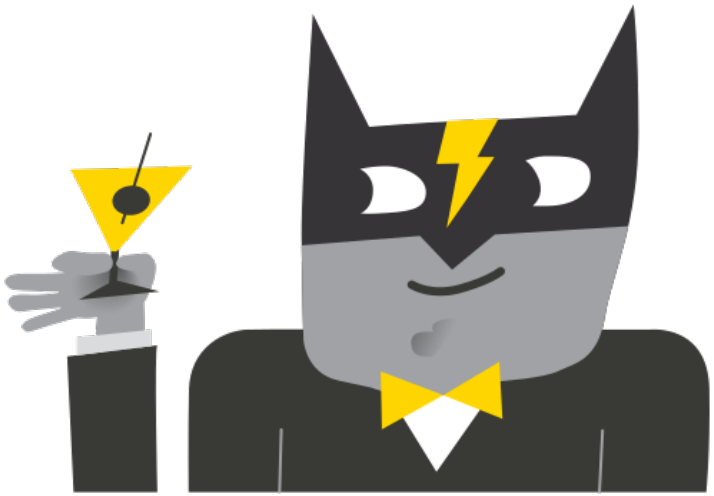
For more information, see Tails for Anarchists[147] and Privacy Guides[148]. To understand the limitations of Tor, see the Whonix docu-

[143] notrace.how/threat-library/
[144] open.oregonstate.education/defenddissent/chapter/digital-threats/
[145] open.oregonstate.education/defenddissent/chapter/surveillance-and-suppression/
[146] torproject.org/
[147] anarsec.guide/posts/tails/#tor
[148] privacyguides.org/en/advanced/tor-overview/

All anarchists should know how to use Tails — this text describes some additional precautions you can take that are relevant to an anarchist threat model†. Not all anarchist threat models are the same, and only you can decide which mitigations are worth putting into practice for your activities, but we aim to provide advice that is appropriate for high-risk activities like claiming an action. If you are new to Tails, start with Tails for Anarchists[1].

We'll begin by looking at the three topics covered on the Tails Warnings page[2]: protecting your identity, limitations of the Tor network, and untrusted computers.

Protecting your identity when using Tails



[1] anarsec.guide/posts/tails/
[2] tails.net/doc/about/warnings/index.en.html

Tails is designed to hide your identity. But some of your activities could reveal your identity:

1. Sharing files with metadata†, such as date, time, location, and device information
2. Using Tails for more than one purpose at a time

1. Sharing files with metadata

You can mitigate this first issue by **cleaning metadata from files before sharing them**:

- To learn how, see Remove Identifying Metadata From Files[3].

2. Using Tails for more than one purpose at a time

You can mitigate this second issue by what's called **"compartmentalization"**:

- Compartmentalization[4] means keeping different activities or projects separate. If you use Tails sessions for more than one purpose at a time, an adversary could link your different activities together. For example, if you log into different accounts on the same website in a single Tails session, the website could determine that the accounts are being used by the same person. This is because websites can tell when two accounts are using the same Tor circuit.
- To prevent an adversary from linking your activities while using Tails, restart Tails between different activities. For example, restart Tails between checking different project emails.
- Tails is amnesiac by default, so to save any data from a Tails session, you must save it to a USB. If the files you save could be used to link your activities together, use a different encrypted (LUKS†) USB stick

[3] anarsec.guide/posts/metadata/

[4] notrace.how/threat-library/mitigations/compartmentalization.html

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[116] 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†.

For a more detailed look, see Defend Dissent: Protecting Your Devices[142].

Spear phishing

Spear phishing is more sophisticated than regular phishing†, which casts a wide net. In spear phishing, attackers customize their forged messages and send them to a smaller number of potential victims. Spear phishing requires more research on the part of the attacker; however, the success rate of spear phishing attacks is higher than the success rate of regular phishing attacks.

Synchronous communication

Unlike asynchronous communication†, both parties must be online at the same time. This does not require servers for the communication and is often referred to as "peer to peer".

Threat model

Threat modeling is a family of activities for improving security by identifying a set of adversaries, security goals[116], and vulnerabilities[116], and then defining countermeasures to prevent or mitigate the effects of threats to the system. A threat is a potential or actual undesirable

[142] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/

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†.

For more information, see Making Your Electronics Tamper-Evident[136], the Threat Library[137], the KickSecure documentation[138], and Defend Dissent: Protecting Your Devices[139].

Public-key cryptography

Public-key cryptography (or asymmetric cryptography) is the opposite of symmetric cryptography[116]. Each party has two keys (public and private). The private key must be kept secret and is used for decryption; the public key must be made public, and is used for encryption. This is the model used for encrypted communication, since the public key cannot be used for decryption. All other parties must verify that a published public key belongs to its intended owner to avoid man-in-the-middle attacks[116].

There are several approaches to public-key cryptography. For example, some cryptosystems are based on the algebraic structure of elliptic curves over finite fields (ECC). Others are based on the difficulty of factoring the product of two large prime numbers (RSA). Public-key cryptography can also be used for digital signatures†.

To learn more, watch this video[140], or for a more detailed look, see Defend Dissent: Public-Key Cryptography[141].

[136] anarsec.guide/posts/tamper
[137] notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html
[138] kicksecure.com/wiki/Protection_Against_Physical_Attacks
[139] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/
[140] youtube.com/watch?v=GSIDS_lvRv4
[141] open.oregonstate.education/defenddissent/chapter/public-key-cryptography/

for each activity. For example, use one Tails USB stick for moderating a website and another for researching actions. Tails has a feature called Persistent Storage, but we do not recommend using it for data storage, which we explain below[5].

Limitations of the Tor network

Tails uses the Tor network† because it is the strongest and most popular network to protect from surveillance and censorship. But Tor has limitations if you are concerned about:

1. Hiding that you are using Tor and Tails
2. Protecting your online communications from determined, skilled attackers

1. Hiding that you are using Tor and Tails

You can mitigate this first issue by **Tor bridges**[6]:

[5] anarsec.guide/posts/tails-best/#using-a-write-protect-switch
[6] tails.net/doc/anonymous_internet/tor/index.en.html#bridges

- Tor Bridges are secret Tor relays that hide your connection to the Tor network. However, this is only necessary where connections to Tor are blocked, such as in heavily censored countries, by some public networks, or by some parental control software. This is because Tor and Tails don't protect you by making you look like any other Internet user, but by making all Tor and Tails users look the same. It becomes impossible to tell who is who among them.

2. Protecting against determined, skilled attackers

An *end-to-end correlation* attack† is a theoretical way that a global adversary could break Tor's anonymity:

> A powerful adversary, who could analyze the timing and shape of the traffic entering and exiting the Tor network, might be able to deanonymize Tor users. These attacks are called *end-to-end correlation* attacks, because the attacker has to observe both ends of a Tor circuit at the same time. [...] End-to-end correlation attacks have been studied in research papers, but we don't know of any actual use to deanonymize Tor users.

Non-Targeted and Targeted Correlation Attacks

As described in the quotation above, a global adversary (i.e. the NSA) may be capable of breaking Tor through a correlation attack. If this happens, the Internet address you used in a coffee shop without CCTV cameras will only lead to your general area (e.g. your city) because it is not associated with you. Of course, this is less true if you use the location routinely. Correlation attacks are even less feasible against connections to an .onion address because you never leave the Tor network, so there is no "end" to correlate with through network traffic analysis (if the server location is unknown to the adversary). It is

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.

Passphrase

A passphrase is similar to a password†, but is made up of words instead of random characters.

Password

A password is a string of characters used for authentication. A strong password consists of randomly chosen characters that all have the same probability of occurrence and can be created with the KeePassXC Password Generator.

For more information, see Defend Dissent: Passwords[134]

Phishing

Phishing is a technique of social engineering[116]. 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[116] onto a system, which can be used as a starting point for hacking. Spear phishing† is a more sophisticated form of phishing. For more information, see the Kicksecure documentation[135].

[134] open.oregonstate.education/defenddissent/chapter/passwords/
[135] kicksecure.com/wiki/Social_Engineering

For more information, see this primer[128]. We don't recommend it for encrypted communications, here's why[129].

LUKS

The Linux Unified Key Setup (LUKS)[130] is a platform-independent specification for disk encryption. It is the standard used in Tails†, Qubes OS†, Ubuntu, etc. LUKS encryption is only effective when the device is powered off. LUKS should use Argon2id[131] to make it less vulnerable to brute-force attacks.

Metadata

Metadata is data that provides information about other data. For example, a JPG file contains the actual image (data) but it may also contain metadata such as the date the file was created, the type of camera, GPS coordinates, and so on. Metadata can be valuable to attackers (to find appropriate exploits for outdated software the target is using), government agencies (to collect information about people to create social graphs), and other parties (to target location-based advertising). Whenever you use a computer, you are likely leaving metadata behind.

For more information, see Remove Identifying Metadata From Files[132] and Defend Dissent: Metadata[133].

Open-source

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

[128] github.com/AnarchoTechNYC/meta/wiki/Pretty-Good-Privacy-%28PGP%29
[129] anarsec.guide/posts/e2ee/#pgp-email
[130] gitlab.com/cryptsetup/cryptsetup
[131] anarsec.guide/posts/tails-best/#passwords
[132] anarsec.guide/posts/metadata
[133] open.oregonstate.education/defenddissent/chapter/metadata/

worth emphasizing that "End-to-end correlation attacks have been studied in research papers, but we don't know of any actual use to deanonymize Tor users."

What we will term a "targeted" correlation attack is much more likely because a non-global adversary (i.e. local law enforcement) is capable of it, if you are already in their sights and a target of physical surveillance[7] and/or digital surveillance[8]. This is a subtype of correlation attack where the presumed target is already known, thus making the attack easier to achieve because it vastly reduces the amount of data to filter through for correlation. A non-targeted correlation attack used to deanonymize a Tor user is unprecedented in current evidence used in court, although a "targeted" correlation attack has been used[9] as corroborating evidence — a suspect had already been identified, which allowed investigators to correlate their observed footprint with specific online activity. Specifically, they correlated Tor network traffic coming from the suspect's house with the times their anonymous alias was online in chatrooms.

To explain how this works, it helps if you have a basic understanding of what Tor information is visible to various third parties — see the EFF's interactive graphic[10]. For a non-targeted correlation attack, the investigator will need to *start from after Tor's exit node*: take the specific online activity coming from the exit node and try to correlate it with an enormous amount of global data that is entering Tor entry nodes. However, if a suspect is already identified, the investigator can instead do a "targeted" correlation attack and *start from before Tor's entry node*: take the data entering the entry node (via the suspect's *physical or digital footprint*) and try to correlate it with *specific online activity* coming from an exit node.

[7] notrace.how/threat-library/techniques/physical-surveillance/covert.html
[8] notrace.how/threat-library/techniques/targeted-digital-surveillance.html
[9] medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8
[10] eff.org/pages/tor-and-https

For your *physical footprint*, a surveillance operation can observe you go to a cafe regularly, then try to correlate this with online activity they suspect you of (for example, if they suspect you are a website moderator, they can try to correlate these time windows with web moderator activity). For your *digital footprint*, if you are using Internet from home, an investigator can observe all your Tor traffic and then try to correlate this with online activity they suspect you of. For your *specific online activity*, a more sophisticated analysis would involve logging the connections to the server for detailed comparison, and a simple analysis would be something that is publicly visible to anyone (such as when your alias is online in a chatroom, or when a post is published to a website).

You can mitigate the techniques available to powerful adversaries by **prioritizing .onion links when available**, by **taking the possibility of targeted surveillance into account** and by **using an Internet connection that is not tied to your identity**.

An Internet connection not tied to your identity

Using an Internet connection that is not tied to your identity means that if an attack on the Tor network succeeds, it still doesn't deanonymize you. You have two options: using Wi-Fi from a public space (like going to a cafe without CCTV cameras), or using a Wi-Fi antenna through a window from a private space.

Working from a public space

If you only need to use the Internet irregularly, such as to submit a communique or do action research, you can **do surveillance detection[11] and anti-surveillance[12] before going to a coffee shop**, just like you would prior to a direct action. See "How to submit an anony-

[11] notrace.how/threat-library/mitigations/surveillance-detection.html
[12] notrace.how/threat-library/mitigations/anti-surveillance.html
[13] notrace.how/resources/#how-submit

Encryption

Encryption is the process of scrambling a message so that it can only be unscrambled (and read) by the intended parties. The method you use to scramble the original message, or *plaintext*, is called the *cipher* or *encryption protocol*. In almost all cases, the cipher is not intended to be kept secret. The scrambled, unreadable, encrypted message is called the ciphertext and can be safely shared. Most ciphers require an additional piece of information, called a *cryptographic key*, to encrypt and decrypt (scramble and unscramble) messages.

For more information, see symmetric cryptography[116], asymmetric cryptography†, or Defend Dissent: What is Encryption?[126]

Forward secrecy

Forward secrecy (FS, also known as "Perfect Forward Secrecy") combines a system of long-term keys and session keys to protect encrypted communications from future key compromise. An attacker who can record every encrypted message (man-in-the-middle[116]) won't be able to decrypt those messages if the keys are compromised in the future. Modern encryption protocols such as TLS[116] 1.3 and the Signal Protocol provide FS. For more information, see Anonymous Planet[127].

GnuPG / OpenPGP

GnuPG (GPG) is a program that implements the OpenPGP (Pretty Good Privacy) standard. GPG provides cryptographic functions for encrypting, decrypting, and signing text and files. It is a classic example of public-key cryptography†. When used with email, metadata† (such as email addresses) remains unencrypted. It does not provide forward secrecy†.

[126] open.oregonstate.education/defenddissent/chapter/what-is-encryption/
[127] anonymousplanet.org/guide.html#forward-secrecy

can verify the checksum[116] of a file using either a GUI (the GtkHash program) or a CLI command (`sha256sum`).

For more information, see Linux Essentials[117]. The Tech Learning Collective's "Foundations: Linux Journey" course on the command line[118] 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†. For more information, see Protecting against determined, skilled attackers[119] and Make Correlation Attacks More Difficult[120]. For research papers on the subject, see Thirteen Years of Tor Attacks[121] and the design proposal on information leaks in Tor[122].

Digital Signatures

Digital signatures are based on public-key cryptography†. A private key is used to digitally sign data, while the corresponding public key is used by third parties to verify the signature. Before a public key is used to verify a signature, its authenticity should be verified.

To learn more, watch this video[123]. For a more detailed look, see Defend Dissent: Authenticity through Cryptographic Signing[124] or our GPG explanation[125].

[117] anarsec.guide/posts/linux/#the-command-line-interface

[118] techlearningcollective.com/foundations/linux-journey/the-shell

[119] anarsec.guide/posts/tails-best/#2-protecting-against-determined-skilled-attackers

[120] anarsec.guide/posts/tails/#make-correlation-attacks-more-difficult

[121] github.com/Attacks-on-Tor/Attacks-on-Tor#correlation-attacks

[122] spec.torproject.org/proposals/344-protocol-info-leaks.html

[123] youtube.com/watch?v=s22eJ1eVLTU&listen=false

[124] open.oregonstate.education/defenddissent/chapter/cryptographic-signing/

[125] anarsec.guide/posts/tails-best/#appendix-gpg-explanation

mous communiqué and get away with it"[13] for more information on what submitting a communique involves.

When using Wi-Fi in a public space, keep the following operational security considerations in mind:

- Timing is a relevant consideration. If you want to submit a report-back the morning after a riot, or a communique shortly after an action (times when there may be a higher risk of targeted surveillance), consider waiting instead. In 2010, the morning after a bank arson in Canada, police surveilled a suspect as he traveled from his home to an Internet cafe, and watched him post the communique and then bury the laptop in the woods. More recently, investigators physically surveilling an anarchist in France[14] installed a hidden camera to monitor access to an Internet cafe near the comrade's home and requested CCTV footage for the day an arson communique was sent.
- Do not get into a routine of using the same cafes repeatedly if you can avoid it. The more regularly you use a space, the more the Internet is tied to your identity. Additionally, if a surveillance effort knows your destination, anti-surveillance will not be effective.
- If you have to buy a coffee to get the Wi-Fi password, pay in cash!
- Position yourself with your back against a wall so that no one can "shoulder surf" to see your screen, and ideally install a privacy screen[15] on your laptop. If you write a communique in an offline Tails session before your trip to the public space, you only need a few minutes locked in a public bathroom to send it in.
- If coffee shops without CCTV cameras are few and far between, you can try accessing a coffee shop's Wi-Fi from outside, out of view of the cameras.
- Maintain situational awareness and be ready to pull out the Tails USB to shut down the computer at a moment's notice. It is very difficult to maintain adequate situational awareness while staying fo-

[14] notrace.how/resources/#ivan

[15] anarsec.guide/posts/tails/#privacy-screen

cused on your Tails session — consider asking a trusted friend to hang out who can dedicate themselves to keeping an eye on your surroundings. If the Tails USB is removed, Tails will shut down and overwrite the RAM with random data[16]. Any LUKS USBs that were unlocked in the Tails session will now be encrypted again. Note that Tails warns[17] "Only physically remove the USB stick in case of emergency as doing so can sometimes break the file system of the Persistent Storage."

- One person in charge of a darknet marketplace had his Tails computer seized while distracted by a fake fight next to him. Similar tactics have been used in other police operations[18]. If his Tails USB had been attached to a belt with a short piece of fishing line, the police would most likely have lost all evidence when the Tails USB was pulled out. A more technical equivalent is BusKill[19] — however, we only recommend buying this in person[20] or 3D printing it[21]. This is because any mail can be intercepted[22] and altered, making the hardware malicious[23].

Working from a private space

If you need to regularly use the Internet for projects like moderating a website or hacking, going to a new Wi-Fi location after doing surveillance countermeasures might not be realistic on a daily basis. Additionally, a main police priority will be to seize the computer while it is unencrypted, and this is much easier for them to achieve in a public space, especially if you are alone. In this scenario, the ideal mitigation is to **use a Wi-Fi antenna positioned behind a window in a private space to access from a few hundred metres away** — a physi-

[16] tails.net/doc/advanced_topics/cold_boot_attacks/index.en.html
[17] tails.net/doc/first_steps/shutdown/index.en.html
[18] dys2p.com/en/2023-05-luks-security.html#attacks
[19] buskill.in/tails/
[20] buskill.in/leipzig-proxystore/
[21] buskill.in/3d-print-2023-08/
[22] docs.buskill.in/buskill-app/en/stable/faq.html#q-what-about-interdiction
[23] en.wikipedia.org/wiki/BadUSB

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[115].

Appendix: Glossary

Asynchronous Communication

Unlike synchronous communication†, both parties do not need to be online at the same time. This relies on some sort of server to store messages until the message recipients come online. This is the type of messaging that most people are familiar with (email, etc.).

Brute-force attack

An attacker who "simply" tries every possible key to access a service or decrypt a file is using "brute force." This process is called a brute-force attack. More powerful computers make brute-force attacks more feasible. Modern cryptographic protocols are designed to force an adversary (who does not have the cryptographic key) to spend (nearly) as much time as it would take to try every possible key to break the code. The parameters of a good protocol are chosen to make this amount of time impractical.

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†, you

[115] anarsec.guide/posts/tamper/
[116] anarsec.guide/glossary

Your Computer

Operating system†: Tails is unparalleled for sensitive computer use (writing and sending communiques, 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†. See Tails for Anarchists[109] and Tails Best Practices[110].

Operating system†: 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[111]. 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[112].

See When to Use Tails vs. Qubes OS[113]. 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[114]

[109] anarsec.guide/posts/tails/
[110] anarsec.guide/posts/tails-best/
[111] anarsec.guide/posts/linux
[112] anarsec.guide/posts/qubes/
[113] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[114] anarsec.guide/posts/e2ee/

cal surveillance effort won't observe you entering a cafe or be able to easily seize your powered-on laptop, and a digital surveillance effort won't observe anything on your home Internet. To protect against hidden cameras[24], you should still be careful about where you position your screen.

If a Wi-Fi antenna is too technical for you, you may even want to **use your home internet** for some projects that require frequent internet access. This contradicts the previous advice to not use an Internet connection that is tied to your identity. It's a trade-off: using Tor from home avoids creating a physical footprint that is so easy to observe, at the expense of creating a digital footprint which is more technical to observe, and may be harder to draw meaningful conclusions from. There are two main deanonymization risks to consider when using your home internet: that the adversary deanonymizes you through a Tor correlation attack, or that they deanonymize you by hacking your system (such as through phishing[25]) which enables them to bypass Tor[26]. To make both of these attacks more difficult, we recommend connecting to a VPN *before* connecting to Tor (i.e. You → VPN → Tor → Internet[27]) when using Tails from home, which requires running the VPN from your networking device (either a router or a hardware firewall). For more information on the rationale, see Privacy Guides[28].

To summarize

For sensitive and irregular Internet activities, use an Internet connection from a random cafe, preceeded by surveillance detection and anti-surveillance. For activities that require daily Internet access such that taking surveillance countermeasures and finding a new cafe isn't realistic, it's best to use a Wi-Fi antenna. If this is too technical for you, using your home Wi-Fi is an option, but this requires trusting Tor's re-

[24] notrace.how/earsandeyes
[25] anarsec.guide/posts/tails-best/#phishing-awareness
[26] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[27] gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN#you-vpnssh-tor
[28] privacyguides.org/en/advanced/tor-overview/#safely-connecting-to-tor

silience to correlation attacks, the measures you take against being hacked, and your VPN provider.

Reducing risks when using untrusted computers

Tails can safely run on a computer that has a virus. But Tails cannot always protect you when:

1. Installing from an infected computer
2. Running Tails on a computer with a compromised BIOS, firmware, or hardware

1. Installing from an infected computer

You can mitigate this first issue by **using a computer you trust to install Tails**:

gence agencies that conduct targeted digital surveillance[102] for the purposes of incrimination[103] and network mapping[104]. 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[105]: "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"[106].

Your Phone

Operating system†: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[107]. 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[108].

[102] notrace.how/threat-library/techniques/targeted-digital-surveillance.html
[103] notrace.how/threat-library/tactics/incrimination.html
[104] notrace.how/threat-library/techniques/network-mapping.html
[105] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/
[106] notrace.how/threat-library/mitigations/digital-best-practices.html
[107] anarsec.guide/posts/grapheneos/
[108] anarsec.guide/posts/nophones/

Step: Verify the Tails public key

- `gpg --import < tails-signing.key` imports the Tails public key into your keyring so that it can be used.
- `gpg --keyring=/usr/share/keyrings/debian-keyring.gpg --export chris@chris-lamb.co.uk | gpg --import` imports the public key of a Debian developer into your keyring so that it can be used.
- `gpg --keyid-format 0xlong --check-sigs A490D0F4D311A4153E2BB7CADBB802B258ACD84F` allows you to verify the Tails public key with the Debian developer's public key by examining the output as instructed. This is so that if the source of the Tails public key (tails.net) is compromised, you have an external source of truth to alert you.
- `gpg --lsign-key A490D0F4D311A4153E2BB7CADBB802B258ACD84F` will certify the Tails public key with the key you created in the last step.

Now we know that we have a genuine version of the Tails public key. `gpg` also knows this because we chose to certify it.

Step: Verify the downloaded Tails .img file

- `TZ=UTC gpg --no-options --keyid-format long --verify tails-amd64-6.1.img.sig tails-amd64-6.1.img` allows you to verify that the .img file is signed as it should be by examining the output as instructed. Version numbers in the command will change.

Now that we know that we have a genuine version of the Tails .img file, we can proceed to install it on a USB.

Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelli-

- According to our recommendations (*rec*), this would ideally be a Qubes OS[29] system, as it is much harder to infect than a normal Linux computer.
- Use the "Terminal" installation method "Debian or Ubuntu using the command line and GnuPG"[30], as it more thoroughly verifies the integrity of the download using GPG†. If using the command line† is over your head, learn the basics of the command line with Linux Essentials[31] and see the Appendix below[32].
- Once installed, do not plug your Tails USB stick (or any LUKS† USBs used during Tails sessions) into any other computer; if the computer is infected, the infection can spread to the USB[33].

2. Running Tails on a computer with a compromised BIOS, firmware, or hardware

This second issue requires several mitigations. Let's start with a few definitions.

- *Software* is the instructions for the computer, which are written in "code".
- *Hardware* is the physical computer you are using.
- *Firmware* is the low-level software that's embedded in a piece of hardware; you can simply think of it as the glue between the hardware and higher-level software of the operating system. It can be found in several different components[34] (hard drives, USB drives, graphics processor, etc.).

[29] anarsec.guide/posts/qubes/
[30] tails.net/install/expert/index.en.html
[31] anarsec.guide/posts/linux/
[32] anarsec.guide/posts/tails-best/#appendix-gpg-explanation
[33] en.wikipedia.org/wiki/BadUSB
[34] kicksecure.com/wiki/Firmware_Security_and_Updates#Firmware_on_Personal_Computers

- *BIOS* is the specific firmware that's embedded in the "motherboard" hardware and responsible for booting your computer when you press the power button.

Our adversaries have two categories of attack vectors: physical attacks† (via physical access) and remote attacks† (via the remote access of the Internet). An adversary with physical access can compromise the software (e.g. by replacing the operating system with a malicious version), the hardware (e.g. by adding a keylogger), and the firmware (e.g. by replacing the BIOS with a malicious version). An adversary with remote access starts by hacking you (a software compromise) and can then proceed to compromise the firmware.

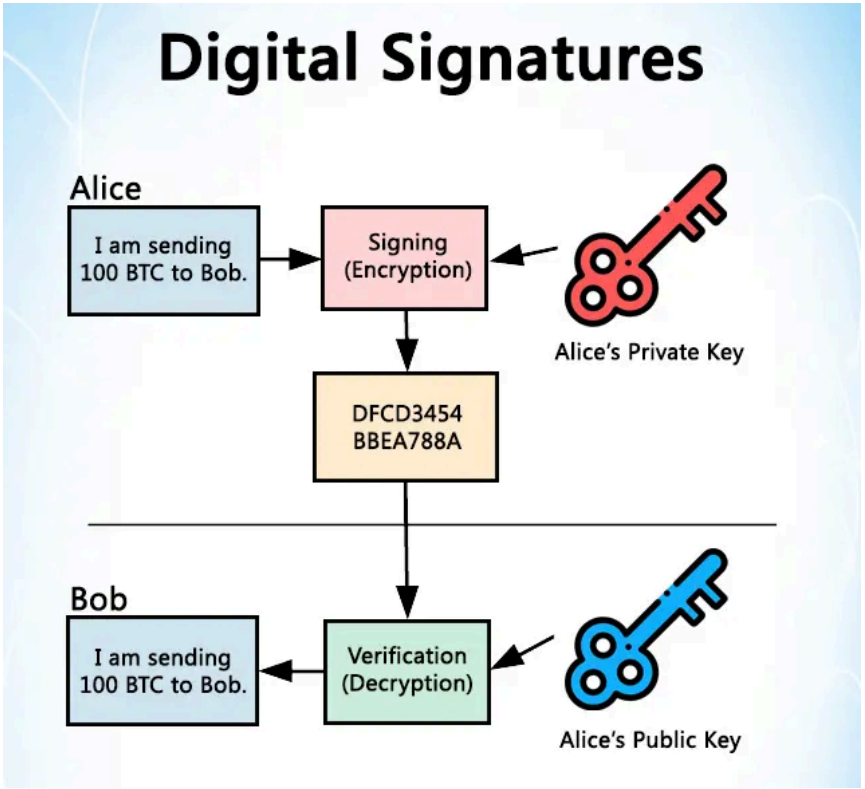
If an adversary has compromised the hardware or firmware of a laptop, this would also compromise a Tails session, given that the operating system would be running on a malicious foundation.

Not everyone will need to apply all of the advice below. For example, if you're only using Tails for anonymous web browsing and writen correspondence, some of this may be overkill. However, if you're using Tails to claim actions that are highly criminalized, a more thorough approach is likely relevant.

To mitigate against physical attacks:

- First, **get a fresh computer**. A laptop from a random refurbished computer store is unlikely to already be compromised[35]. Buy your computer with cash so it cannot be traced back to you, and in person because mail can be intercepted — a used Thinkpad is a cheap and reliable option. It is best to use Tails with a dedicated laptop, which prevents the adversary from targeting the firmware through a less secure operating system or through your normal non-anonymous activities. Another reason to have a dedicated laptop is that if something in Tails breaks, any information that leaks and exposes the lap-

[35] arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/



Tails signs their releases, and only they can do this because only they have their private key. However, I can verify that this signature is valid by having a copy of their public key. Now I'll explain the `gpg` commands in the Tails verification instructions[100].

Step: Generate a Key-Pair

Tails recommends this Riseup guide[101] to generate your own key-pair.

- `gpg --gen-key` will prompt you for some configuration options and then generate your key-pair.

[100] tails.net/install/expert/index.en.html

[101] riseup.net/en/security/message-security/openpgp/gpg-keys#using-the-linux-command-line

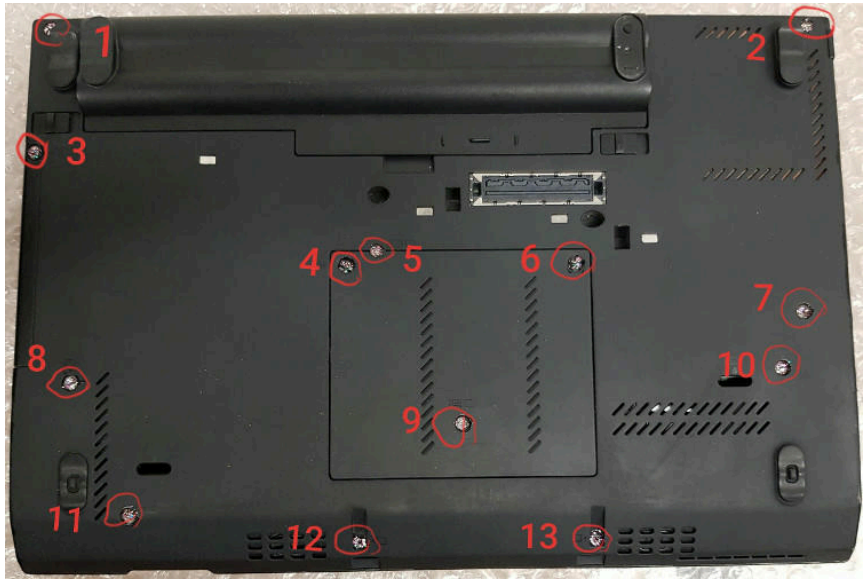
First, some clarification. PGP and GPG† are terms that can be used interchangeably; PGP (Pretty Good Privacy) is the encryption standard, and GPG (GNU Privacy Guard) is a program that implements it. PGP/GPG is also used for encrypted email communication[98]), but we use it here only to verify the integrity and authenticity of files.

GPG is a classic example of public-key cryptography†. GPG provides cryptographic functions for encrypting†, decrypting, and signing files; our concern here is digitally signing files. The Tails team digitally signs† their .img releases. GPG gives us a way to verify that the file has actually been "signed" by the developers, which allows us to trust that it hasn't been tampered with.

Now you need to understand the basics of public-key cryptography. This Computerphile video[99] has a great overview with visual aids. To summarize, a **secret/private** key is used to **sign** messages, and only the user who has that key can do so. Each **private** key has a corresponding **public** key — this is called a **key pair**. The public key is shared with everyone and is used to verify the signature. Confused? Watch the video!

[98] anarsec.guide/posts/e2ee/#pgp-email
[99] youtube.com/watch?v=GSIDS_lvRv4

top won't automatically be tied to you and your daily computer activities.



- **Make the laptop's screws tamper-evident, store it in a tamper-evident manner, and monitor for break-ins**. With these precautions in place, you'll be able to detect any future physical attacks. See the guide "Make Your Electronics Tamper-Evident"[36] to adapt your laptop's screws, use some form of intrusion detection, and store your laptop properly. Store any external devices you'll be using with the laptop in the same way (USB, external hard drive, mouse, keyboard). When physical attack vectors are mitigated, an adversary can only use remote attacks.

To mitigate against remote attacks:

- **Use Wi-Fi that is unrelated to your identity**. We recommend this not only to protect against deanonymization, but also to protect against hacking. It is best to never use the dedicated Tails laptop on

[36] anarsec.guide/posts/tamper/

your home Wi-Fi. This makes the laptop much less accessible to a remote attacker than a laptop that is regularly connected to your home Wi-Fi. An attacker targeting you needs a starting point, and your home Wi-Fi is a pretty good one.

- **Remove the hard drive** — it's easier than it sounds. If you buy the laptop, you can ask the store to do it and potentially save some money. If you search on youtube for "remove hard drive" for your specific laptop model, there will probably be an instructional video. Make sure you remove the laptop battery and unplug the power cord first. We remove the hard drive to completely eliminate the hard drive firmware, which has been known to be compromised by hackers[37]. A hard drive is part of the attack surface and it is unnecessary on a live system like Tails that runs from a USB.
- Consider **removing the Bluetooth interface, camera, and microphone** while you're at it, although this is more involved — you'll need the user manual for your laptop model. The camera can at least be "disabled" by putting a sticker over it. The microphone is often connected to the motherboard via a plug — in this case just unplug it. If this is not obvious, or if there is no connector because the cable is soldered directly to the motherboard, or if the connector is needed for other purposes, cut the microphone cable with a pair of pliers. The same method can be used to permanently disable the camera. It is also possible to use Tails on a dedicated "offline" computer by removing the network card as well. Some laptops have switches on the case that can be used to disable the wireless interfaces, but for an "offline" computer it is preferable to actually remove the network card.
- **Establish boot integrity by replacing the BIOS with Heads[38]**. Security researchers demonstrated an attack[39] on the BIOS firmware of a Tails user, allowing them to steal GPG keys and emails. Unfortunately, the BIOS cannot be removed like the hard drive. It is needed

[37] wired.com/2015/02/nsa-firmware-hacking/
[38] osresearch.net/
[39] youtube.com/watch?v=sNYsfUNegEA

all messages, rather than just a single message, which is the standard in encrypted messaging today. It is the opposite of "metadata protecting", and has several other shortcomings[93].

For synchronous† and asynchronous† messaging we recommend Cwtch[94], unless its for an anonymous public-facing project, in which case we still recommend PGP. For more information, see Encrypted Messaging For Anarchists[95].

To Conclude

Using Tails without any of this advice is still a vast improvement over many other options. Given that anarchists regularly entrust their freedom to Tails, taking these extra precautions can further strengthen your trust in this operating system.

Appendix: GPG Explanation

Most Linux users will rarely need to use the command line interface[96]. If you're using Tails, you shouldn't need it at all, although you will need the following commands for a more secure installation[97]:

- `wget`: this downloads files from the Internet using the Command Line (rather than a web browser)
- `gpg`: this handles GPG encryption† operations. This is used to verify the integrity and authenticity of the Tails download.
- `apt`: this manages packages in Debian.
- `dd`: this copies a file from one disk to another.

Using `gpg` during the installation of Tails will be less confusing if you understand how it works.

[93] anarsec.guide/posts/e2ee/#pgp-email
[94] anarsec.guide/posts/e2ee/#cwtch
[95] anarsec.guide/posts/e2ee/
[96] anarsec.guide/posts/linux/#the-command-line-interface
[97] tails.net/install/expert/index.en.html

Creating an encrypted volume

Using SiriKali to create a volume will make two new directories: a "cipher" directory where the encrypted files are actually stored (`VolumeName/` on your "personal data" USB), and a "plain" directory where you access your decrypted volume once it is mounted there (`/home/amnesia/.SiriKali/VolumeName`).

- Plug in the "personal data" USB where you will store this encrypted volume and enter its LUKS passphrase.
- Then in SiriKali, press "Create Volume" and select the option "gocryptfs."
  - You will be prompted for a password. Create a new entry in your KeepassXC file and generate a password using the Generate Password feature (the dice icon).
  - For the "Volume Path" option, select the "personal data" USB that you just unlocked.

Accessing your encrypted volume

Whenever you want to decrypt the volume, click "Mount Volume":

- This happens automatically upon volume creation.
- You can now add files to your mounted volume: right-click the volume and select "Open Folder".
  - You can verify SiriKali is working by creating a test file here. This file will show up encrypted in the cipher directory.
- When you are done, right-click the volume and select "Unmount."

Before storing important files in the volume, you should run a test to make sure it works as expected, especially if its your first time using it.

Encrypted Communication

PGP email is the most established form of encrypted communication on Tails in the anarchist space. Unfortunately, PGP does not have forward secrecy† — that is, a single secret (your private key) can decrypt

to turn on the laptop, so it must be replaced with open-source† firmware. This is an advanced process because it requires opening the computer and using special tools. Most anarchists will not be able to do this themselves, but hopefully there is a trusted person in your networks who can set it up for you. The project is called Heads because it's the other side of Tails — where Tails secures software, Heads secures firmware. It has a similar purpose to the Verified Boot[40] found in GrapheneOS, which establishes a full chain of trust from the hardware. Heads has limited compatibility[41], so keep that in mind when buying your laptop if you plan to install it — we recommend the ThinkPad X230 because it's less involved to install than other models. The CPUs of this generation are capable of effectively removing the Intel Management Engine[42] when flashing Heads, but this is not the case with later generations of CPUs on newer computers. Heads can be configured to verify the integrity and authenticity of a Tails USB — see the documentation[43], preventing it from booting if it has been tampered with. Heads protects against physical and remote classes of attacks on the BIOS firmware and the operating system software! If Heads ever detects tampering, you should immediately treat the device as untrusted. Forensic analysis[44] may be able to reveal how the compromise occured, which helps to prevent it from happening again. You can get in touch with a service like Access Now's Digital Security Helpline[45], though we recommend not sending them any personal data.
- **Use USBs with secure firmware**, such as the Kanguru FlashTrust[46], so that the USB will stop working[47] if the firmware is

[40] privacyguides.org/en/os/android-overview/#verified-boot
[41] osresearch.net/Prerequisites#supported-devices
[42] en.wikipedia.org/wiki/Intel_Management_Engine#Assertions_that_ME_is_a_backdoor
[43] osresearch.net/InstallingOS/#generic-os-installation
[44] notrace.how/threat-library/mitigations/computer-and-mobile-forensics.html
[45] accessnow.org/help
[46] kanguru.com/products/kanguru-flashtrust-secure-firmware-usb-3-0-flash-drive
[47] kanguru.com/blogs/gurublog/15235873-prevent-badusb-usb-firmware-protection-from-kanguru

compromised. Kanguru has retailers worldwide[48], allowing you to buy them in person to avoid the risk of mail interception.

- **Run Tails from a USB with a physical write-protect switch**.

Using A Write-Protect Switch

What's a *write-protect* switch? When you insert a normal USB into a computer, the computer does *read* and *write* operations with it, and a *write* operation can change the data on

[48]kanguru.com/pages/where-to-buy

Tails passphrases

For Tails, you need to memorize two passphrases:

1) The LUKS† "personal data" USB passphrase, where your KeePassXC file is stored.
2) The KeePassXC passphrase

If you are using Persistent Storage, this is another passphrase that you will have to enter on the Welcome Screen at boot time, but it can be the same as the LUKS password. Shutdown Tails whenever you are away from the computer for more than a few minutes.

Encrypted volumes

LUKS† is great, but defense-in-depth can't hurt. If the police seize your USB in a house raid, they will try a variety of tactics to bypass the authentication[88], so a second layer of defense with a different encryption implementation can be useful for highly sensitive data.

Installing SiriKali

SiriKali is an encrypted volume program that uses gocryptfs[89] behind the scenes. It is available in the Debian repository[90] and can be easily installed as additional software[91]. In Synaptic, install both sirikali and gocryptfs (if you are comfortable on the command line†, you can use gocryptfs directly and you don't actually need sirikali). If you don't want to reinstall SiriKali every session, you will need to configure Additional Software in Persistent Storage[92].

[88]notrace.how/threat-library/techniques/targeted-digital-surveillance/authentication-bypass.html
[89]nuetzlich.net/gocryptfs/
[90]packages.debian.org/bookworm/sirikali
[91]anarsec.guide/posts/tails#installing-additional-software
[92]anarsec.guide/posts/tails-best/#unlocking-the-switch

encryption password. An example of a diceware passphrase is `viewable fastness reluctant squishy seventeen shown pencil`." The Password Generator feature in KeePassXC can generate diceware passphrases and random passwords. If you prefer to generate diceware passphrases using real dice, see Privacy Guides[86].

General recommendations

- Memorize diceware passphrases of 7-10 words for everything that you'll need to enter before you have access to an unlocked KeePassXC database (in other words, your Full Disk Encryption passphrase and the KeePassXC master passphrase).
- Generate passwords of 21 random characters for everything that can be stored in a KeePassXC database. Maintain an off-site backup of your KeePassXC database(s) in case it is ever corrupted or seized.

Tip

Your memorized diceware passphrases can be easy to forget if you have several to keep track of, especially if you use any of them infrequently. To reduce the risk of forgetting a diceware passphrase permanently, you can use Tails to store all "memorized" passphrases on a LUKS USB then store it off-site where it won't be recovered during a police raid. You should be able to reconstruct the LUKS passphrase of this USB if a lot of time has passed. See the Threat Library[87] for two different approaches you can take: one relies on a trusted comrade, and the other is self-sufficient. As with all important backups, you should have at least two.

[86] privacyguides.org/en/basics/passwords-overview/#diceware-passphrases
[87] notrace.how/threat-library/mitigations/digital-best-practices.html#header-use-strong-passwords

the USB. Some special USBs developed for malware analysis have a physical switch that can lock the USB, so that data can be *read* from it, but no new data can be *written* to it.

If your Tails USB stick has a write-protect switch like the Kanguru FlashTrust[49], when the switch is locked you are protected from an attacker compromising the Tails software stored on the USB. This is critical. To compromise your Tails USB stick, an attacker would need to be able to write to it. This means that even if a Tails session is infected with malware, your Tails USB is immutable, so the compromise cannot carry over to subsequent Tails sessions ("malware persistence") by modifying operating system files. The only other way to establish "malware persistence" is firmware compromise, which you have already mitigated.

Note that Heads firmware makes a write-protect switch unnecessary because it can be configured to verify the integrity and authenticity of your Tails USB[50] before booting.

If you aren't using Heads and you are unable to obtain a USB with a write-protect switch, you have three options.

1) Install Tails on a SD card, and use a USB 3.0 to SD card adapter, because SD cards have a write-protect switch.
2) Burn Tails to a new DVD-R/DVD+R[51] (write once) for each new version of Tails — this is quite inconvenient. Don't use DVDs labeled "DVD+RW" or "DVD+RAM", which can be rewritten.
3) Boot Tails with the `toram` option, which loads Tails completely into memory. Eject the Tails USB at the beginning of your session before you do anything else (whether it is connecting to the Internet or plugging in another USB), and then use Tails like normal. How you

[49] kanguru.com/products/kanguru-flashtrust-secure-firmware-usb-3-0-flash-drive
[50] osresearch.net/InstallingOS/#generic-os-installation
[51] tails.net/install/dvd/index.en.html

use the `toram` option depends on whether your Tails USB boots with SYSLINUX or GRUB[52].

- For SYSLINUX, when the boot screen appears, press Tab, and type a space. Type `toram` and press Enter.
- For GRUB, when the boot screen appears, press `e` and use the keyboard arrows to move to the end of the line that starts with `linux`. The line is probably wrapped and displayed on multiple lines, but it is a single configuration line. Type `toram` and press F10 or Ctrl+X.

Unlocking the switch

On a USB with a write-protect switch, you will not be able to make any changes to the Tails USB when the switch is locked. If you can make changes, so can malware. There are only two cases where the switch must be unlocked:

1. For a dedicated upgrade session.

If you need to upgrade Tails, you can do so in a dedicated session with the switch unlocked — this is necessary because the upgrade needs to be written to the Tails USB. Once you are done, you should restart Tails with the switch locked.

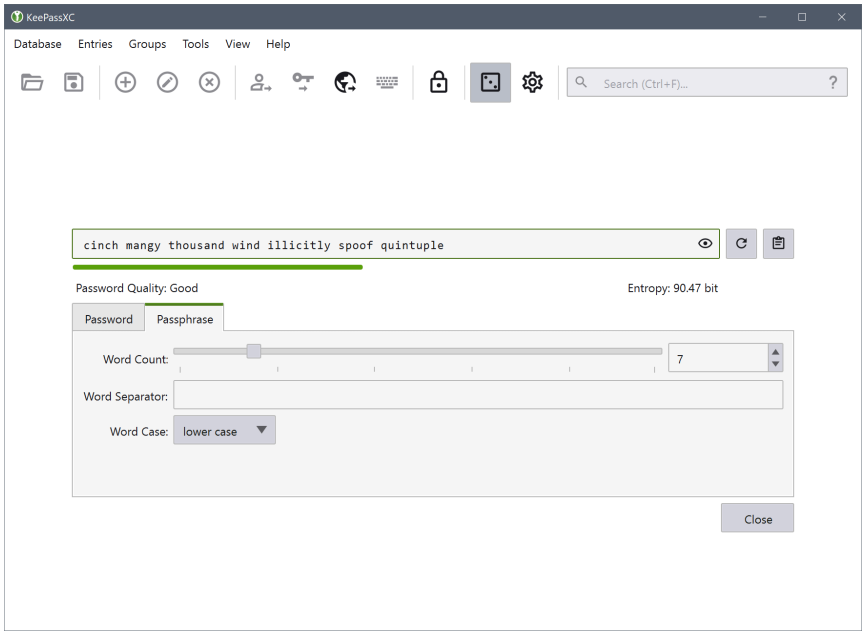
2. For a dedicated configuration session, if you decide to use Persistent Storage.

Persistent Storage[53] is a Tails feature that allows data to carry over between sessions that would otherwise be amnesiac, by saving data onto the Tails USB itself. Because Persistent Storage requires writing to the Tails USB, it is generally impractical to use with a write-protect switch. An alternative to the write-protect switch is using Heads — Heads verifies the authenticity and integrity of the Tails USB through

[52] tails.net/doc/advanced_topics/boot_options/index.en.html
[53] anarsec.guide/posts/tails/#optional-create-and-configure-persistent-storage

overview[82] or dys2p's[83].

Password strength is measured in "bits of entropy[84]". Your passwords/passphrases should ideally have an entropy of about 128 bits (diceware passphrases of **ten words**, or passwords of **21 random characters**, including uppercase, lowercase, numbers, and symbols) and shouldn't have less than 90 bits of entropy (diceware passphrases of seven words).



What is a diceware passphrase? As Privacy Guides notes[85], "Diceware passphrases are a great option when you need to memorize or manually input your credentials, such as for your password manager's master password or your device's

[82] systemli.org/en/2023/04/30/is-linux-hard-disk-encryption-hacked/
[83] dys2p.com/en/2023-05-luks-security.html
[84] en.wikipedia.org/wiki/Password_strength#Entropy_as_a_measure_of_password_strength
[85] privacyguides.org/en/basics/passwords-overview/#diceware-passphrases

This is why its important to **use Tor Browser on the Safest security setting**[78] by default, even for "trusted" websites, to greatly reduce the risk of a successful malware attack on Tor Browser.

Encryption

Passwords

Encryption† is the only thing standing in the way of our adversaries reading all our data, if it's used well. The first step in securing your encryption is to make sure that you use very strong passwords — most passwords don't need to be memorized because they are stored in a password manager called KeePassXC, so they can be completely random. Never reuse a password for multiple things ("password recycling") — KeePassXC makes it easy to store unique passwords that are dedicated to one purpose. To learn how to use KeePassXC, see Password Manager[79].

> 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.

LUKS† encryption **is only effective when the device is powered off** — when the device is powered on, the password can be retrieved from memory. Adversaries can attempt to brute-force attack† encryption with massive amounts of cloud computing[80]. The newer version of LUKS (LUKS2 using Argon2id) is less vulnerable to brute-force attacks[81] — this is the default as of Tails 6.0 and Qubes OS 4.1. If you'd like to learn more about this change, we recommend Systemli's

[78] anarsec.guide/posts/tails/#tor-browser-security-settings
[79] anarsec.guide/posts/tails/#password-manager-keepassxc
[80] blog.elcomsoft.com/2020/08/breaking-luks-encryption/
[81] mjg59.dreamwidth.org/66429.html

a digital signature upon boot, and this makes it safe to write to the Tails USB, so Persistent Storage will work as expected.

Another reason to avoid using Persistent Storage features is that many of them store personal data to the Tails USB. If your Tails session is compromised, the data you access during that session can be used to tie your activities together. If there is personal data on the Tails USB, such as an email inbox, compartmentalization of Tails sessions is no longer possible *when Persistent Storage is unlocked*. To achieve compartmentalization with Persistent Storage unlocked, you would need a dedicated Tails USB for each identity, and updating them all every month would be a lot of work.

However, you may want to use some Persistent Storage features that don't store personal data, such as the additional software feature. This requires unlocking the switch for a dedicated Persistent Storage configuration session:

- Start an "unlocked" session, create Persistent Storage[54] with additional software enabled, install the additional software[55], and select to "Install Every Time" when prompted.
- Now that the configuration is complete, restart Tails into a "locked" session before actually using the software. Don't set an Administration password, which is only required during the initial installation. In a "locked" session, none of the files you work on are saved to the Tails USB because it is "locked", but now the additional software is configured to install every time you enter your Persistent Storage password at the Welcome Screen. To have a "locked" session with Persistent Storage, the USB switch will need to be switched to the read-only position *after* you receive the notification "Additional Software installed succesfully" (and before you connect to the Internet).

The Persistent Storage feature is not possible with the DVD or `toram` boot option.

[54] anarsec.guide/posts/tails#optional-create-and-configure-persistent-storage
[55] anarsec.guide/posts/tails#installing-additional-software

"Personal data" USBs

Where can we store personal data for use between Tails sessions if the write-protect switch prevents us from using Persistent Storage? We recommend storing personal data on a second LUKS USB. This "personal data" USB should not look identical to your Tails USB to avoid confusion. To create this separate USB, see How to create an encrypted USB[56]. If you are reading this from a country like the UK where not providing encryption passwords can land you in jail, this second drive should be an HDD containing a Veracrypt Hidden Volume[57] (SSD and USB drives are not suitable for Hidden Volumes[58]).

The compartmentalization approach discussed above[59] neatly separates different identities by using separate Tails sessions for separate activities — for example, in Tails session #1 you do website moderation activities, and in Tails session #2 you do action research activities. This approach has implications for how you organize your "personal data" USBs. If the files you save could be used to link your activities together, use a different "personal data" USB for each activity.

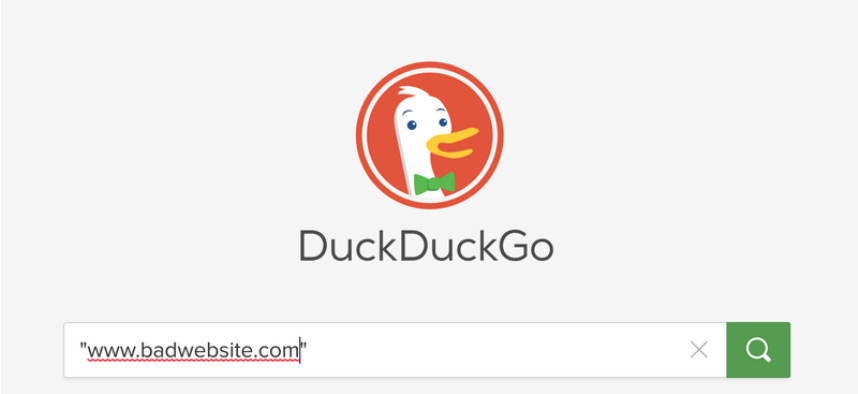
[56] anarsec.guide/posts/tails/#how-to-create-an-encrypted-usb

[57] veracrypt.fr/en/Hidden%20Volume.html

[58] veracrypt.fr/en/Trim%20Operation.html

[59] anarsec.guide/posts/tails-best/#2-using-tails-for-more-than-one-purpose-at-a-time

preserving search engine (such as DuckDuckGo) to see if it's a legitimate website. This isn't a surefire solution, but it's a good precaution to take.



- **Don't enter any identifying information into the website**. If you follow a link from an email and are asked to log in, be aware that this is a common endgame for phishing campaigns. Instead, manually go to the website of the service you are trying to access and sign in there. That way, you'll know you're logging in to the right website because you've typed in the address yourself, rather than having to trust the link in the email.

Watering hole attacks

An adversary can also compromise a "trusted" website — this allows them to install malware on the computers of anyone who visits the website, without needing to engage in phishing. This is called a "watering hole attack" or a "drive-by compromise"[76] because it attacks many people simultaneously. For example, the FBI hacked a website then used a Tor Browser exploit[77] to hack 8,000 users who visited it.

[76] attack.mitre.org/techniques/T1189/

[77] vice.com/en/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant

in a dedicated 'offline mode'[72] Tails session. This will prevent code execution from establishing a remote connection to the adversary, which is usually needed to further the attack. Shutting the session down immediately afterward will minimize the chance of malware persisting. However, unless you use Dangerzone to sanitize the files, they will remain untrusted.

Links

With untrusted links, there are two things you must protect: your anonymity and your information.

- **It is best to open untrusted links in a dedicated Tails session without unlocked Persistent Storage or attached "personal data" USBs.** You can put the link on a Riseup Pad to access it.
- **Use Tor Browser on the Safest security setting[73]!** The vast majority of exploits against Tor Browser will not work with the Safest setting.
- **Manually copy and paste the address into your browser, and retype the domain**. For example, after pasting the link `anarsec.guide/posts/tails`, retype `anarsec.guide` yourself. Do not click through a hyperlink (i.e. always copy and paste) because it can be used to mislead you about where you are going. Retyping the domain protects against "typo-squatting" (mailriseup.net instead of mail.riseup.net) as well as "homograph attacks"[74] (where Cyrillic letters are substituted for normal letters).
- **Never follow a shortened link** (e.g. a site like bit.ly that takes long web addresses and makes a short one) because it cannot be verified before redirection. Unshorten.me[75] can reveal shortened links.
- **If you don't recognize the domain, research it**. Search for the domain with the domain name in quotation marks using a privacy-

[72] tails.net/doc/first_steps/welcome_screen/index.en.html#index3h2
[73] anarsec.guide/posts/tails/#tor-browser-security-settings
[74] theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers
[75] unshorten.me/

If a "personal data" USB is used to save very sensitive files (such as the text of a communique), it is best to overwrite and then destroy the USB once you no longer need the files (see Really delete data from a USB drive[60]). This is another reason to use a separate USB for any files that need to be saved — you don't accumulate the forensic history of all your files on your Tails Persistent Storage, and you can easily destroy these "personal data" USBs as needed.

If you already use Tails and encrypted email, you may be familiar with Thunderbird's Persistent Storage feature for your inbox and PGP keys. This feature won't work with a write-protect switch enabled. Instead of using Persistent Storage for email, simply login to Thunderbird with IMAP in each new session. PGP keys can be stored on the "personal data" USB like any other file, and imported when needed with Thunderbird's "OpenPGP Key Manager" (File → Import Public Key(s) from File / Import Secret Key(s) from File). This approach has the advantage that if law enforcement manages to bypass LUKS, they still don't have your inbox without knowing your email password.

[60] anarsec.guide/posts/tails/#really-delete-data-from-a-usb

Phishing Awareness

Let's return to the subject of how an adversary would conduct a remote attack† targeting you or your project for hacking; the answer is most likely "phishing"†. *Phishing* is when an adversary crafts an email (or a message in an application) to trick you into revealing information or to introduce malware onto your machine. *Spear phishing*† is when the adversary has done some reconnaissance and uses information they already know about you to tailor their phishing attack.

Phishing only works if the adversary has a way of sending you a message: you don't need to worry about this attack vector for activities like submitting a communique or doing action research, but it is relevant for public-facing projects that have a communication channel. Be aware that the "from" field in emails can be spoofed to fool you — PGP signing[61] mitigates this to prove that the email is actually from who you expect it to be from.

You have probably heard the advice to be skeptical about clicking on links and opening file attachments — this is why. Phishing relies on your actions to succeed, so your awareness is your best defense.

A malicious file or link works by executing code[62] on your machine. For malicious files, the code executes when the file is opened. For malicious links, the code executes when you visit the website, usually with the help of JavaScript. The point of this code execution is to give an entry point ("inital access") to infect your machine with malware.

Tails protects against malware deanonymizing you by forcing all internet connections through the Tor network. However, once the adversary has "initial access" they will try to further their attack;

- to make the infection persistent[63],
- to install a screen or key logger[64],

[61] anarsec.guide/posts/e2ee/#pgp-email
[62] en.wikipedia.org/wiki/Arbitrary_code_execution
[63] attack.mitre.org/tactics/TA0003/

- to exfiltrate your data[65],
- to achieve "privilege escalation"[66]

Privilege escalation (i.e. going from an unprivileged user to the administration user on the system) is usually necessary to bypass Tor. Tails does not have a default Administration password (it must be set on the session's Welcome Screen if needed) in order to make "privilege escalation" more difficult.

The most recent Tails audit[67] found several "privilege escalation vulnerabilities," and even a vulnerability that leaked the IP address from the non-privileged user. If resilience to malware attacks is an important part of your threat model, see When to Use Tails vs. Qubes OS[68].

Files

In 2017, the FBI and Facebook worked together to develop a malicious video file that deanonymized a Tails user[69] after he opened it while using his home Wi-Fi.

For untrusted attachments, you would ideally use Dangerzone[70] to **sanitize all files sent to you before opening them**. Dangerzone takes untrusted PDFs, office documents, or images and turns them into trusted PDFs. See the documentation[71] for how to install Dangerzone on Tails — unfortunately, it currently requires using the command line†.

If you are not using Dangerzone, **it is best to open untrusted files**

[64] attack.mitre.org/tactics/TA0009/
[65] attack.mitre.org/tactics/TA0010/
[66] en.wikipedia.org/wiki/Privilege_escalation
[67] tails.net/news/audit_by_ROS/index.en.html
[68] anarsec.guide/posts/qubes#when-to-use-tails-vs-qubes-os
[69] vice.com/en/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez
[70] dangerzone.rocks/
[71] tails.net/doc/persistent_storage/additional_software/dangerzone/index.en.html