# How to submit an anonymous communique

and get away with it

**MARCH 2024**

A communiqué, also sometimes called a reportback or hit report, is a report on (typically) illegal direct actions that is shared online via counter-info sites or in print publications. Mainstream media may suppress reporting about certain tactics or the reason for choosing a target may be unclear, so submitting a communiqué is a way to share news, tactics, and political motivations directly.

This guide describes how to securely submit an anonymous communiqué online. It is written for anarchists, but could be useful to other audiences like journalists or dissident groups sharing information while concealing their identities. While some communiqués are signed by a group or individual claiming responsibility, this guide focuses on anonymity.

Nothing you do on computers or the internet is ever totally safe, but you can reduce most technology-based risk by following some simple steps. There are many methods beyond those shared here, but this is a set of instructions that will hopefully help you.

## Key Terms

**Communiqué**: A report on (typically) illegal direct actions that is shared online via counter-info sites or in print publications.

**Threat model**: An analysis of risks that could compromise security, how likely they are to happen, and how they may be mitigated.

**Tor**: Short for "the onion router." Tor is a strong anonymity system that routes your internet traffic through a series of random volunteer-run nodes across the planet. Learn more and download Tor Browser at torproject.org.

**Browser**: The application that allows you to access the internet. In addition to Tor Browser, other common examples include Firefox, Edge, Brave, and Chrome.

**Operating system**: Software programs that tell the hardware in a computer how to function. Common examples include Windows, Mac, Linux, and Tails.

**Tails**: An operating system that runs off a flash drive and leaves very few digital forensic traces on your computer. Tails also provides strong anonymity to your browsing traffic by routing all of it through Tor. Learn more and install at tails.net.

**Stylometric analysis (stylometry)**: A forensics technique that analyzes word choice and style to identify authors and guess about their characteristics, for example regional dialect, education level, and unique word choice/phrases/typos.

**Metadata**: Data about data. For digital media, this is data contained within a photo or video file like camera type and date and time of capture. It can also refer to data about your typical patterns of internet use or date and time an account is created.

**Disposable email**: An anonymous email account that is temporary or single-use, typically with no login or account information. Also sometimes marketed as "spam email" sites.

**Encryption**: A method of hiding content in a message so it is only visible to your intended recipient.

# The Guide

## 1. Obtain a Tails stick and identify a computer to use

Make or borrow a Tails stick, a USB drive that contains files to run the amnesiac operating system Tails. Install from tails.net or ask a tech-savvy friend to help you with the process. When making your Tails stick, use Tor Browser and space it out from when you send the actual communiqué so as to not leave as strong of a correlation. Making your own Tails stick is recommended over borrowing one since that keeps your digital habits or plans more private and makes it harder to compromise multiple people's security through one contaminated device.

The general recommendation for most people is to use a personal computer that is only for Tails, on public WiFi. The risks of using Tails on

a personal computer that you also use for other tasks are fairly low, but not zero. Avoid sitting where your screen or keyboard would be visible to any surveillance cameras. (If you are fast enough at it, single stall public restrooms or restrooms with tightly closing stalls can be great for this.)

Depending on your threat model, different computer and network options could be better suited to your security needs. Using public WiFi or a public computer (for example in a library or cybercafé) could reveal information about your movements, especially if you are already under physical surveillance. Public computers themselves could be compromised at the hardware level or through intentional collaboration between their owner-operators and law enforcement, and this could be almost impossible to detect. Using a device in your home, on your home WiFi, could leave you more vulnerable to threats like hidden cameras or sophisticated Tor correlation attacks. And, of course, if the place where you store your computer is insecure, the device could be compromised by hardware tampering (like a keylogger) or malicious software (less likely to matter when using Tails). For more information on threat modeling for your specific situation and learning about ways these attacks have been used against other activists, visit the No Trace Project (notrace.how) or AnarSec (anarsec.guide).

## 2. Boot into Tails OS

Plug the Tails stick into the computer while it is off. Turn on the computer and hold down specific keys to access the boot menu. Refer to the included table (taken from tails.net, which also has more detailed instructions) to see which keys are relevant for your device. If you must search for this information online, use Tor Browser and try to space that search out significantly from when you intend to submit your communiqué.

On startup, you will probably see phrases like "Press [key] to access boot menu" or "Press [key] to access BIOS options" Some computers tell you to "Press [key] to interrupt normal startup" which brings you to the boot

menu. From there, select your USB drive from the list and your computer will boot into Tails.

At the Tails welcome menu, when given the option to unlock Persistent Storage (if you have it set up), do not. Anything saved to Persistent Storage will be impossible to truly delete, short of reformatting and destroying your Tails stick. If you must save data between Tails sessions, use a second encrypted USB that you can destroy afterwards. To learn how to create an encrypted USB on Tails, read "Tails for Anarchists" on anarsec.guide.

Tails comes with many helpful programs pre-installed, including Tor Browser (to access the internet), Metadata Cleaner (to remove metadata from files including photos & videos), GIMP (for photo editing), the LibreOffice Suite (open-source versions of Microsoft Word/PowerPoint/Excel), and more.

| Manufacturer | Key |
|---|---|
| Acer | F12, F9, F2, Esc |
| Apple | Option |
| Asus | Esc |
| Clevo | F7 |
| Dell | F12 |
| Fujitsu | F12, Esc |
| HP | F9 |
| Huawei | F12 |
| Intel | F10 |
| Lenovo | F12, Novo |
| MSI | F11 |
| Samsung | Esc, F12, F2 |
| Sony | F11, Esc, F10 |
| Toshiba | F12 |
| Others... | F12, Esc |

## 3. Open Tor Browser and find submission sites

Connect to the internet and use Tor Browser to identify counter-info sites that may be interested in your communiqué. Here are some relevant sites, sorted by region:

**North America:**

- unravel.noblogs.org
- scenes.noblogs.org

- animalliberationpressoffice.com
- unsalted.noblogs.org (Michigan/Midwest US)
- phlanticap.noblogs.org (Philadelphia)
- rosecitycounterinfo.noblogs.org (Portland)
- indybay.org (California)
- mtlcounterinfo.org (Montreal)

**Europe:**

- Germany: de.indymedia.org; chronik.blackblogs.org
- Italy: ilrovescio.info; lanemesi.noblogs.org
- France: attaque.noblogs.org; sansnom.noblogs.org

**Central & South America:**

- informativoanarquista.noblogs.org

**International:**

- unoffensiveanimal.is
- actforfree.noblogs.org
- anarquia.info
- abolitionmedia.noblogs.org

These sites usually have a "contact" or "submissions" page which tell you how to send information you want published. This can be an email address or a form built into the website. Some offer both options (see steps 5-7).

## 4. Write your communiqué*

*If your action has already been reported in the mainstream media, consider whether publishing a communiqué is worth the risk. Ask yourself: Does it include specific helpful information that will encourage other people to act? Will your intended audience see the already existing reporting? Does the target of the action understand why it happened, if

that is important? Sometimes it may be better to submit a mainstream news article to counter-info sites, instead of writing an original communiqué.

If you decide that writing your own submission is worthwhile, type your communiqué in a text editing program like LibreOffice Writer or Text Editor, NOT in the browser. The timing of keystrokes is very unique, especially for large blocks of text, and tracked by default on many web services. Do not save the document.

Only include information the police already know. Don't add details like how many of you were involved, your background or identities, where you got supplies, entry or escape routes, or a long and stylistically unique personal political diatribe. These could unintentionally help an investigation against you.

To avoid stylometric analysis identifying you or grouping multiple of your submissions together, keep it short—less than 300 words if you can. If you're writing with a friend, edit collaboratively to disguise your style. LibreOffice Writer can check for typos and punctuation errors, but will usually try to enforce formal linguistic rules. Unusual or specific dialect choices could help investigators link a communiqué to other writing. Making all letters the same case (upper or lowercase) disguises some style choices, but can be notable as a style choice itself. Some people recommend running text through Google translate or similar software to further disguise specific word choices and phrasing. This can be especially effective when translating between several languages with less online prevalence and/or different translation engines between languages. An English translation of the text "Who wrote that?" from Zündlumpen #76 on the No Trace Project website (notrace.how) deals with this topic extensively.

## 5. Compress then remove metadata from photos and videos

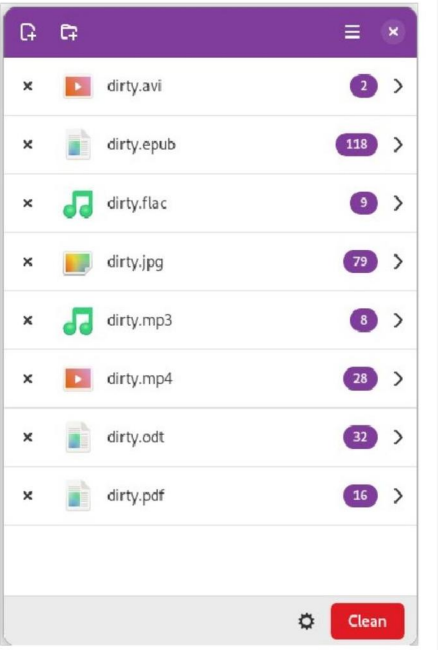
First, seriously consider if posting visual media of your clandestine action, especially videos, is worth it. Such media can give investigators a lot of

information they might not have already have. Read up on open source intelligence techniques and video analysis. Details like faces, skin, tattoos, scars, height, gait, or unique clothing or accessories could lead to identification. For videos, things as simple as the hum of the electrical wires in your walls, road noise, or a single leaf can give very damaging information to the police, or any bored person with a laptop and an internet connection (yes really, *any*). And of course, the sound of your voice or car engine could be damning. Best practice is to use a burner camera (obtained for this purpose only, then discarded) to avoid photos or videos from different actions being linked together based on sensor noise.

If you decide submitting photos or videos is worth the risk, compress them to remove extra details by reducing the number of pixels. Lower resolution media can support your overall message without accidentally providing evidence like detailed reflections or tread marks. As a bonus, this reduces the file size which will make it easier to upload and share. For images, open them in GIMP then go to File > Export As. Click “Select File Type” and choose “JPEG” from the list. Use the “Quality” slider to reduce image quality, using the preview to check that it isn’t degraded too much.


Compressing videos is more complicated; look at the Tails OS documentation on sound and video for suggested programs and how to install them. There are websites that compress videos for you, but the most secure option is always something offline. If you upload a high-quality version to any website, that website could retain a copy and/or provide information to law enforcement. If you are in doubt about the potential evidence contained in your video, or are unsure how to remove potentially-identifying information, it might be best to leave it out of your submission entirely.

Once your files are compressed, the final step is to remove metadata, digital information that isn't visible in the media but can be viewed in the file properties. Open Metadata Cleaner, click the "Add files" icon in the top left, and select your files. Click "Clean" in the bottom right to remove metadata and overwrite the originals.




## 6. Open the site submission form (if applicable)

As mentioned in step 3, some counter-info sites have built-in submission forms. These are often an easy and secure option to submit a communiqué, especially if you are sending only text. Each site is slightly different, so check the "submissions" or "contact" page for the exact sites where you want to send your communiqué.

Some sites accept media files through their online form, while others suggest specific filesharing sites. If files cannot be uploaded directly, one option is to upload them to file.espiv.net so you can paste a URL into a text box instead of attaching a media file directly to your submission. Note that some counter-info sites may not accept files submitted this way, as it poses a risk to site administrators. Check the relevant submission guidelines and use their suggested file sharing site(s) if available.

Paste your communiqué into the text field, enter fake non-identifying information in any other fields, upload cleaned media files or paste the filesharing URL if applicable, and submit! If that all works, skip to step 9.

If the site you want to submit to just has an email address or you experience technical difficulties using their submission form (including the communiqué not being received, which you might not notice until days

later if it hasn't been posted yet), it may be better to send your communiqué via email, as detailed in steps 7-8.

## 7. Create a Protonmail account, or other disposable email

If you are not using an in-site submission form, you can send an email from an account created just for this purpose. One option is Protonmail (proton.me)—many submission sites also use Protonmail, making your email end-to-end encrypted by default. Note that this encryption is not as strong as something like PGP through a trusted email provider and Protonmail as a company is not your ally (they previously collaborated with cops and lied about it). However, the contents of your message are intended to be posted publicly. The intent here is not to keep the contents of your message absolutely secret, but to minimize any metadata or personal identifying information you could accidentally send with your message. NEVER send identifying information in connection with a communiqué.

For the username, pick 2-3 random words. The website randomwordgenerator.com can help with randomness. Use a different set of random words for the password (ideally 6+ for good password security). Do not save this login information anywhere.

When using Tor, Protonmail will ask for a secondary method of verification. Enter a disposable email address created on guerrillamail.com, yopmail.com, tempr.email, or a similar disposable email site so you can receive the confirmation code.

If you do not want to use Protonmail, you could try sending your communiqué from a disposable email site. However, many of these sites only receive emails and the ones that let you send an email (tempr.email) are sometimes less reliable, especially with media attachments.

Consider trying multiple methods, or varying methods between communiqués, in order to avoid creating metadata about your submission process.

## 8. Create and send the submission email

Paste your communiqué into the body of the email. If sending your email between two Protonmail accounts (or another service that advertises end-to-end encryption between accounts they provide), the content of your email will be encrypted. The subject line, however, is never encrypted—for the safety of you and your recipient put something vague in that field or leave it blank.

Photos can usually be attached directly to the email. Videos or other large files can be uploaded to Proton Drive (same account as the email) or file.espiv.net and sent as a link. Note that some counter-info sites may not accept files submitted this way, as it poses a risk to site administrators. Check the relevant submission guidelines and use their suggested file sharing site(s) if available.

Read over everything one last time to make sure there are no mistakes and you attached everything you wanted. Then send the email!

## 9. Close out, clean up

Close any open programs, do not save any login info, and do not use the email account (if you made one) for anything else. Shut down the computer and remove your Tails stick. It can be safely used again, with no connection to the prior session, on the same computer or a different one.

If relevant, delete any photos or videos then destroy and dispose of any camera or SD card used in the action. Breaking a device into small pieces is best (the NSA recommends pieces <2 mm), which can be achieved in a good quality household blender. Other options include using a hammer, plumbing torch, or strong acid. Avoid inhaling fumes from burning, melting, or other chemical reactions with metals or plastics.

Consider disposing of this zine if you're using a hard copy, by destroying it or gifting to a trusted friend. It doesn't prove you've done any crimes, but wouldn't look great in court as potential corroborating evidence.

**That's it! This might seem like a lot of steps at first, but it's not that hard and gets easier every time you do it.**

**Stay safe, be dangerous, don't get caught.**

## Relevant Websites

**tails.net**

**torproject.org**

**notrace.how**

**anarsec.guide**

**file.espiv.net**

**randomwordgenerator.com**

**proton.me**

**guerrillamail.com**

**yopmail.com**

**tempr.email**