The Briarthorn OpSec Guide

Anonymous

12/01/2025

Contents

Introduction

There's a lot of work that goes into figuring out how not to get arrested, and how to minimise the damage if you are. To try to make it easier for our comrades, we want to share the techniques we've developed while operating an illegal activist organisation. This is a guide for non-experts, but for some procedures it will help to be moderately techy or at least be working with some techy friends.

Caveats

DON'T TRUST US TOO MUCH. We've put a lot of thought into this and we haven't been caught yet, but it's always possible we've just been getting lucky. Where possible, do your own research and think it through for yourself. These procedures are starting points to develop from, provided because they're a better place to start from than the usual insecure ways of doing things. We've tried to make it harder to blindly trust us by explicitly noting when there's something we don't know.

THIS INFORMATION WILL GO OUT OF DATE. We're writing this in 2025. The longer after that you're reading this, the more likely some details are no longer true.

ASSUMPTIONS ABOUT WHAT THE POLICE CAN OR WILL DO ARE RELEVANT TO THE UNITED KINGDOM (UK), because that's where we work.

And perhaps most importantly, DON'T LET WORRYING ABOUT SECURITY STOP YOU FROM GETTING SHIT DONE! If you get paranoid and don't do something because it's too difficult to do perfectly safely, the surveillance state wins. Do things safely enough for the level of risk they carry, and always take *easy* opportunities to make things safer, but if you spend days setting things up perfectly safely just to do some graffiti or something then they've won by virtue of stopping whatever other thing you could have done with all that effort.

General Principles

There are two fundamental principles to bear in mind across all of this.

Threat Modeling

In order to know what to do to keep yourself safe, you need to know what the realistically likely dangers are. A threat model is an idea of who's trying to stop you and what they can do, and if you're doing operational security then you need to have one. The procedures in this document are written on the assumption that you're mainly up against the UK police, and they're not willing to invest more resources into stopping you than they are any random low-to-mid-level illegal activist group (i.e. you're not doing any terrorism or anything). It also assumes that you're not doing anything very public, that most of your operations will never be reported to the police. If you're doing headline-grabbing propaganda stuff then you may face a different threat profile, for instance you don't have to keep the existence of the group secret but you might have to worry more about infiltrators. The reason we've chosen this threat model is that it's the situation we have experience with, and also that we feel more groups could do with focusing on changing the world directly ourselves rather than trying to convince the government to do it for us.

Defense In Depth

There will always be things you overlook, and things you couldn't have known. When your defenses inevitably fail, you should have other defenses in place so that it's not a total disaster. This means that even if you trust someone completely, you still don't tell them incriminating things they don't need to know. Even if your encrypted drive is secure, you still delete things off it when you don't need them anymore. Even if you're using an encrypted messaging app, you still use pseudonyms. When you fuck something up, it shouldn't be the end of the world.

Procedures

This section is the bulk of the guide. It contains a set of procedures for doing various things more securely. Often they refer to each other, e.g. part of the procedure for securely buying things from the internet is to apply the procedure for securely using the web. Each procedure has three increasingly secure versions: Acceptable, Good and Paranoid. More secure versions include doing all the things mentioned in the less secure versions as well unless otherwise specified. We've made this division so that people won't get bogged down worrying about security that's way over the top for what they're doing. As a rough guide, we feel that for crimes that don't necessarily invite police attention every time as described in the introduction, the Acceptable level is appropriate for when we're risking up to maybe six months, Good for up to a couple of years, Paranoid for up to maybe five or six years. But that's just our personal comfort levels at this particular stage in our lives, so don't take that as gospel. For crimes that do invite police attention, we'd probably move everything down one category — no custodial sentence, six months, a couple of years.

Going Somewhere

Acceptable

Wear a mask and nondescript clothing.

Good

Leave your phone behind — the phone company knows its location at all times and keeps records for years. Pay for public transport in cash if possible. Be aware of CCTV, especially cameras that may be government-operated rather than belonging to private businesses since the police can access them more easily.

Paranoid

Don't bring anything with your name on it. Possibly arrange for a comrade to alibi you if necessary.[1]

[1] No Trace Project (N.T.P.) note: For this level, you may also want to take precautions to ensure you are not being followed. For more information, see our Threat Library mitigations "Surveillance detection" and "Anti-surveillance".

Using The Web

Acceptable

Use Tor Browser. If you're not familiar with it, Tor Browser is a web browser that routes your connection through a series of other computers before it reaches the website you're connecting to. This means the website doesn't know who you are because your connection appears to come from somewhere else, unless of course you tell it who you are yourself (e.g. by signing into an account in your own name). It's easy to install and use on pretty much any computer, including smartphones. See torproject.org.

Good

Use Tails. If you're not familiar with it, Tails is a piece of software you put on a USB stick or SD card (see the procedure for storing digital information) that lets you boot the computer you plug it into using a secure operating system. Tails ensures all internet traffic goes through Tor, and leaves no trace on the computer of what you were doing. See tails.net.

Paranoid

Use Tails from a public wifi network, such as in a coffee shop. This will probably involve applying the procedure for going somewhere, unless you live across the road from a coffee shop or something and can connect to the wifi from your house. Be aware of CCTV, but most businesses don't store CCTV records for too long. If you get a coffee, pay in cash. Don't make a habit of using the same place every time.

Messaging Someone On The Internet

Acceptable

Use Signal. If you're not familiar with it, Signal is an encrypted messaging app. It requires a phone number to sign up, but can be used on a computer as long as the account is tied to a phone. Apply the procedure for storing digital information to any device that you install Signal on. If you think you might be arrested, uninstall Signal. When you reinstall it you will have lost all your messages, this is an unavoidable consequence of the security features that prevent the police from recovering your Signal messages from a device you've uninstalled it from. Note that the way that your Signal messages with someone are most likely to be leaked is if the police get hold of your or that person's inadequately-secured device and simply unlock it and read the messages the same way the intended recipient would. However, if that happens they won't necessarily know who the other person in the conversation is (unless you revealed who you are in one of the messages they read). See signal.org.

Other encryted messaging platforms exist, but Signal is very popular, so firstly it's less suspicious to be using it and secondly it's been extensively tested in practice. If Signal isn't an option, we like the look of Matrix or SimpleX, but we don't have experience with them.[2]

[2] N.T.P. note: We would recommend SimpleX rather than Matrix, as Matrix does not protect communication metadata as well as SimpleX does. Compared to Signal, SimpleX does not require a phone number to create an account. For more information, see AnarSec's guide "Encrypted Messaging for Anarchists".

Good

Use separate Signal accounts for different purposes, so if one of them is identified as you the others may not be. You need a separate phone number for each account, so you'll need to get a SIM card, they're sold in many supermarkets (apply the procedure for buying something in person, or just apply the procedure for going somewhere and steal one). You don't have to activate the SIM card in order to receive the verification text, so don't — that will connect your bank account to it. You'll need to keep hold of the SIM card in case you lose access to your account (e.g. by having to uninstall Signal), but you should keep it hidden because if the police search your house and find it they may be able to discover and maybe even impersonate the account it's associated with. Alternatively, if you set a Signal PIN (see below) you may be able to use that to recover your account without the SIM.

Configure Signal settings to be more secure — set "who can see my number" and "who can find me by number" to nobody, set a default disappearing messages timer, turn off link previews, read receipts and typing indicators, turn on call relaying, turn on screen lock, set a Signal PIN (use a secure alphanumeric PIN) and enable registration lock.

Consider using Molly (molly.im). Molly is an alternative frontend for Signal. It makes it harder for someone who has your phone to get into your account, but it isn't widely-used enough to be quite sure it's well-made and safe.

Paranoid

Instead of using a phone, have your sensitive Signal accounts on Tails using signal-cli. We won't go into detail about signal-cli because if you're technical enough to use it you'll be able to figure it out yourself. You can connect signal-desktop to the account for ease of use. Don't put the SIM in your own phone, use a burner phone (acquired with the procedures for buying something, either online or in person). Never turn the burner on at home or in a location connected to you, or in the presence of your or your comrades' phones, as the phone company will know where it is and what other phones are nearby and store that information. Once you've registered your account, get rid of the burner. Apply the procedure for storing an object for the burner and SIM. They should be stored together, as getting access to either one will reveal all the information that could be acquired from either, unless you decide to just dispose of the phone and get a new one if you need it.

Eventually, the phone company deactivates unregistered or registered but unused SIMs and allows a new one to be made with the same number. When this happens you'll no longer be able to recover your account using the SIM, and it's possible that the person who buys the new SIM will use it to register for Signal, kicking you out of your account (note that they won't gain access to your account, it'll just be lost). In order to prevent this, note when your SIM will expire and move your account to a new number before it happens. If you're getting reasonably newly made SIMs this shouldn't be more than every couple of years. You'll need to do this even if you haven't kept the SIM card and you're just using the PIN to get back in if you lose access.

Using Cryptocurrency

A detailed guide to the non-security aspects of using cryptocurrency is out of scope for this document, so this procedure is written assuming you know how to use cryptocurrency.

Acceptable

Apply the procedure for using the web, and use monero. Monero is a privacy-focused cryptocurrency, which is important, because contrary to popular belief most cryptocurrencies are extremely traceable. For regulatory reasons it's difficult to buy monero in the UK, but you can buy other currencies and easily exchange them. Apply the procedure for storing digital information to your wallet. You can buy cryptocurrency from an onramp service or an exchange.

If the thing you want to buy can't be bought with cryptocurrencies, you can buy virtual prepaid debit cards using monero on sites like coinsbee.com (not forgetting to still apply the procedure for using the web) and use those to pay for it.

Since storing information securely leads to an increased risk of losing it, you may want to keep a record of your wallet seed. This should be stored securely itself, either as digital information or written down. Someone who gets access to it gets full access to the wallet.

Good

Make sure you're using a local wallet rather than an exchange (but it's unlikely you can get monero on an exchange these days anyway). Access the monero network over Tor, the feather wallet has a facility for this built in (featherwallet.org). Make sure to transfer your monero between two wallets you control, so that more than one transaction has to be compromised to trace what you're spending it on. If you're buying cryptocurrency, consider buying it from a peer-to-peer exchange so it's harder to tie to your bank account.

When storing the seed, consider writing the seed words out of order, as long as you'll be able to remember how to put them back in order.

Paranoid

When moving money through any kind of series of accounts, always put more in than you take out at the far end, so someone watching both ends can't guess that it's the same money because it's the same amount. Likewise don't do it all at once, leave delays between transfers.

If you're keeping the seed words written out of order, recover the wallet corresponding to the order they're written in and make some small, non-incriminating transaction with it, so if the seed is found you can make a plausible case that this is the real wallet.

Buying Something In Person

Acceptable

Apply the procedure for going somewhere. Pay in cash.

The Good and Paranoid versions of this procedure are just the same using the Good and Paranoid versions of the procedure for going somewhere.

Buying Something On The Internet

Acceptable

If it's something that's not illegal in itself, have someone who's not doing anything else illegal order it and pick it up from them. You can reimburse them in cash. Don't forget to remove the

label with their address on it from the box if you're keeping it, so if your house is searched the police won't find out about this person from the label.

Good

Apply the procedure for using the web and order it using the procedure for using cryptocurrency, either still to someone else's address or poste restante[3] in a name that you have a good fake ID for (if you can't give a valid ID the post office may refuse to give you the parcel).

There isn't a Paranoid level for this, because we don't have the experience with ordering anything that warrants that level of security to be able to speak authoritatively on it. Anything we could say would be speculative.

Laundering Money

Acceptable

Buy things with the money and sell them. Buy and/or sell things in a similar way with your own money to obscure it. This process is okay at a glance but won't stand up to actual investigation, and isn't practical for large quantities of money.

Good

Using the procedure for accessing the web, buy monero with the money (see the procedure for using cryptocurrency). At this point the money should be disconnected from its source. Use the monero to buy prepaid virtual debit cards as mentioned in the procedure for using cryptocurrency. Note that although the source of the money is obscured, the fact that it came in the form of monero isn't, so it may still look suspicious.

Paranoid

Buy monero with the money and move it between two accounts. At this point the money should be disconnected from its source. Trade the monero for cash sent to you by mail on a peer-to-peer exchange such as retoswap (retoswap.com) (using the advice in the procedure for buying something on the internet for receiving it by post securely).

Sending Post

Acceptable

Apply the procedure for going somewhere. Buy postage in cash. Alternate between various post offices. Follow the post office rules (e.g. on the proper way to post liquids) as far as possible to reduce the chances of your packages being opened.

[3] N.T.P. note: Poste restante is a service where the post office holds mail until the recipient calls for it.

Good

Buy stamps and envelopes in cash, and post at postboxes. Alternate between various postboxes. If you need to send large items, use parcel postboxes, but if you're not in a city there might not be many to alternate between. Don't post lots of things all at once in one postbox, as this might raise suspicions and get them opened. With stamps, be aware that the barcodes on them can't be used to trace where they were bought, but they are scanned by the sorting office so they can be used to trace at least to the sorting office of the place where something was posted from (and that's one of their purposes).

Paranoid

For occasional posting, use commemorative stamps, as they don't have the barcodes on them (but posting lots of parcels with commemorative stamps in one place would be suspicious). Buy envelopes from different places so which brands of envelope you use can't be used to identify where you're going to buy them (or more likely as circumstantial evidence after the fact based on the fact you frequently went somewhere that sold those envelopes). Pick postboxes in locations such that your house isn't in the centre of all the locations you use.

Storing An Object

Acceptable

If your address is unlikely to be a target of investigation, just keep it in your house. If you or your housemates are at risk of arrest, or if the address is used to order things to, hide it. Small things like SD cards and SIMs are easy to hide very well, so don't just stick them behind a picture frame and call it a day, unscrew the back of something that isn't ever opened up under normal circumstances or something.

Good

Even if your house isn't likely to be searched, hide it anyway. If it doesn't need to be regularly accessed, keep it at the house of someone who isn't doing anything dodgy.

Don't be tempted to hide things in public places, since a search warrant then isn't needed to get at them.[4] Storage units are probably a bad idea too, since they'll be connected to whoever pays for them.

Paranoid

If the item is replaceable, and it's cheap and/or rarely used, consider not storing it at all and getting a new one whenever you need it. If the item can be split into parts that aren't (as) incriminating on their own, store it across several people's houses. We know of no good way to hide a unique, single item to a Paranoid standard of security, so if you find yourself needing to do so all we can recommend is minimising the time you need to do so for.

[4] N.T.P. note: We think storing things in public places can be a viable solution if done properly. For more information, see our Threat Library mitigation "Stash spot or safe house".

Storing Digital Information

Acceptable

Store it on a computer with full disk encryption. If you don't know how to set this up, see VeraCrypt (veracrypt.fr).[5]

If you must store it on a smartphone, e.g. because it's a messaging app that's hard to make work on a computer or because you need access to it on the go, then set a strong password on your phone (i.e. NOT just a numeric PIN) and disable fingerprint unlocking. If you think you may be going to be arrested, turn your phone off, as some methods of unlocking it only work if it's been unlocked previously since it was turned on.

If the police believe that encrypted data they've found is relevant to an investigation and that you know the password, they can legally compel you to decrypt it. The penalty for refusing can be up to two years imprisonment, or five if it's a terrorism investigation. For this reason, don't assume that even totally secure encryption will keep the police out if the evidence it protects is worth less that two years. There is a defense if you can cast doubt on whether there really is any encrypted data (this requires technical skills to set up) or on whether you really know the password.

Using cryptpad (cryptpad.org) is okay as long as you remember to set a password, and don't share the password right next to the link as this defeats most of the point of having one.

When you no longer need the information, apply the procedure for destroying digital information.

Good

Store it on an encrypted microSD card and keep it hidden, or store it in a VeraCrypt hidden volume on a traditional hard drive (i.e. not an SSD, and not a USB stick or SD card, as these can't hide the existence of a hidden volume reliably). If using an SD card or USB stick, note that they can sometimes fail. If the information is important, keep a backup, also encrypted. If you're using Tails (see the procedure for using the web), you can use the persistent storage to store information in this way, and it'll sometimes warn you before the device fails.[6]

Paranoid

We don't have a good strategy for storing digital information with a Paranoid level of security.[7] We can only recommend minimising the amount of time you have to store it for, and making it as hard as possible to prove that any one person knows the password.

[5] N.T.P. note: On computers (i.e. not smartphones) we recommend encrypting all your digital information using the full disk encryption system Linux Unified Key Setup (LUKS), which is available by default in most modern Linux systems, and thus does not require installing additional software such as VeraCrypt.

[6] N.T.P. note: The Tails persistent storage uses LUKS.

[7] N.T.P. note: An additional strategy for this level is to store the devices that contain the digital information in a tamper-evident way. For more information, see our Threat Library mitigation "Tamper-evident preparation".

Destroying Digital Information

There isn't an Acceptable level for this procedure, because overwriting is good enough to be Good but just deleting isn't good enough to be Acceptable.

Good

When a file is deleted it's not removed from the drive, it's just marked as deleted until it's overwritten by something else being stored in the same place. In order to delete it properly, you'll need to overwrite it with meaningless data first. This can be achieved with tools such as sdelete and secure-delete. However, this only applies if you're using a traditional hard drive, as opposed to an SSD (almost certainly the case in a laptop), USB stick or SD card. If you're using an one of these, this approach won't work for individual files. Instead you'll need to wipe the whole thing at once, by overwriting the entire drive using a tool like DBAN or dd.

Paranoid

Overwrite the entire drive multiple times (even if it's a traditional hard drive in case a copy has been stored somewhere for automatic backups or something). Alternatively, and this is probably overkill but quicker if you're in a hurry, physically destroy the drive it was stored on. You'll need to make sure you're actually getting at the part where the data is held. The traditional approach of drilling holes in a hard drive isn't actually that reliable, ideally you'll want intense heat or powerful magnetism.

If You Do Get Arrested

(As a reminder, this document is based on UK police practices.)

If, despite your precautions, you do get arrested, there are still things you can do — or mostly, avoid doing — to minimise the damage. What it boils down to is: DO NOT TALK TO THE POLICE FOR ANY REASON. The police are very good at tricking you into saying something incriminating or that they can use as the basis for reasonable suspicion. There are many circumstances under which talking to the police can make your life harder. There are no circumstances under which talking to the police will make your life easier (with maybe two exceptions, discussed later). If they suspect you, nothing you can possibly say will make them suspect you less. It doesn't matter how you refuse to talk to them — you can say "no comment", "I'm not going to answer that", "Am I legally obliged to answer that?", nothing at all, whatever, just don't tell them anything. Here is a list of circumstances under which you should not answer police questions:

- If they tell you they'll let you go quicker if you talk, or keep you longer if you don't. This is generally not true, and they can't keep you for too long without charging you anyway.
- If they make any kind of offer to reduce your sentence. The police don't have the authority to reduce your sentence, that's a matter for the court.
- If they offer only to charge you for a small offense if you admit to it, and drop a more serious charge. They are lying.

- If they tell you they have enough evidence already to convict you, or that an accomplice has confessed. They are probably lying, and even if they aren't, unless a competent lawyer says otherwise you probably still stand a better chance of minimising your sentence by keeping quiet.
- If they make polite small talk. Once you start talking it's easier for them to keep you talking. Remember, they're trained to extract information from people.
- If they ask questions whose answers are definitely not incriminating. If you answer these questions but then refuse to answer the questions which are incriminating, it looks pretty bad in court.
- If you have an alibi. Save it for your lawyer and the court. The police don't need to know your alibi, and they won't believe it. Anything you say to the police, you've effectively committed to saying in court. You don't have to commit to anything, so don't.
- Likewise, if they're accusing you of something you can easily prove you didn't do. It's to your advantage if they try to charge you with something you can easily prove you didn't do, as it makes the rest of the charges look less credible. Save it for your lawyer and the court.
- If they're demonstrating ignorance. It may be genuine, or they may be baiting you into showing knowledge of a topic relevant to the accusations. Either way, making fun of them isn't worth the risk.
- ANY OTHER CIRCUMSTANCES AT ALL, apart from the exceptions mentioned below.

The two cases in which it might possibly be to your advantage to tell the police something are these:

- When you arrive at the station (and not before), you may want to tell them your name and address. This is because if you refuse to provide your name and address and they decide to charge you, they can keep you locked up until the court date regardless of what you're accused of (because if they let you go they wouldn't be able to find you again). Giving false details is an offense, and they can usually check pretty easily. Note that if you do you give your address, they may go and search it.
- Under some rare circumstances, refusing to answer certain questions may be an offense in itself. A specific example of this is mentioned in the section on storing digital information — under some circumstances it may be an offense not to give up the password for encrypted data. This kind of thing doesn't come up very often, and if it is the case they'll tell you (or they should, and probably will if they actually intend to charge you with it since the court would likely require them to demonstrate that they did). Conversely though, if they tell you that you're legally obliged to answer a question, they may be lying — if at all possible verify that with your lawyer.

Last Words

Having read all that, the thing we most want to make sure is that you're not too intimidated. Like we said at the start, if the attempt to be secure leads to not taking action, the surveillance state wins without having to do anything. If you don't feel capable of achieving the level of security that you feel you'd need for the actions you want to take, take less dangerous actions in the meantime rather than focusing exclusively on learning everything about security. Real life experience is the best way to learn.

<3

Anonymous
The Briarthorn OpSec Guide
12/01/2025

Retrieved on July 31, 2025 from
https://www.notrace.how/resources/read/the-briarthorn-opsec-guide.html

theanarchistlibrary.org